ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE COMANDO E ESTADO-MAIOR

WELLINGTON AZEVEDO DOS SANTOS**,** Maj Inf

GUERRA CIBERNÉTICA E OS PRINCÍPIOS DO DIREITO INTERNACIONAL HUMANITÁRIO: um estudo de caso do conflito russo-ucraniano (2014 a 2022)

Rio de Janeiro - RJ

2024

ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE COMANDO E ESTADO-MAIOR

WELLINGTON AZEVEDO DOS SANTOS**,** Maj Inf

GUERRA CIBERNÉTICA E OS PRINCÍPIOS DO DIREITO INTERNACIONAL HUMANITÁRIO: um estudo de caso do conflito russo-ucraniano (2014 a 2022)

Trabalho de conclusão de curso apresentado à Escola de Comando e Estado-Maior da Aeronáutica como requisito parcial para aprovação no Curso de Comando e Estado-Maior.
Linha de Pesquisa: Política e Defesa.
Orientador: Gerson Monteiro Siqueira, Cel QOECOM R1.

Rio de Janeiro - RJ

2024

RESUMO

O conflito russo-ucraniano evidenciou a relevância da guerra cibernética em apoio às operações militares. Por outro lado, os efeitos produzidos no campo cibernético por vezes transbordaram para a população geral e afetaram a infraestrutura civil, fatos estes considerados ilegais de acordo o ordenamento jurídico aplicável: o DIH. Nesse contexto, objetivo geral deste estudo foi analisar em que medida os efeitos produzidos pelos ataques cibernéticos da guerra russo-ucraniana apresentam indícios de violação dos princípios do Direito Internacional Humanitário, no período de 2014 a 2022. Para cumpri-lo, utilizaram-se as técnicas de levantamento bibliográfico e documental no subsídio da coletada de dados e da análise. Assim, classificou-se a guerra russo-ucraniana como um conflito armado internacional sendo, portanto, passível da aplicação dos princípios do DIH (necessidade militar, distinção, proporcionalidade e limitação). A partir do Manual de Tallinn foi estabelecida a correlação teórica entre as operações cibernéticas e os princípios DIH, a qual viabilizou a identificação de seis ataques cibernéticos com probabilidade de causar ferimentos ou morte em pessoas ou danos ou destruição a objetos civis realizados no conflito em questão. Recorreu-se, então, ao método de estudo de caso de Yin para a tabulação e análise dos dados em função do tipo de alvo e dos respectivos efeitos. Dessarte, foi possível concluir que os efeitos produzidos pelos ataques cibernéticos analisados apresentaram indícios de violação dos princípios da necessidade militar e distinção (em 50% dos casos) e da proporcionalidade e limitação (em 100% dos casos).

Palavras-chave: ataque cibernético; conflito russo-ucraniano; direito internacional humanitário; manual de Tallinn.

RESUMEN

El conflicto ruso-ucraniano puso de relieve la relevancia de la guerra cibernética en el apoyo a las operaciones militares. Por otro lado, los efectos producidos en el ámbito cibernético en ocasiones se extendieron a la población en general y afectaron la infraestructura civil, hechos considerados ilegales según el ordenamiento jurídico aplicable: el DIH. En este contexto, el objetivo general de este estudio fue analizar en qué medida los efectos producidos por los ciberataques de la guerra ruso-ucraniana presentan signos de violación de los principios del Derecho Internacional Humanitario, en el período de 2014 a 2022. Para lograrlo, utilizamos las técnicas de levantamiento bibliográfico y documental para apoyar la recolección y análisis de datos. Así, la guerra ruso-ucraniana fue catalogada como un conflicto armado internacional y, por tanto, sujeta a la aplicación de los principios del DIH (Necesidad Militar, Distinción, Proporcionalidad y Limitación). Utilizando el Manual de Tallin, se estableció una correlación teórica entre las operaciones cibernéticas y los principios del DIH, que permitió identificar seis ataques cibernéticos que podrían causar lesiones o la muerte a personas o daños o destrucción a bienes civiles perpetrados en el conflicto en cuestión. Luego se utilizó el método de estudio de caso de Yin para tabular y analizar los datos según el tipo de objetivo y los efectos respectivos. Por lo tanto, se pudo concluir que los efectos producidos por los ciberataques analizados mostraron signos de vulneración de los principios de necesidad militar y distinción (en el 50% de los casos) y de proporcionalidad y limitación (en el 100% de los casos).

***Palabras-clave**: Ataque cibernético; Conflicto ruso-ucraniano; Ley Humanitaria Internacional; Manual de Tallinn.*

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

CAI	Conflito Armado Internacional
CANI	Conflito Armado Não Internacional
CICV	Comitê Internacional da Cruz Vermelha
DICA	Direito Internacional dos Conflitos Armados
DIH	Direito Internacional Humanitário
OE	Objetivo Específico
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
TIC	Tecnologia da Informação e da Comunicação
TPI	Tribunal Penal Internacional

SUMÁRIO

1 INTRODUÇÃO

No ano de 2014, a Rússia invadiu a Crimeia, território ucraniano. Tal ação teve como principal precedente a deposição do ex-presidente da Ucrânia, o líder pró-Rússia Viktor Yanukovy, após protestos da população local. Frente a esse cenário e sob a alegação de uma possível aliança entre a Ucrânia e a União Europeia - seguida de uma provável adesão à Organização do Tratado do Atlântico Norte (OTAN) – o presidente russo, Vladimir Putin, ordenou a ocupação daquela região (British Broadcasting Company, 2022). Posteriormente, foi orquestrado um referendo para formalizar a anexação da península, ato este considerado inválido por uma resolução da Assembleia-Geral da Organização das Nações Unidas (ONU) (Reuters, 2014).

Sobre o episódio, cabe ressaltar que a ocupação não consentida da Crimeia constitui um ato de agressão e configura uma clara violação dos princípios da Carta da ONU e do Direito Internacional, conforme definido na resolução 3314:

> Definição de Agressão [...] A invasão ou o ataque do território de um Estado pelas forças armadas de outro Estado, ou qualquer ocupação militar, ainda que temporária, que resulte dessa invasão ou ataque, ou qualquer anexação mediante o uso da força do território ou de parte do território de outro Estado (United Nations, 1974, grifo nosso).

Essa situação gerou um aumento nas tensões internacionais e a aplicação de sanções políticas e econômicas ao país invasor, com vistas a pressionar a retirada incondicional de tropas russas da região ilegalmente ocupada. No entanto, essas medidas não atingiram o objetivo e a Rússia surpreendeu o mundo lançando uma nova ofensiva militar em larga escala contra a Ucrânia, no dia 24 de fevereiro de 2022.

A ocupação da Crimeia (2014) e a invasão da Ucrânia (2022) se diferenciaram claramente quanto ao nível de intensidade das operações militares cinéticas. A primeira foi considerada a operação “mais suave dos tempos modernos”, visto que o Kremlin infiltrou militares sem insígnias ou distintivos para apoiar os movimentos separatistas locais e tomar o controle do governo, sem praticamente qualquer resistência bélica (Simpson, 2014). No extremo oposto tem-se a segunda ofensiva, considerada por especialistas como o maior confronto militar da Europa desde a Segunda Guerra Mundial, devido ao alto grau de atrito, destruição e perda de vidas humanas (Herb; Starr; Kaufman, 2022).

Não obstante, o conflito comprovou, sobretudo, a relevância da guerra cibernética em apoio às operações militares. Isso se deve à capacidade das operações cibernéticas produzirem efeitos cinéticos e não-cinéticos nos demais domínios (terrestre, marítimo, aéreo e espacial). Tal fato pôde ser comprovado na ofensiva terrestre russa, precedida de ataques cibernéticos,

que desestabilizaram as defesas ucranianas:

> Também foram verificadas as ações cibernéticas desenvolvidas pelos russos, antecedendo a ofensiva terrestre, que foram preparadas com bastante antecedência. Máquinas vitais ucranianas previamente infectadas com *softwares* maliciosos tiveram seus sistemas comprometidos antes do ataque principal, o que teve reflexos positivos para o Exército Russo de Putin (Brasil, 2022, p.115).

Ressalta-se que a guerra cibernética foi travada de forma tão intensa quanto às operações militares convencionais. Como exemplo, a Rússia lançou ataques cibernéticos que derrubaram os sites do governo, paralisaram todo o setor financeiro e comprometeram o sistema de GPS ucraniano (Jesus, 2023). Em que pese o fato de tais ataques visarem contribuir direta ou indiretamente nas operações militares, os seus efeitos por vezes transbordaram para a população geral e afetaram a infraestrutura civil, o que seria ilegal de acordo o ordenamento jurídico aplicável: o Direito Internacional Humanitário (DIH).

O DIH visa proteger as pessoas que não participam das hostilidades e regula os meios e métodos de guerra. Sua base filosófica pode ser sintetizada nos seus cinco princípios: humanidade, necessidade militar, distinção, proporcionalidade e limitação (Comitê Internacional da Cruz Vermelha, 2001). Cabe ressaltar que todos esses princípios são de cumprimento obrigatório em um conflito armado, portanto, devem ser respeitados inclusive na guerra cibernética. Isso posto, decorre a seguinte inquietação: em que medida os efeitos produzidos pelos ataques cibernéticos na guerra russo-ucraniana indicam prováveis violações dos princípios do Direito Internacional Humanitário, no período de 2014 a 2022?

Dessa forma, o objetivo geral deste estudo é analisar em que medida os efeitos produzidos pelos ataques cibernéticos da guerra russo-ucraniana apresentam indícios de violação dos princípios do Direito Internacional Humanitário, no período de 2014 a 2022.

As operações cibernéticas têm sido cada vez mais empregadas nos conflitos armados contemporâneos, tendo em vista a produção de efeitos cinéticos e não-cinéticos a partir de ataques realizados por meio do ciberespaço. No entanto, esse tipo de operação apresenta um desafio crucial ao DIH: limitar os meios e métodos e combate e assegurar a responsabilização por ataques indiscriminados que venham a afetar aos civis ou aos bens de caráter civil. Assim, a relevância da presente pesquisa recai no potencial de contribuição para o aperfeiçoamento da Doutrina Militar de Defesa Cibernética, no que concerne à observância dos princípios humanitários do direito da guerra.

2 METODOLOGIA

Na esteira de atingir o objetivo geral foi utilizada a técnica de levantamento bibliográfico, documental e delineados cinco objetivos específicos (OE), conforme se descreve a seguir:

a) definir a guerra cibernética, as operações cibernéticas e a ações cibernéticas (OE1) - Optou-se por adotar as definições previstas na doutrina brasileira, visto que foram identificadas divergências nas conceituações adotadas por outros países. Assim, a base principal de consulta foi a Doutrina Militar de Defesa Cibernética Brasileira (Brasil, 2023), sendo complementada por dados ostensivos correlatos do Departamento de Defesa Americano e publicações da Escola Superior de Guerra. Esse passo possibilitou tanto a compreensão das características da guerra cibernética quanto a delimitação dos estudos para os ataques cibernéticos, devido à capacidade de produzir efeitos cinéticos e não cinéticos no campo de batalha;

b) definir os princípios do Direito Internacional Humanitário (OE2) - Adotou-se como fonte primária os documentos e publicações constantes no site do CICV, visto que esse último é considerado o guardião do direito da guerra. Dessa forma, foram visitadas as quatro Convenções de Genebra, de 1949; os dois Protocolos Adicionais, de 1977; o Direito Internacional Relativo à Condução das Hostilidades, de 1996; e a base de dados do DIH consuetudinário. A partir disso, conheceu-se o âmbito de aplicação do DICA, os tipos de conflitos armados (internacional e não internacional) e os cinco princípios do DIH (humanidade, necessidade militar, distinção, proporcionalidade e limitação). No entanto, por se tratar de um conflito em andamento que, somado à carência de julgamentos por tribunais competentes, tornaria por deveras complexa a inferência de violações do princípio da humanidade, julgou-se coerente focar o trabalho no estudo de apenas quatros desses (necessidade militar, distinção, proporcionalidade e limitação). Por conseguinte, foi possível classificar a guerra russo-ucraniana como um conflito armado internacional sendo, portanto, aplicáveis os princípios do DIH desde a ocupação da Crimeia em 2014 até 2022 (período delimitado para estudo);

c) identificar as regras correlatas aos princípios do DIH aplicados à guerra cibernética e a imputação de responsabilidades pelos ataques (OE3) - Nessa etapa, foram consultadas as duas publicações existentes do citado documento: a primeira edição de 2013 e a mais recente de 2017. Considerando que a nova versão revisa e amplia a anterior, elegeu-se esta última como fonte de embasamento. Consequentemente, a leitura da parte IV (A Lei dos Conflitos Armados Cibernéticos) possibilitou destacar algumas regras (94, 99, 100, 104 e 119) que

claramente faziam alusão aos princípios da necessidade militar, distinção, proporcionalidade e limitação. Ainda, foi possível extrair da parte I (Direito Internacional Geral e Ciberespaço) as responsabilidades dos Estados e dos indivíduos nas operações cibernéticas, descritas nas regras 14, 15, 16, 17, 84 e 85;

d) identificar as operações cibernéticas com probabilidade de causar ferimentos ou morte em pessoas ou danos ou destruição a objetos civis realizados no conflito russo-ucraniano (OE4) - Para tanto, com base no critério de credibilidade, utilizou-se como fontes primárias o relatório da Microsoft (*Defendind Ukraine: Early Lessos From the Ciber War*) e o documento do Parlamento Europeu (*Russia's war on Ukraine: Timeline of cyber-attacks*). Já como fontes complementares foram consultados trabalhos acadêmicos do Curso Superior de Segurança e Defesa Cibernética, da Escola Superior de Guerra; e foram realizadas buscas em fontes abertas do google, utilizando a expressão "guerra cibernética Rússia Ucrânia", tendo retornado trinta e oito resultados classificados como relevantes pelo algoritmo do buscador. Com base na análise dos conteúdos desses materiais foi possível identificar seis ataques cibernéticos que causaram (ou tinham a possibilidade de causar) danos em civis ou em objetos civis; e

e) proceder um estudo de caso dos seis ataques cibernéticos selecionados à luz dos princípios do DIH e do Manual de Tallinn, com o fito de identificar potenciais violações (OE5) - Para isso, devido à inexistência de consenso teórico para o método de estudo de caso, elegeu-se como adequado ao objetivo do presente trabalho os preceitos de Yin (2001, p.32): "Um estudo de caso é um investigação empírica que investiga um fenômeno contemporâneo dentro do seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos". Ademais, o autor afirma que essa técnica é adequada quando a situação é crítica para testar uma teoria previamente estabelecida, o que seria o caso da aplicabilidade dos princípios do DICA ao conflito considerado. Nessa direção, os seis ataques selecionados foram tabulados cronologicamente em função do tipo de alvo e dos efeitos correspondentes, visando facilitar a posterior avaliação. Ato contínuo, seguindo os ensinamentos de Yin (2001), empregou-se o método de adequação ao padrão, a qual propiciou a confrontação entre a teoria (os princípios do DIH devem ser respeitados) e o caso concreto (os princípios do DIH foram respeitados?). Alicerçado nisso, consolidou-se um quadro global que viabilizou analisar o respeito aos princípios do DICA e às regras correspondentes do Manual de Tallinn nos ataques cibernéticos destacados.

Assim, logrou-se atingir o objetivo geral deste estudo que foi analisar em que medida

os efeitos produzidos pelos ataques cibernéticos da guerra russo-ucraniana apresentam indícios de violação dos princípios do Direito Internacional Humanitário, no período de 2014 a 2022.

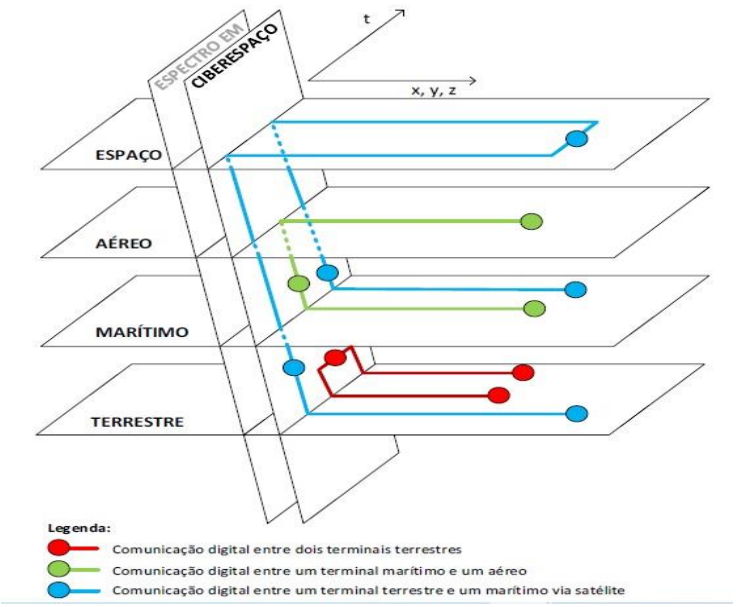
Cabe aqui pontuar alguns fatores de limitaram a presente pesquisa. Primeiramente, considerando que o conflito permanecia em andamento até a publicação deste artigo, observou-se uma carência de trabalhos acadêmicos específicos dos efeitos dos ataques cibernéticos no intervalo de estudo (2014 a 2022). Outra questão foi a ausência de sentenças judiciais transitadas em julgado (emitidas por um tribunal internacional competente) que ratificassem integralmente os dados coletados.

3 REFERENCIAL TEÓRICO

3.1 GUERRA CIBERNÉTICA

A guerra cibernética é considerada o quinto domínio da guerra contemporânea. Suas operações são desencadeadas em um espaço distinto dos demais domínios (terrestre, aéreo, marítimo e espacial), qual seja, no ciberespaço (Pagliusi, 2022). De acordo com Carneiro (2017), um dos principais diferenciais desse ambiente é a sua transversalidade em relação aos demais domínios (figura 1), o que possibilita o transbordamento de efeitos sobre o meio físico.

Figura 1 – Transversalidade do ciberespaço.



Fonte: Honorato, Santos e Mateus (2016, p. 14).

Considerando a relevância dessa recente forma de combate, torna-se imprescindível conhecer a sua definição, características e capacidades de geração de efeitos no campo de batalha.

3.1.1 Definição de Guerra Cibernética

O termo “cibernética” foi cunhado no período da Segunda Guerra Mundial pelo matemático americano Norbert Wiener, em seu livro publicado em 1948, o qual a definiu da seguinte forma: "a ciência do controle e comunicação no animal e na máquina" (Wiener, 1970 apud Filho, 2007, p.137). Naquele contexto, o estudioso buscava soluções para melhorar a eficiência do controle automático de tiro da artilharia antiaérea americana. A partir disso, construíram-se as bases para o estabelecimento de uma nova disciplina de estudo: a cibernética.

Posteriormente, com o avanço das Tecnologias da Informação e da Comunicação (TICs), os Estados buscaram aperfeiçoar os seus respectivos sistemas militares de comando e controle enquanto, por outro lado, visavam negar o acesso ao seu opositor. Essa dinâmica bidirecional de operações ofensivas e defensivas perpetradas por meio de um sistema de computares e redes, no contexto de um conflito armado, grosso modo caracteriza uma guerra cibernética.

Considerando-se a inexistência de uma definição única de guerra cibernética, elegeu-se para o presente trabalho aquela já consagrada na doutrina militar brasileira:

> Corresponde ao **uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário**, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e da Comunicação (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2 (Brasil, 2016, p. 134, grifo nosso).

Uma vez conhecido o conceito de guerra de cibernética, passemos a explorar os meios e métodos utilizados nas chamadas operações cibernéticas.

3.1.2 Operações Cibernéticas

As operações cibernéticas são basicamente ações cibernéticas realizadas no ciberespaço que visam atingir os objetivos propostos e gerar efeitos cinéticos ou não cinéticos (Brasil, 2023). Em outras palavras, seria a operacionalização efetiva do planejamento da guerra cibernética no campo de batalha.

No que tange a intencionalidade das missões, as operações cibernéticas são classificadas em defensivas e ofensivas.

3.1.2.1 Operações Cibernéticas Defensivas

Na primeira vertente estão as operações cibernéticas defensivas que têm por meta a

proteção dos sistemas de informação, das redes, da infraestrutura e dos dados contra os ataques cibernéticos inimigos. Nesse escopo ainda se enquadram, entre outros, os seguintes ativos: as redes de comando e controle; as infraestruturas críticas; os sistemas de defesa; e os recursos estratégicos nacionais. Nota-se que tais recursos têm impactos na campanha militar, logo, devem ser defendidos, como corrobora o Departamento de Defesa Americano:

> Garantiremos a segurança cibernética da Rede de Informação do Departamento de Defesa e conduziremos operações cibernéticas defensivas para protegê-la. O Departamento aumentará a resiliência cibernética da Força Conjunta e garantirá a sua capacidade de lutar dentro e através do ciberespaço contestado e congestionado (Department of Defense, 2023, p.3. tradução nossa).

3.1.2.2 Operações Cibernéticas Ofensivas

Já na segunda vertente se encontram as operações cibernéticas ofensivas, as quais objetivam explorar, atacar ou comprometer sistemas de computadores, redes ou infraestruturas digitais do oponente. Nesse diapasão, exemplificam-se algumas atividades: ataques de negação de serviço distribuída (DDoS, do inglês *Distributed Denial of Service*); intrusão em sistemas; implantação de *malware*[1]; engenharia social; e ataques de *ransomware*[2].

De acordo com um estudo publicado em 2023 pelo Instituto Internacional de Estudos Estratégicos, o uso coordenado dessas ferramentas pode produzir os seguintes efeitos: afetar cognitivamente o adversário, por meio da manipulação de informações; interromper temporariamente *websites* estratégicos; sabotar infraestruturas críticas de um Estado; desestabilizar a estrutura de comando e controle; interferir no sistema de armas; e corromper a consciência situacional do adversário (Willett, 2023).

A história recente ilustra uma série de ataques que geraram impactos significativos aos alvos, como foi o caso da Estônia, que sofreu um ataque DDoS, o qual paralisou os sistemas governamentais e financeiros, no ano de 2007 (Guedes, 2023). Outro exemplo emblemático foi o ataque *Wannacry* em 2017, um *ransomware* que se espalhou pelo mundo, atingiu mais de 150 países e causou prejuízos econômico estimados em 4 bilhões de dólares (Cybersecury & Infraestructure Security Agency, 2018). Já no contexto dos conflitos armados, cita-se a guerra russo-ucraniana, na qual o chefe da Seção de Defesa Cibernética da OTAN, Christian-Marc Liflände, afirmou que a Rússia utilizou operações preemptivas no ambiente cibernético com o intuito de moldar o campo de batalha favoravelmente à invasão (Levy, 2023).

Assim, comprova-se que por meio das operações cibernéticas se produzem resultados tangíveis e intangíveis no mundo real e virtual. Logo, torna-se importante conhecer os tipos de ações cibernéticas previstas na doutrina brasileira.

---

[1] Software malicioso para roubar dados, danificar aplicativos ou o sistema operacional.

[2] Software malicioso que criptografa os dados do computador alvo e impede o seu acesso.

3.1.3 Ações Cibernéticas

Tendo por base a Doutrina Militar de Defesa Cibernética brasileira, há três tipos de ações cibernéticas que podem ser empregadas tanto de forma ofensiva como defensiva, a saber:

Quadro 1 – Definição das Ações Cibernéticas.

TIPO DE AÇÃO CIBERNÉTICA	DEFINIÇÃO
Ataque Cibernético	"Ação sobre dispositivos, redes de computadores e comunicações do oponente para causar os seguintes efeitos cinéticos e não-cinéticos: a) destruir ou degradar equipamentos e sistemas, provocando baixas e/ou danos permanentes ou temporários, que sejam favoráveis à operação; b) degradar a capacidade de operação do oponente, reduzindo a eficácia de funcionamento dos seus sistemas; c) corromper dados de sistemas do oponente, manipulando informações de interesse do TO/A Op; d) negar o acesso do oponente a sistemas de interesse do TO/A Op; e e) interromper o funcionamento de sistemas do oponente que tragam vantagem ao TO/A Op." (Brasil, 2023, p.24)
Exploração Cibernética	"Consiste em ações destinadas a mapear sistemas e ativos de informação presentes no espaço cibernético de interesse, identificar vulnerabilidades e realizar a preparação para futuras ações ofensivas." (Brasil, 2023, p.24)
Proteção Cibernética	"Ações para garantir o funcionamento dos dispositivos computacionais, bem como prover a proteção contra ações de exploração e ataque do oponente. É uma atividade de caráter permanente." (Brasil, 2023, p.24)

Fonte: adaptado de Brasil (2023).

A partir das definições apresentadas no quadro anterior e levando-se em consideração o objetivo geral da pesquisa, restringir-se-á doravante os estudos aos ataques cibernéticos, devido ao caráter ofensivo e, principalmente, a capacidade de gerar efeitos cinéticos e não-cinéticos no Teatro de Operações.

Nessa esteira, julga-se relevante ilustrar tais efeitos com o ataque cibernético ao sistema de energia elétrica ucraniano em 2016 que afetou a aproximadamente 230 mil pessoas (Guedes, 2023). Sobre esse episódio, uma pesquisa descobriu que havia sido desenvolvido um *malware*, denominado *industroyer*, com o objetivo específico de afetar subestações de energia, a partir da abertura de disjuntores. Não obstante, tal ataque foi seguido de um *wiper*[3], projetado para apagar os computadores infectados e atrasar ainda mais o reestabelecimento dos serviços (Lameiras, 2022). Segundo investigações da inteligência americana, o responsável pela ação teria sido o governo russo, por meio do grupo denominado *Sandworm*. Ainda, de acordo com a mesma fonte, a Ucrânia estaria servindo com uma espécie de "laboratório" para operações cibernéticas.

O último exemplo nos induz ao paradoxo que pode ser observado no conflito russo-

[3] Software malicioso que destrói ou exclui permanentemente os dados do computador ou sistema alvo.

ucraniano: se por um lado um ataque cibernético se mostra mais eficaz em determinado cenário, por outro, a sua eficiência é questionável, uma vez que pode produzir efeitos indiscriminados e ser de difícil responsabilização. Diante disso, a doutrina vigente reforça a aplicabilidade do DIH à guerra cibernética, conforme corrobora Nunes (2015, p.53): "No que tange ao *jus in bello*, ou DIH, constatou-se sua plena aplicabilidade à guerra cibernética, devendo toda e qualquer ação cibernética observar seus princípios, que, em última análise, nortearão sua execução".

Logo, torna-se essencial conhecer os objetivos principais desse normativo jurídico bem como os seus princípios.

3.2 DIREITO INTERNACIONAL HUMANITÁRIO (DIH)

Na história, o código de Hamurabi (aproximadamente 1700 a.c) é considerado o primeiro conjunto de leis escritas que buscavam evitar que o mais forte oprimisse o mais fraco. Nessa toada, ao longo do tempo surgiram outros instrumentos que visavam estabelecer certa ordem nas batalhas entre tribos, povos, civilizações e, mais recentemente, entre Estados. Quanto a esse último desafio, dar-se-á um salto histórico para o século XIX - mais precisamente para a batalha de Solferino (1859) – da qual foi testemunha um homem de negócios suíço chamado Jean Henry Dunant. Indignado com as atrocidades cometidas nas disputas entre as tropas franco-italianas, Dunant publicou suas memórias na obra intitulada Lembranças de Solferino, apelando para que a comunidade internacional ratificasse acordos de prestação de serviço às vítimas e assegurasse a proteção do pessoal sanitário (Comitê Internacional da Cruz Vermelha, 2016b). Suas ideias ecoaram pelo mundo e estabeleceram as bases para a criação do Comitê Internacional da Cruz Vermelha (CICV), órgão considerado o guardião do DIH ou Direito Internacional dos Conflitos Armados (DICA).

O DIH é um ramo do direito internacional público que visa proteger os civis, os bens de caráter civis, os combatentes e os não-combatentes. Adicionalmente, intenciona limitar os meios e métodos de combate, a fim de evitar danos supérfluos e o sofrimento desnecessário. Explicando de outra forma, apresentar-se-á a definição de um renomado ex-consultor jurídico do CICV:

> [...] um corpo de normas internacionais, de origem convencional ou consuetudinária, especificamente aplicável aos conflitos armados [...] e que limita, por razões humanitárias, o direto das partes em conflito de escolherem livremente os método e meios de utilizados na guerra, ou que protege as pessoas e os bens afetados (Swinarsky, 1984, p. 18).

Torna-se fundamental pontuar que o DICA se aplica a dois tipos de hostilidades: o Conflito Armado Internacional (CAI) e o Conflito Armado Não Internacional (CANI). O

primeiro refere-se àqueles em que as hostilidades se processam entre as forças armadas dos Estados ou, eventualmente, de um povo contra uma dominação colonial (guerra de libertação nacional), no território de uma das Partes (Comitê Internacional da Cruz Vermelha, 2008). Já o segundo (CANI), diz respeito ao embate entre as forças armadas estatais e grupos armados organizados ou entre esses grupos, no território do Estado. Tais grupos de insurgentes devem apresentar um nível mínimo de organização e a capacidade de executar operações militares ofensivas e defensivas (Comitê Internacional da Cruz Vermelha, 2017).

Como base na tipologia apresentada, constata-se que a guerra russo-ucraniano pode ser classificada como um CAI, visto que há o confronto entre as forças armadas de ambas as partes. Ademais, convém ressaltar que a violação da integridade territorial de outro Estado, com o emprego de tropas, ainda que não enfrente resistência, configura o início de um conflito armado: "A Convenção se aplicará, igualmente, em todos os casos de ocupação da totalidade ou de parte do território de uma Alta Parte Contratante, mesmo que essa ocupação não encontre resistência militar" (Comitê Internacional da Cruz Vermelha, 2016a, p.37). Logo, no caso em estudo, o DICA se aplica desde a ocupação da Crimeia em 2014 até o fim do conflito.

Uma vez compreendida a origem e o propósito do DIH, discorrer-se-á sobre as suas fontes.

3.2.1 Fontes do DIH

As três fontes do DIH são: os costumes, os tratados e os princípios.

No que concerne ao primeiro, trata-se de práticas reiteradas dos Estados que passam a ter validade jurídica, desde que sejam reconhecidas pela maioria da comunidade internacional (Paula, 2003).

Já o segundo (os tratados) seriam instrumentos diplomáticos codificados na forma escrita que estabelecem acordos, aos quais os Estados se submetem de forma voluntária. A título de exemplos citam-se as Convenções de Genebra, de 1949; os dois Protocolos Adicionais, de 1977; o Direito Internacional Relativo à Condução das Hostilidades, de 1996; dentre outros.

Por fim e tão relevante quanto os demais, tem-se os princípios do DIH, os quais podem ser entendidos como uma filosofia que perpassa tanto os costumes quanto os tratados e serve de guia para a condução de um conflito ético. Logo, a concepção de novas tecnologias, armas, formas ou métodos de combate estarão sujeitos aos princípios do DIH, ainda que não haja costumes ou tratados que os regulem. O cenário descrito aplica-se perfeitamente ao

contexto da guerra cibernética russo-ucraniana, assim, faz-se mister detalhá-los doravante.

3.2.2 Princípios do DIH

O **princípio da humanidade** constitui a própria essência do Direito Humanitário, uma vez que prevê o respeito à dignidade humana, independentemente da parte a qual pertença, da condição prévia (civil ou combatente), da posição política, da crença, da raça ou de qualquer outra categorização análoga. É também considerado o princípio fundamental e busca garantir a proteção independentemente da previsão em regulamentos, conforme constata-se na Cláusula de Martens:

> **Nos casos não previstos** pelo presente Protocolo ou por outros acordos internacionais, os civis e os combatentes **ficarão sob a proteção e a autoridade dos princípios de direito internacional**, tal como resulta do costume estabelecido, dos princípios humanitários e das exigências da consciência pública (Comitê Internacional da Cruz Vermelha, 2017, p.10, grifo nosso).

Já o **princípio da necessidade militar** pode ser entendido, de forma simples, como aquele que justifica o emprego do uso da força contra pessoas ou bens. Nesse contexto, torna-se imperioso pontuar que tais ataques só serão lícitos quando deles se prever advir vantagens militares concretas. Portanto, ferir, matar ou destruir indiscriminadamente são condutas ilícitas à luz desse princípio.

> Além das proibições estabelecidas por convenções especiais, é particularmente proibido: [...] (g) Destruir ou tomar propriedades inimigas, a menos que tais destruições ou expropriações sejam exigidas **imperativamente pelas necessidades da guerra** (Comitê Internacional da Cruz Vermelha, 2001, p.25, grifo nosso).

No que tange ao **princípio da distinção**, este prevê que os ataques devem ser dirigidos única e exclusivamente contra objetivos militares, ou seja, aos bens que por sua natureza, destinação ou finalidade contribuam efetivamente para o esforço de guerra inimigo. Quanto às pessoas, são lícitas as ações direcionadas contra os combatentes ou àqueles que participarem diretamente das hostilidades sendo vedada, por consequência, atos violentos contra civis ou não-combatentes.

> [...] as Partes em conflito devem sempre fazer a distinção entre população civil e combatentes, assim como entre bens de caráter civil e objetivos militares, devendo, portanto, **dirigir suas operações unicamente contra objetivos militares** (Comitê Internacional da Cruz Vermelha, 2017, p. 38, grifo nosso).

Tem-se, ainda, um quarto quesito balizador, o **princípio da proporcionalidade**, o qual orienta que mesmo em se tratando de um objetivo militar, um ataque deverá ser evitado sempre que se supor que este possa gerar danos colaterais excessivos frente à vantagem militar esperada.

> [...] abster-se de lançar um ataque do qual se possa esperar que venha a causar acidentalmente perdas de vidas humanas na população civil, ferimentos nos civis, danos nos bens de caráter civil ou uma **combinação dessas perdas e danos que seriam excessivos relativamente à vantagem militar concreta e direta esperada** (Comitê Internacional da Cruz Vermelha, 2017, p. 44, grifo nosso).

Por fim, tem-se o **princípio da limitação** que tem por objetivo estabelecer limitação aos meios e métodos de combate, a fim de evitar os danos supérfluos e o sofrimento desnecessário. Ou seja, buscar restringir a forma de fazer a guerra, seja por meio da proibição ou restrição do emprego de certos tipos de armas ou mesmo através da proibição de táticas de guerra que produzam efeitos excessivamente danosos.

> [...] tomar todas as precauções praticamente possíveis quanto à escolha dos meios e métodos de ataque de forma a evitar ou, seja como for, **reduzir** ao mínimo, as **perdas de vidas** humanas na população civil, os **ferimentos** nos civis e os **danos** nos bens de caráter civil que puderem ser acidentalmente causados (Comitê Internacional da Cruz Vermelha, 2017, p. 44, grifo nosso).

Em que pese a existência dos cinco princípios descritos, o presente trabalho focará doravante em apenas quatros desses (necessidade militar, distinção, proporcionalidade e limitação), com vistas ao cumprimento do objetivo geral. Tal restrição se justifica pela complexidade da inferência de violações do princípio da humanidade, considerando-se tratar de um conflito em andamento somado a carência de julgamentos por tribunais competentes.

Não obstante reafirmar a aplicabilidade dos princípios do DIH à guerra cibernética, essa nova forma de combate ainda carece de regulações mais precisas. Visando atenuar essa lacuna, um grupo de especialista debateu sobre o assunto e produziu um documento denominado o Manual de Tallinn, o qual será abordado na sequência.

3.3 MANUAL DE TALLINN E O DIREITO INTERNACIONAL HUMANITÁRIO

É inegável o aumento exponencial do uso do espaço cibernético para realizar ataques em tempo de paz ou de guerra. Atento a essa realidade e a ausência de instrumentos regulatórios, um grupo de especialistas convidados pelo Centro de Excelência de Ciberdefesa Cooperativa da OTAN publicou o Manual de Tallinn, tendo a sua primeira edição lançada em 2013 e a mais recente em 2017. Tais documentos, apesar de apresentarem cunho acadêmico e caráter não vinculativo, constituem marcos fundamentais para um futuro reconhecimento internacional e a criação de tratados impositivos sobre a temática.

Tendo em vista o objeto de estudo da pesquisa, restringir-se-á a exploração desse normativo nos assuntos ligados ao *jus in bello*[4], ou seja, à guerra cibernética.

[4] É o direito na guerra, ou seja, trata-se do próprio Direito Internacional Humanitário.

3.3.1 A Guerra Cibernética e o Direito Internacional Humanitário

O Manual de Tallinn dedica a parte IV para abordar exclusivamente as operações cibernéticas no contexto dos conflitos armados. Os assuntos são divididos em cinco capítulos, a saber: a lei dos conflitos armados em geral; condução das hostilidades; certas pessoas, objetos e atividades; ocupação; e neutralidade. Considerando-se o objetivo do presente trabalho, o estudo será focado no segundo capítulo (condução das hostilidades) e buscará ressaltar as regras correlatas aos princípios do DIH anteriormente explicados, conforme demonstrado no quadro a abaixo:

Quadro 2 – Os princípios do DIH e o Manual de Tallinn.

DIH	**MANUAL DE TALLIN**	
PRINCÍPIO	**ITEM**	**DESCRIÇÃO**
NECESSIDADE MILITAR	REGRA 100	Objetivos Militares Objetivos militares são aqueles que por sua natureza, localização, finalidade ou utilização, contribuem efetivamente para a ação militar e cuja destruição, captura ou neutralização total ou parcial, nas circunstâncias vigentes no momento, oferece uma vantagem militar definitiva. (Schmitt, 2017, p. 435, tradução nossa, grifo nosso)
DISTINÇÃO	REGRA 94	Proibição de atacar civis "A população civil enquanto tal, bem como os civis individuais, não devem ser objeto de ataque cibernético." (Schmitt, 2017, p. 422, tradução nossa)
	REGRA 99	Proibição de atacar objetos civis "Objetos civis não devem ser alvos de ataques cibernéticos. A infraestrutura cibernética só poder ser objeto de ataque se for qualificado com um Objetivo Militar." (Schmitt, 2017, p. 434, tradução nossa)
PROPORCIONALIDADE	REGRA 113	Proporcionalidade "Um ataque cibernético que se suponha que possa causar perda acidental de vidas civis, danos a bens civis ou que a combinação destes seja excessivo em relação a vantagem militar esperada é proibido. (Schmitt, 2017, p. 470, tradução nossa, grifo nosso)
LIMITAÇÃO	REGRA 104	Danos Supérfluos e Sofrimento Desnecessário "É proibido empregar meios ou métodos de guerra cibernética que sejam de natureza a causar danos supérfluos e sofrimento desnecessários." (Schmitt, 2017, p. 453, tradução nossa)

Fonte: adaptado de Schmitt (2017).

Nota-se no quadro 2 que as regras destacadas do Manual de Tallinn incorporam a essência dos princípios do DICA, reafirmando a sua aplicabilidade no contexto da guerra cibernética. Portanto, julga-se crível a sua utilização no processo de análise dos efeitos produzidos pelos ataques cibernéticos no conflito em estudo, a fim de identificar eventuais descumprimentos dos princípios humanitários.

Antes de avançar, porém, convém salientar que a regra 92 do citado documento introduz a nomenclatura de "ataque" para as operações cibernéticas que tenham probabilidade de ferir pessoas ou danificar bens, no contexto de um conflito armado (Schmitt, 2017). Dessa maneira, daqui em diante as expressões que remeterem à ideia de "ataque cibernético" devem

ser interpretadas com o sentido semântico ora apresentado, visto que os efeitos descritos coincidem com os critérios de seleção das operações a serem analisadas.

Isso posto, as condutas ilícitas à luz de tal normativo devem gerar responsabilização estatal e individual.

3.3.2 Responsabilidades dos Estados

Um dos mecanismos fundamentais que estabelece o respeito às normas é a imputação de responsabilidades e a consequente penalidade. Nesse sentido, o Manual de Tallinn define um conjunto de regras aplicáveis aos Estados, dentre as quais convém destacar quatro delas no quadro a seguir:

Quadro 3 – Responsabilização Estatal.

ITEM	DESCRIÇÃO
REGRA 14	Atos Cibernéticos Intencionalmente Ilícitos "Um Estado assume responsabilidade internacional por um ato cibernético que é imputável ao Estado e que constitui uma violação de uma obrigação legal internacional." (Schmitt, 2017, p. 84, tradução nossa)
REGRA 15	Atribuição de operações cibernéticas por órgãos de Estado "As operações cibernéticas conduzidas por órgão de um Estado, ou por pessoas ou entidades habilitadas pela legislação nacional para exercer elementos de autoridade governamental, são atribuíveis ao Estado. (Schmitt, 2017, p. 87, tradução nossa)
REGRA 16	Atribuição de operações cibernéticas por órgãos de outros Estados "As operações cibernéticas realizadas por um órgão de um Estado que tenha sido colocado à disposição de outro Estado são imputáveis a este último quando o órgão atue no exercício de elementos da autoridade governamental do Estado à disposição do qual é colocado." (Schmitt, 2017, p. 93, tradução nossa)
REGRA 17	Atribuição de operações cibernéticas por atores não estatais "As operações cibernéticas conduzidas por um interveniente não estatal são atribuíveis a um Estado quando: a) envolvido de acordo com suas instruções ou sob sua direção ou controle; ou b) o Estado reconhece e adota as operações como suas." (Schmitt, 2017, p. 94, tradução nossa)

Fonte: adaptado de Schmitt (2017).

A partir de leitura das regras destacadas no quadro anterior, percebe-se que o agente estatal responde não apenas por seus atos diretos - executados por órgãos públicos ou por outros agentes habilitados pela legislação nacional - mas também por atos praticados por órgãos de outros Estados ou por atores não estatais que estejam agindo sob seu controle. Isso representa um passo fundamental na tentativa de coibir que os contendores utilizem de subterfúgios como as denominadas *cybers proxy operations*, ou seja, as operações cibernéticas por procuração. À guisa de exemplo, recorrer-se-á à análise do Departamento de Defesa dos Estados Unidos sobre o conflito russo-ucraniano:

> Essa estratégia é fortemente influenciada pela guerra de 2022 entre a Rússia e a Ucrânia, que testemunhou uma significativa utilização de capacidades cibernéticas durante o conflito armado. Nesse campo de batalha cibernética saturado, **operações militares conduzidas por Estados e *proxies* não estatais têm se chocado com os**

> **esforços de defesa cibernética de inúmeros atores do setor privado**. O conflito tem demonstrado o caráter da guerra no domínio cibernético (Department of Defense, 2023, p.1, tradução nossa, grifo nosso).

Depreende-se, portanto, que os governos russo e ucraniano poderiam responder de maneira direta (ataques executados por órgãos estatais) ou solidária (ataque executados por órgãos não estatais, a serviço do Estado interessado) por crimes de guerra que tenham sido cometidos a partir das operações cibernéticas.

Salienta-se que a responsabilização estatal não exclui o arrolamento dos indivíduos. À vista disso, faz-se imprescindível conhecer o regramento aplicável a essa categoria.

3.3.3 Responsabilidades dos indivíduos

A hiperconectividade, a dependência tecnológica dos meios militares e a capacidade de produzir efeitos, dentre outros fatores, tendem a induzir as pessoas a recorrerem à guerra cibernética de forma indiscriminada. Consequentemente, tem-se um incremento na probabilidade de cometimento de crimes de guerra, os quais redundarão na responsabilização de civis e militares envolvidos nas hostilidades, segundo descrito a seguir:

Quadro 4 – Responsabilização Individual.

ITEM	DESCRIÇÃO
REGRA 84	Responsabilidade criminal individual por crimes de guerra “Operações cibernéticas podem configurar crimes de guerra e, portanto, dar origem a responsabilidade criminal individual sob o direito internacional.” (Schmitt, 2017, p. 391, tradução nossa)
REGRA 85	Responsabilidade criminal de comandantes e superiores “a) Comandantes e outros superiores são criminalmente responsáveis por ordenar operações cibernéticas que constituam crimes de guerra. b) Comandantes também são criminalmente responsáveis se sabiam ou, devido às circunstâncias na época, deveriam saber que seus subordinados estavam cometendo, prestes a cometer ou já haviam cometido crimes de guerra, e não tomaram todas as medidas razoáveis e disponíveis para prevenir sua ocorrência ou punir os responsáveis.” (Schmitt, 2017, p. 396, tradução nossa)

Fonte: adaptado de Schmitt (2017).

Sobre essa temática, embora até a finalização deste artigo não se tenha notícias de condenações por crimes de guerra no quinto domínio, o Tribunal Penal Internacional (TPI) já iniciou as investigações para verificar em que medida os ataques cibernéticos russos afetaram a infraestrutura crítica civil (centrais de energia, bancos, hospitais, etc.) e proceder com a identificação dos responsáveis, conforme assegura o Procurador daquele órgão: “[...] como parte das investigações, o meu escritório coletará e revisará evidências de tal conduta” (Khan Kc, 2022, tradução nossa).

4 APRESENTAÇÃO DE DADOS E ANÁLISE DE RESULTADOS

4.1 APRESENTAÇÃO DE DADOS

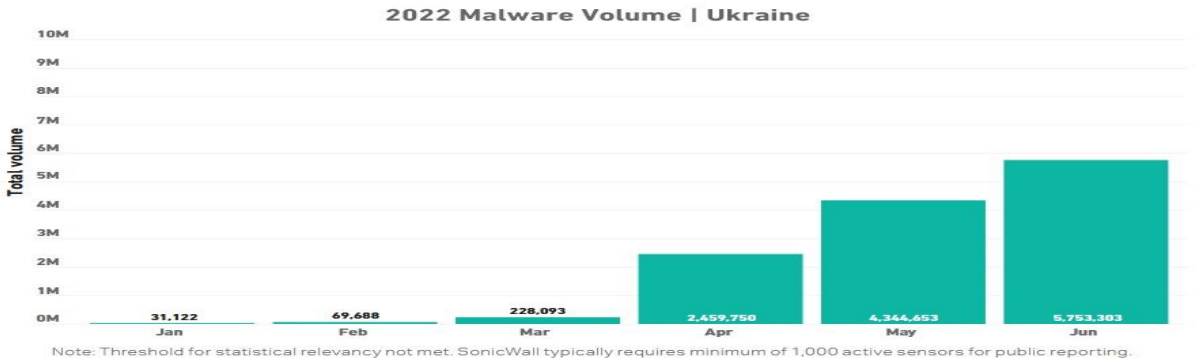
De antemão, torna-se fundamental reiterar que os dados doravante apresentados são aqueles que se encaixaram nos parâmetros de uma operação cibernética classificada como ataque, nos termos do Manual de Tallinn: “Ataque cibernético é uma operação cibernética [...] que se espera razoavelmente que cause ferimentos ou morte a pessoas ou danos ou destruição de objetos” (Schmitt, 2017, p. 415, tradução nossa). Por dita razão, foram desconsideradas as ações cibernéticas cujos propósitos eram meramente exploratórios ou defensivos.

Nesse sentido, o primeiro ataque selecionado ocorreu em 23 de dezembro de 2015, um ano após a ocupação da Crimeia, tendo sido perpetrado por grupos *hacker*s ligados à Rússia que conduziram a campanha denominada *BlackEnergy*. Essa operação consistia na realização de ataques cibernéticos direcionados às instalações ucranianas de geração e distribuição de energia nas regiões de Kiev, Ivano-Frankivsk e Chernivtsi (Mueller et al, 2023). Informações do grupo *Cyber Solution by Thales* estimam que essas ações culminaram em um blecaute que durou seis horas e afetou cerca de 230 mil pessoas (Przetacznik; Tarpova, 2022). Um segundo ataque similar ocorreu em 2016, utilizando *o malware industroyer*, que paralisou o sistema de energia em parte da capital Kiev por aproximadamente 75 minutos (Thales, 2023).

Um ano depois, em 2017, o grupo pró-russo *TeleBots* lançaram o *malware* denominado *NotPetya*, cujos alvos iniciais seriam as empresas e a infraestrutura ucraniana (Mueller et al, 2023). De fato, a usina nuclear de Chernobil, instituições públicas, companhias privadas, o sistema de transporte, o setor energético e de comunicações da Ucrânia foram afetados, tendo os seus dados criptografados e as operações comprometidas. No entanto, tais impactos não se limitaram àquele território, visto que o vírus se espalhou pelo mundo e atingiu 65 países, causando impactos econômicos da ordem de US$ 10 bilhões (Przetacznik; Tarpova, 2022).

Já em 2022 - no contexto da preparação e da consolidação da invasão militar russa - testemunhou-se um aumento exponencial nas operações cibernéticas. Alinhado a isso, um relatório divulgado pela empresa SonicWall demonstrou que só no primeiro semestre do ano o volume mensal de ataques por *malware* variou de 31.122 para 5.753.303, o que representa um acréscimo percentual de 18.383% (SonicWall, 2022). O gráfico a seguir ilustra esse cenário:

Figura 2 – Volume mensal de ataques por *malware* na Ucrânia no primeiro semestre de 2022.



Fonte: SonicWall (2022, p.11).

Esse aumento no volume de *malware* coincidiu com a mobilização de mais de 300.000 *hacktivistas*[5] de todo o mundo pelo governo ucraniano e de um movimento similar por parte de Moscou (Barros, 2023).

De acordo com o relatório publicado pela Microsoft (2023), no dia 24 de fevereiro (data da invasão) a Rússia lançou um *malware* chamado *AcidRain* contra a rede de controle dos satélites KA-SAT que, por meio do desligamento de mais de 10.000 modems, paralisou as comunicações e as redes de internet da Ucrânia e de vários países europeus, prejudicando a vida de milhões de pessoas. Houve também impactos na rede de comando e controle das forças armadas ucranianas, afirmou Dmitri Alperovitch, especialista cibernético e co-fundador do *National Security Institute* (Nakashima, 2022). Além disso, diversos Estados foram atingidos dentre os quais se destaca a Alemanha, que sofreu um grande impacto no sistema de segurança das turbinas eólicas, uma vez que a conexão via satélite era primordial para o gerenciamento remoto de mais de 5800 turbinas, em caso intempéries ou emergências.

Outra ocorrência foi registrada em 04 de março quando um *malware* foi utilizado contra sites do governo, sistema financeiro, organizações não-governamentais e de ajuda humanitária, tendo, neste último alvo, prejudicado a distribuição de alimentos, de medicamentos, roupas e a prestação de socorro às vítimas do conflito (Przetacznik; Tarpova, 2022).

Em contrapartida, *hackers* pró-ucrânia implementaram operações cibernéticas contra alvos russos. No dia 24 de junho, o grupo *GhostSec* lançou a operação *Collapse* que resultou na paralização de duas usinas de energia térmicas e na consequente falta de energia elétrica que atingiu 2 milhões de pessoas, por um período de oito horas, nas cidades de Gusinoozyorskaya e Kharanorskaya (Thales, 2023).

[5] Hackers que agem individualmente ou em grupos sob o pretexto de promover uma causa política ou social.

4.2 ANÁLISE DE RESULTADOS

O processo de análise dos dados seguiu a estratégia de estudo de caso denominada adequação ao padrão que "consiste em comparar um padrão fundamentalmente empírico com outro de base prognóstica. Se os padrões coincidirem, os resultados podem ajudar o estudo de caso a reforçar sua validade interna" (Yin, 2001, p. 136). Portanto, baseado nesses preceitos, avaliou-se os efeitos gerados pelos ataques cibernéticos à luz dos referenciais teóricos do DIH e do Manual de Tallinn, a fim de obter um prognóstico da lacuna teórico-prático.

Antes de prosseguir, porém, convém relembrar que foram abordados somente os princípios da necessidade militar, distinção, proporcionalidade e limitação, com base nas justificativas explanadas anteriormente.

Yin (2001), recomenda o uso de tabelas para categorizar/classificar os dados, com vistas a facilitar o processo de análise. Desse modo, a partir das informações coletadas na etapa anterior, foi possível agrupar os ataques cibernéticos em função do tipo de alvo e identificar os efeitos decorrentes, conforme observado a seguir:

Quadro 5 – Efeitos dos ataques cibernéticos do conflito russo-ucraniano (2014-2022).

OPERAÇÕES CIBERNÉTICAS NO CONFLITO ARMADO RÚSSIA VS UCRÂNIA		
ALVOS	**ATAQUES**	**EFEITOS**
Sistema de energia elétrica (Ucrânia)	ATAQUE 1 23/12/2015	❖ blecaute que durou seis horas e afetou cerca de 230 mil pessoas.
	ATAQUE 2 (2016)	❖ paralisou o sistema de energia em parte da capital Kiev por aproximadamente 75 minutos.
Infraestrutura pública e privada (Ucrânia)	ATAQUE 3 (2017)	❖ a usina nuclear de Chernobil, instituições públicas, companhias privadas, o sistema de transporte, o setor energético e de comunicações da Ucrânia foram afetados, tendo os seus dados criptografados e as operações comprometidas. ❖ atingiu 65 países, causando impactos econômicos da ordem de US$ 10 bilhões.
Sistema de comunicações (Ucrânia)	ATAQUE 4 (24/02/2022)	❖ paralisou as comunicações via satélite e as redes de internet da Ucrânia e de vários países europeus, prejudicando a vida de milhões de pessoas. ❖ degradou a rede de comando e controle das forças armadas ucranianas. ❖ impacto no sistema de segurança via satélite das turbinas eólicas (alemães).
Organizações governamentais e não-governamentais (Ucrânia)	ATAQUE 5 (04/03/2022)	❖ paralisou sites do governo, setor financeiro e instituições de ajuda humanitária. ❖ prejudicou a distribuição de alimentos, de medicamentos, roupas e a prestação de socorro às vítimas do conflito.
Sistema de energia elétrica (Rússia)	ATAQUE 6 (24/06/2022)	❖ paralização de duas usinas de energia térmicas e a consequente falta de energia elétrica que atingiu 2 milhões de pessoas, por um período de oito horas, nas cidades de Gusinoozyorskaya e Kharanorskaya.

Fonte: o autor.

Com base no quadro 5, nota-se que os ataques cibernéticos 1 e 2 causaram impactos significativos ao sistema de energia ucraniano, enquanto o ataque 3 afetou a infraestrutura pública e privada na Ucrânia e transbordou para outros países.

Quanto a esses três primeiros ataques, é primordial pontuar que ocorreram no contexto pré-invasão militar russa e que, segundo especialistas, a Ucrânia serviu como um laboratório de testes para o desenvolvimento de novas armas cibernéticas do Kremlin (Fonseca, 2023). Diante desse cenário, os dados mostraram que o ataque 1 (russo) produziu um blecaute que durou seis horas e afetou cerca de 230 mil pessoas, não tendo sido encontrados quaisquer indícios de que tenha sido dirigido contra objetivos militares. Avaliação similar foi feita para ataque 2 (russo), que paralisou o sistema de energia em parte da capital Kiev por aproximadamente 75 minutos. Quanto ao ataque 3 (russo), houve o comprometimento das operações da usina nuclear de Chernobil, de instituições públicas, de companhias privadas, do sistema de transporte, do setor energético, do sistema de comunicações da Ucrânia e impactos econômicos mundiais da ordem de US$ 10 bilhões.

A análise dos ataques contra os sistemas de energia elétrica e a infraestrutura pública e privada dos contendores produziram efeitos que trouxeram transtornos à população civil, sendo desconhecida, até o momento, quaisquer necessidades militares imperiosas que as justificassem. Ademais, a situação que sucedeu no intervalo entre a anexação “suave” e ilegal da Crimeia e a invasão militar de 2022 configurou uma zona cinzenta na qual, embora fosse classificada como um conflito armado nos termos do DICA, não se testemunharam operações militares clássicas que permitissem identificar claramente os objetivos militares, tanto na região ocupada quanto em outras partes do território ucraniano. Logo, fica constatada uma provável violação da regra 100 do Manual de Tallinn, visto que os alvos atingidos pelos ataques cibernéticos não pareciam contribuir efetivamente para a operações militares nem ofereciam uma vantagem militar definitiva (Schmitt, 2017). Por conseguinte, a inexistência de justificativas que permitam classificar um determinado alvo como objetivo militar tornam o ataque ilegal a luz do DICA e, consequentemente, ferem os princípios da necessidade militar (não ofereceu uma vantagem militar definitiva), proporcionalidade (os danos colaterais foram excessivos frente ao imperceptível ganho operacional), distinção (atingiu a população civil e os bens civis) e limitação (causou sofrimento desnecessário) (Comitê Internacional da Cruz Vermelha, 2017).

As discussões conduzidas até o momento podem ser sintetizadas no próximo quadro:

Quadro 6 – Análise dos ataques cibernéticos pré-invasão.

SISTEMA DE ENERGIA ELÉTRICA E A INFRAESTRUTURA PÚBLICA E PRIVADA					
OS PRINCÍPIOS DO DIH E AS REGRAS NO MANUAL DO TALLINN FORAM RESPEITADAS?					
PERÍODO	AÇÃO	NECESSIDADE MILITAR (regra 100)	DISTINÇÃO (regras 94 e 99)	PROPORCIONALIDADE (regra 113)	LIMITAÇÃO (regra 104)
Pré-invasão	Ataque 1	Não	Não	Não	Não
	Ataque 2	Não	Não	Não	Não
	Ataque 3	Não	Não	Não	Não

Fonte: o autor.

Revisitando o quadro 5, proceder-se-á a avaliação dos demais ataques, ou seja, aqueles direcionados aos alvos do sistema de comunicações, organizações governamentais e não-governamentais. Antes, porém, deve-se ponderar que o ambiente de análise difere do anterior dado que doravante serão discutidas as hostilidades pós invasão russa, ou seja, em um cenário de operações militar ostensivas e de alta intensidade.

Um outro parêntese que se deve aqui pontuar, foi que o recrutamento de mais de 300.000 *hacktivistas* e o crescimento exponencial dos ataques por *malware* (18.383%) não geraram um incremento de similar proporção de efeitos nocivos à integridade física das pessoas ou dos bens protegidos. Quanto a esse ponto particular, o Manual de Tallinn pode embasar uma possível resposta, posto que nele consta a previsão da imputação de responsabilidade penal ao Estado agressor que atue por intermédio de seus próprios órgãos (regras 14 e 15), de órgãos de outros Estados (regra 16) ou de atores não estatais (regra 17). Ademais, estende-se a responsabilidade pessoal aos comandantes, superiores (regras 85) e indivíduos (regra 84) que venham a cometer crimes de guerra (Schimitt, 2017). Portanto, a mera previsão de punibilidade pelos atos praticados no ciberespaço nessa fase do conflito pode justificar, em certa medida, a limitação dos efeitos desses ataques cibernéticos.

Feitas as considerações preliminares, passemos ao estudo dos ataques 4, 5 e 6 direcionados aos sistemas de comunicações, organizações governamentais e não-governamentais.

O ataque 4 (russo) paralisou as comunicações via satélite, degradando a rede de comando e controle das forças armadas ucranianas. No aspecto militar, os sistemas de comunicações do inimigo constituem objetivos militares claros, uma vez que são fundamentais para o gerenciamento das atividades no campo de batalha, fatores esses que permitem embasar o ataque à luz dos princípios da necessidade militar (gera uma vantagem militar) e da distinção (se trata de um objetivo militar) (Comitê Internacional da Cruz Vermelha, 2017). Por outro lado, esse ataque também comprometeu o sistema de internet da

Ucrânia e de vários países europeus, prejudicando a vida de milhões de pessoas, além de afetar o sistema de segurança via satélite das turbinas eólicas (alemães). Logo, todos esses danos colaterais parecem excessivos frente à vantagem militar pretendida (proporcionalidade) e o meios ou métodos inapropriados (limitação), segundo os princípios do DICA e o Manual de Tallinn (Schmitt, 2017).

Com relação ao ataque 5 (russo), atingiu sites do governo e do setor financeiro. No que concerne a esses alvos, têm o potencial de afetar o poder político e econômico do Estado, buscando comprometer a vontade e a capacidade de combater pois, como prega Clausewitz (1996, p. 27), "a guerra é um ato de força para compelir o inimigo a fazer a nossa vontade". Por isso, a operação pode ser justificada à luz do princípio da necessidade militar, posto que pode influenciar o poder político adversário e ocasionar transtornos às transações financeiras essenciais ao esforço de guerra (Comitê Internacional da Cruz Vermelha, 2017). Argumentos similares permitem caracterizar esses alvos como objetivos militares, fato este que ampara o princípio da distinção. Sob outro ângulo, a mesma ação cibernética prejudicou a distribuição de alimentos, medicamentos, roupas e a prestação de socorro às vítimas do conflito, o que caracteriza um dano colateral excessivo aos não-combatentes. Assim, uma vez mais, os princípios da proporcionalidade e da limitação parecem ter sido inobservados.

Já para o ataque 6 (ucraniano), as fontes apontaram que teria ocorrido em retaliação às investidas russas e implicou na paralização de duas usinas de energia térmicas e na consequente falta de energia elétrica que atingiu 2 milhões de pessoas, por um período de oito horas, nas cidades de Gusinoozyorskaya e Kharanorskaya. Embora se desconheça com exatidão a localização das bases militares russas e a sua cadeia logística, considerando a natureza do alvo, pode-se presumir a probabilidade de que este exercesse alguma influência no esforço de guerra nacional, fato que o caracterizaria como um objetivo militar, cumprindo os princípios da necessidade militar e da distinção. No que tange aos 2 milhões de cidadãos que sofreram pelos apagões, isso retrata os danos acidentalmente produzidos que parecem excessivos frente a uma suposta vantagem militar, fatos que culminam na inobservância dos já definidos princípios da proporcionalidade e da limitação.

Findada a avaliação dos três últimos ataques selecionados, convém sintetizá-la no quadro vindouro.

Quadro 7 – Análise dos ataques cibernéticos pós-invasão.

SISTEMA DE COMUNICAÇÕES, ORGANIZAÇÕES GOVERNAMENTAIS E NÃO-GOVERNAMENTAIS					
OS PRINCÍPIOS DO DIH E AS REGRAS NO MANUAL DO TALLINN FORAM RESPEITADAS?					
PERÍODO	AÇÃO	NECESSIDADE MILITAR (regra 100)	DISTINÇÃO (regras 94 e 99)	PROPORCIONALIDADE (regra 113)	LIMITAÇÃO (regra 104)
Pós-Invasão	Ataque 4	Sim	Sim	Não	Não
	Ataque 5	Sim	Sim	Não	Não
	Ataque 6	Sim	Sim	Não	Não

Fonte: o autor.

Com o propósito de lograr uma análise global dos ataques cibernéticos à luz dos princípios do DIH e de Manual de Tallinn, faz-se mister agrupar todos os resultados auferidos, a fim de embasar conclusões subsequentes.

Quadro 8 – Análise global percentual dos ataques cibernéticos (pré e pós-invasão).

ATAQUES CIBERNÉTICOS (2014 – 2022)					
OS PRINCÍPIOS DO DIH E AS REGRAS NO MANUAL DO TALLINN FORAM RESPEITADAS?					
PERÍODO	AÇÃO	NECESSIDADE MILITAR (regra 100)	DISTINÇÃO (regras 94 e 99)	PROPORCIONALIDADE (regra 113)	LIMITAÇÃO (regra 104)
Pré-invasão	Ataque 1	Não	Não	Não	Não
	Ataque 2	Não	Não	Não	Não
	Ataque 3	Não	Não	Não	Não
Pós-Invasão	Ataque 4	Sim	Sim	Não	Não
	Ataque 5	Sim	Sim	Não	Não
	Ataque 6	Sim	Sim	Não	Não
PERCENTUAL DE VIOLAÇÃO		50%	50%	100%	100%

Fonte: o autor.

Observando o quadro 8, percebe-se que os ataques cibernéticos pré-invasão russa tiveram como ponto de convergência o desrespeito a todos os princípios do DIH e as regras correspondentes do Manual de Tallinn. Sobre isso, o estudo apontou que a zona cinzenta (limiar entre guerra e paz) foi característica marcante do período entre a anexação ilegal da Criméia (2014) e a invasão militar (2022), fato que teria transformado a Ucrânia em um campo de provas de armas cibernéticas russas. Nesse contexto, a resolução 3314 da ONU classificou a ocupação da Crimeia como um ato de agressão, o que permitiu enquadrar a disputa como um conflito armando internacional. Diante desse cenário, a lei internacional estipula que são proibidos os ataques indiscriminados contra a população civil e os bens civis, algo que foi reiteradamente descumprido pelo governo russo e seus simpatizantes.

Passando o período pós-invasão, tem-se um cenário explícito de conflito armado. Nesse ambiente, foram considerados os objetivos militares clássicos (quartéis, aeronaves, hangares, etc.) bem como os que, em determinados contextos, passam a ter esse status devido

à sua finalidade (infraestruturas críticas, sistemas de uso civil-militar, dentre outros). Contudo, ainda que se trate de um objetivo militar, o DIH prevê que deverá ser feito todo o possível para que não haja danos colaterais aos civis (pessoas ou bens). Levando-se em conta esses preceitos, verificou-se que a totalidade dos ataques foram dirigidos à objetivos militares clássicos ou com tal status, sendo, portanto, respeitado os princípios da necessidade militar e da distinção. Apesar disso, foram produzidos danos colaterais que afetaram de forma considerável a população civil, sem a justificativa clara de uma vantagem militar concreta esperada, fato este que redundou na violação dos princípios da proporcionalidade e da limitação.

Considerando tudo o que foi posto, é possível concluir que os efeitos produzidos pelos ataques cibernéticos analisados apresentaram indícios de violação dos princípios da necessidade militar e distinção (em 50% dos casos) e da proporcionalidade e limitação (em 100% dos casos).

5 CONCLUSÃO

No ano de 2014, a Rússia ocupou de forma “suave” a Crimeia (território ucraniano) dando início ao conflito armado internacional, segundo resolução da ONU. Posteriormente, no dia 24 de fevereiro de 2022, a Rússia surpreendeu o mundo lançando uma nova ofensiva militar em larga escala contra a Ucrânia.

Esse conflito evidenciou a relevância da guerra cibernética em apoio às operações militares. Tal fato pôde ser comprovado na ofensiva terrestre russa, precedida de ataques cibernéticos, que desestabilizaram as defesas ucranianas. Por outro lado, os efeitos produzidos no campo cibernético por vezes transbordaram para a população geral e afetaram a infraestrutura civil, fatos estes considerados ilegais de acordo o ordenamento jurídico aplicável: o Direito Internacional Humanitário (DIH).

O DIH visa proteger as pessoas que não participam das hostilidades e regula os meios e métodos de guerra. Sua base filosófica pode ser sintetizada nos seus cinco princípios de cumprimento obrigatório: humanidade, necessidade militar, distinção, proporcionalidade e limitação. Nesse contexto, objetivo geral deste estudo foi analisar em que medida os efeitos produzidos pelos ataques cibernéticos da guerra russo-ucraniana apresentam indícios de violação dos princípios do Direito Internacional Humanitário, no período de 2014 a 2022.

Na esteira de atingir o objetivo geral, foram desdobrados cinco objetivos específicos. Assim, o primeiro possibilitou definir a guerra cibernética, as operações cibernéticas e a ações cibernéticas, convencionando-se adotar aquelas previstas na doutrina brasileira. Com base

nesse conhecimento, delimitou-se os estudos subsequentes para os ataques cibernéticos, devido à capacidade de produzir efeitos cinéticos e não cinéticos no cambo de batalha.

Quanto ao segundo objetivo específico, permitiu definir os princípios do Direito Internacional Humanitário. Além disso, conheceu-se o âmbito de aplicação desse ramo do direito, os tipos de conflitos armados (internacional e não internacional) e os princípios da humanidade, necessidade militar, distinção, proporcionalidade e limitação. No entanto, excluiu-se das análises o primeiro princípio (humanidade) devido à carência de evidências minimamente confiáveis de violações. A partir desses conhecimentos foi possível classificar a guerra russo-ucraniana como um conflito armado internacional passível da aplicação dos princípios do DIH, desde a ocupação da Crimeia em 2014 até 2022 (período delimitado para estudo).

Por meio do terceiro objetivo específico, logrou-se identificar no Manual de Tallinn as regras correspondentes aos princípios do DIH aplicados à guerra cibernética e a previsão de imputação de responsabilidades pelos ataques. Nessa etapa, foi estabelecida a correlação teórica entre as operações cibernéticas e os quatro princípios (necessidade militar, distinção, proporcionalidade e limitação) que serviram de base para a fase de análise dos dados.

No que concerne ao quarto objetivo específico, viabilizou a identificação de seis ataques cibernéticos com probabilidade de causar ferimentos ou morte em pessoas ou danos ou destruição a objetos civis realizados no conflito em questão. Tais dados tiveram como fontes primárias o relatório da Microsoft e o documento do Parlamento Europeu, sendo complementadas por trabalhos acadêmicos do Curso Superior de Segurança e Defesa Cibernética, da Escola Superior de Guerra e por fontes abertas do google.

Já o quinto e último objetivo específico, possibilitou identificar potenciais violações dos princípios do DIH nos seis ataques cibernéticos selecionados. Para isso, recorreu-se ao método de estudo de caso de Yin, haja vista o alto grau de criticidade e complexidade do ambiente a ser investigado. Assim, os ataques cibernéticos foram tabulados em função do tipo de alvo e dos respectivos efeitos. Essa organização permitiu realizar a análise em duas etapas: pré e pós invasão. Na primeira, verificou-se indícios de que os três ataques infringiram todos os quatro princípios do DICA. Na outra etapa (pós-invasão), as evidências apontaram que os três ataques remanescentes teriam cumprido dois princípios (necessidade militar e distinção), porém, descumprido outros dois (proporcionalidade e limitação). Alicerçado nisso, consolidou-se um quadro global que possibilitou analisar o respeito aos princípios do DICA e as regras do Manual de Tallinn nos ataques cibernéticos destacados. Dessarte, foi possível

concluir que os efeitos produzidos pelos ataques cibernéticos analisados apresentaram indícios de violação dos princípios da necessidade militar e distinção (em 50% dos casos) e da proporcionalidade e limitação (em 100% dos casos).

Seguindo todas as etapas anteriores, logrou-se cumprir o objetivo geral e responder ao problema de pesquisa, posto que foi possível analisar os efeitos dos ataques cibernéticos no conflito russo-ucraniano (2014 a 2022) e gerar resultados que permitiram indicar grau de inobservância dos princípios do DIH.

Em que pese as limitações de estudo impostas por um conflito em andamento (escassez de publicações científicas e a ausência de sentenças judiciais transitadas em julgado), os resultados aqui postulados podem contribuir para o fortalecimento da doutrina de guerra cibernética da FAB e para o aprimoramento das táticas, técnicas e procedimentos, a fim de assegurar o respeito ao DICA no cumprimento das missões e evitar o cometimento de crimes de guerra.

À guisa de arremate, esta pesquisa não teve a pretensão de esgotar a discussão sobre a aplicabilidade dos princípios do DIH no âmbito da guerra cibernética. Logo, sugere-se a realização de trabalhos que investiguem os efeitos das operações cibernéticas em outros conflitos armados, com o objetivo de gerar novos subsídios que permitam apurar cada vez mais a doutrina nacional de defesa cibernética, sem descuidar do respeito às leis da guerra.

REFERÊNCIAS

BARROS, Marcelo. **Ucrânia quer integrar hackers voluntários às Forças Armadas**. [*S.l.*], 2023. Disponível em: https://dciber.org/ucrania-quer-integrar-hackers-voluntarios-as-forcas-armadas/. Acesso em: 14 maio 2024.

BRASIL. Ministério da Defesa. Gabinete do Ministro. **ESTUDOS MILITARES CONJUNTOS:** conflito Rússia-Ucrânia, possíveis ensinamentos para o emprego conjunto das Forças Armadas**.** Rio de Janeiro, RJ, 2022. Disponível em: https://www.gov.br/esg/pt-br/centrais-de-conteudo/publicacoes/operacoes-conjuntas-artigos-doutrinarios/arquivos/idoc__conflito-rus-x-ucr-estudo-emprego-conj_monografia_24ago2022__impressao-final-atualizado.pdf. Acesso em 24 fev. 2024.

BRASIL. Ministério da Defesa. Portaria 9/GAP/MD, de 13 de janeiro de 2016. Glossário das Forças Armadas - MD35-G-01 (5ª Edição/2015). **Diário Oficial da União.** Brasília, n. 14, 21 jan 2016. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/141. Acesso em: 02 abr. 2024.

BRASIL. Ministério da Defesa. Portaria GM-MD n° 5.081, de 16 de outubro de 2023. Aprova a Doutrina Militar de Defesa Cibernética - MD31-M-07 (2ª Edição/2023). **Diário Oficial da União.** Brasília, n. 203, 25 out 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 27 fev. 2024.

BRITISH BROADCASTING COMPANY. **Por que a invasão da Crimeia em 2014 é relevante agora**. [*S.l.*], 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60570951. Acesso em: 03 mar. 2024.

CARNEIRO, João Marinonio Enke. As relações entre Defesa e Soberania no Espaço Cibernético. [*S.l.*], 2017. Disponível em: https://www.encontro2017.abri.org.br/resources/anais/8/1498479573_ARQUIVO_artigo_ABRI_Joao_Carneiro.pdf. Acesso em: 25 fev. 2024.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **Direito Internacional Relativo à Condução das Hostilidades**. Genebra: Comitê Internacional da Cruz Vermelha, 2001.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **Como o Direito Internacional Humanitário define conflitos armados?** [*S.l.*], 2008. Disponível em: https://www.icrc.org/pt/doc/assets/files/other/rev-definicao-de-conflitos-armados.pdf. Acesso em: 25 fev. 2024.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **Convenções de Genebra de 1949**. Genebra: Comitê Internacional da Cruz Vermelha, 2016a.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **LEMBRANÇA DE SOLFERINO**. Genebra: Comitê Internacional da Cruz Vermelha, 2016b. Disponível em: https://www.icrc.org/pt/document/lembranca-de-solferino-publicacao. Acesso em: 05 abr. 2024.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **Protocolos Adicionais às Convenções de Genebra de 1949**. Genebra: Comitê Internacional da Cruz Vermelha, 2017.

CYBERSECURY & INFRAESTRUCTURE SECURITY AGENCY. **Indicators Associated With WannaCry Ransomware**. [*S.l.*], 2018. Disponível em: https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware. Acesso em: 02 maio 2024.

CLAUSEWITZ, Carl von. **Da Guerra**. Tradução de Maria Teresa Ramos. 2. ed. São Paulo: Martins Fontes e Brasília: EdUNB, 1996.

DEPARTMENT OF DEFENSE. **CYBER ESTRATEGY 2023**. Washington, D.C, 2023. Disponível em: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF. Acesso em: 02 abr. 2024.

FONSECA, Leila Oliveira. **A guerra cibernética e o conflito Rússia versus Ucrânia**. Revista de Relações Exteriores. [*S. l.*], 24 fev. 2023. Disponível em: https://relacoesexteriores.com.br/a-guerra-cibernetica-e-o-conflito-russia-versus-ucrania/. Acesso em: 1 abr. 2024.

FILHO, Cléuzio Fonseca. **História da Computação:** O caminho do pensamento e da tecnologia. Porto Alegre: EDIPUCRS, 2007. 204 p.

GUEDES, Richard. **Guerra cibernética: tipos, armas, objetivos e exemplos de guerra tecnológica**. [*S. l.*], 2023. Disponível em: https://dciber.org/guerra-cibernetica-tipos-armas-objetivos-e-exemplos-de-guerra-tecnologica/. Acesso em: 06 abr. 2024.

HERB, Jeremy; STARR, Barbara; KAUFMAN, Ellie. CNN. **US orders 7,000 more troops to Europe following Russia's invasion of Ukraine**. [*S. l.*], 2022. Disponível em: https://edition.cnn.com/2022/02/24/politics/us-military-ukraine-russia/index.html. Acesso em: 25 abr. 2024.

HONORATO, Manuel Costa; SANTOS, Luís Filipe Camelo Duarte; MATEUS, Regina Maria Jesus Ramos. **O Ciberespaço como 5º Domínio Operacional**. Instituto Universitário Militar, Lisboa, 2016. Disponível em: https://comum.rcaap.pt/handle/10400.26/21956. Acesso em: 06 abr. 2024.

JESUS, Emanuel Ferreira. **OS EFEITOS DAS AÇÕES CIBERNÉTICAS SOBRE AS CAPACIDADES MILITARES NO COMBATE CONTEMPORÂNEO**: qual é o impacto dos ataques cibernéticos preemptivos nas operações militares contemporâneas? 2023. 20 f. TCC - Curso de Curso Superior de Segurança e Defesa Cibernética, Departamento de Estudos, Escola Superior de Guerra, Rio de Janeiro, 2023. Disponível em: https://repositorio.esg.br/bitstream/123456789/1792/1/cssdc.10.CF.%20Jesus.REV.pdf. Acesso em: 27 fev. 2024.

KHAN KC, Karim Asad Ahmad. **Technology Will Not Exceed Our Humanity**. [*S. l.*], 2022. Disponível em: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/. Acesso em: 06 abr. 2024.

LAMEIRAS, André. **Industroyer**: uma ameaça cibernética que derrubou uma rede elétrica.

[*S. l.*], 2022. Disponível em: https://www.welivesecurity.com/br/2022/06/13/industroyer-uma-ameaca-cibernetica-que-derrubou-uma-rede-eletrica/. Acesso em: 02 maio 2024.

LEVY, Clarissa. **O que o conflito na Ucrânia nos ensina sobre guerra cibernética?** [*S. l.*], 2023. Disponível em: https://www.swissinfo.ch/por/economia/o-que-o-conflito-na-ucr%c3%a2nia-nos-ensina-sobre-guerra-cibern%c3%a9tica/48238890. Acesso em: 02 maio 2024.

MICROSOFT. **Microsoft Digital Defense Report 2023**: Global Cyberattacks. [*S. l.*], 2023. Disponível em: https://www.microsoft.com/en/security/securityinsider/microsoft-digital-defense-report-2023/. Acesso em: 24 fev. 2024.

MUELLER, Grace B., *et al*. **Cyber Operations during the Russo-Ukrainian War: from strange patterns to alternative futures**. [*S. l.*], 2023. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-07/230713_Mueller_CyberOps_RussiaUkraine.pdf?VersionId=BwNbsmkThLIPVpB0tctC59kwVpZ2aXeI. Acesso em: 06 abr. 2024.

NAKASHIMA, Ellen. **Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say**. [*S. l.*], 2022. Disponível em: https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/. Acesso em: 14 jun. 2024.

NUNES, Luiz Artur Rodrigues. **GUERRA CIBERNÉTICA E O DIREITO INTERNACIONAL**: aplicabilidade do jus ad bellum e do jus in bello. 2015. 60 f. Monografia - Curso de Altos Estudos de Política e Estratégia, Departamento de Estudos, Escola Superior de Guerra, Rio de Janeiro, 2015. Disponível em: https://repositorio.esg.br/bitstream/123456789/1277/1/Luiz%20Artur%20RODRIGUES%20Nunes.pdf. Acesso em: 01 jul. 2024.

PAGLIUSI, Paulo Sergio. GUERRA CIBERNÉTICA RUSSO-UCRANIANA: lições para o brasil e o mundo. **Revista do Clube Naval**: Soberania pela Ciência, Brasília, v. 2, p. 74-79, 25 ago. 2022. Disponível em: https://portaldeperiodicos.marinha.mil.br/index.php/clubenaval/article/view/3189/3020. Acesso em: 27 fev. 2024.

PAULA, Alexandre Sturion de. **Costumes Internacionais**. [*S. l.*], 2003. Disponível em: https://www.direitonet.com.br/artigos/exibir/992/Costumes-Internacionais. Acesso em: 04 abr. 2024.

PRZETACZNIK, Jakub; TARPOVA, Simona. **Russia's war on Ukraine**: timeline of cyber-attacks. Timeline of cyber-attacks. [*S. l.*], 2022. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf. Acesso em: 14 jun. 2024.

REUTERS. **ONU aprova resolução que condena anexação russa da Crimeia**. [*S. l.*], 2014. Disponível em: https://g1.globo.com/mundo/noticia/2014/03/onu-aprova-resolucao-que-condena-anexacao-russa-da-crimeia.html. Acesso em: 27 mar. 2024.

SCHMITT, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warfare**. New York: Cambridge University Press, 2017.

SIMPSON, John. **O plano que permitiu à Rússia a anexação secreta da Crimeia**. [*S. l.*], 2014. Disponível em: https://www.bbc.com/portuguese/noticias/2014/03/140319_golpe_crimeia_lk. Acesso em: 06 abr. 2024.

SONICWALL. **Cyber Threat Report**. [*S. l.*], 2022. Disponível em: https://www.sonicwall.com/resources/white-papers/2022-sonicwall-cyber-threat-report/. Acesso em: 06 abr. 2024.

SWINARSKY, Christophe. **Introdução ao Direito Internacional Humanitário**. Genebra: Comitê Internacional da Cruz Vermelha, 1984.

THALES. Cyber Solution by Thales. **A year of Cyber Conflict in Ukraine**. [*S. l.*], 2023. Disponível em: https://myfeed.thalesgroup.com/cyber-conflict-ukraine-extensive-report. Acesso em: 24 fev. 2024.

UNITED NATIONS. **Definition of Aggression**: general assembly resolution 3314 (XXIX). General Assembly resolution 3314 (XXIX). New York, 1974. Disponível em: https://legal.un.org/avl/ha/da/da.html. Acesso em: 06 mar. 2024.

WILLETT, Marcus. **Offensive cyber and the responsible use of cyber power**. [*S. l.*], 2023. Disponível em: https://www.iiss.org/online-analysis/online-analysis/2023/03/offensive-cyber-and-the-responsible-use-of-cyber-power/. Acesso em: 06 abr. 2024.

YIN, Robert K. **Estudo de caso**: planejamento e métodos. Porto Alegre: Boookman, 2001.