



**UNIVERSIDADE FEDERAL DO CEARÁ**  
**FACULDADE DE DIREITO**  
**CURSO DE GRADUAÇÃO EM DIREITO**

**TALES MESQUITA MUNIZ**

**OS CIBERATAQUES NO CONTEXTO DAS GUERRAS VIRTUAIS: A APLICAÇÃO  
DO DIREITO INTERNACIONAL HUMANITÁRIO FRENTE A ESSAS CONDUTAS**

**FORTALEZA**

**2022**

TALES MESQUITA MUNIZ

OS CIBERATAQUES NO CONTEXTO DAS GUERRAS VIRTUAIS: A APLICAÇÃO DO  
DIREITO INTERNACIONAL HUMANITÁRIO FRENTE A ESSAS CONDUTAS

Monografia apresentada ao Curso de Direito da Faculdade de Direito da Universidade Federal do Ceará, na qualidade de Trabalho de Conclusão de Curso, como requisito parcial para obtenção do título de Bacharel em Direito. Área de concentração: Direito Internacional Público.

Orientador: Prof. D.r William Paiva Marques Júnior.

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação  
Universidade Federal do Ceará  
Sistema de Bibliotecas

Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

---

M936c Muniz, Tales Mesquita.

Os ciberataques no contexto das guerras virtuais : a aplicação do Direito Internacional Humanitário frente a essas condutas / Tales Mesquita Muniz. – 2022.  
60 f.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2022.

Orientação: Prof. Dr. William Paiva Marques Júnior.

1. Direito Internacional Humanitário. 2. Guerras Virtuais. 3. Ciberataques. 4. Internet. I. Título.

CDD 340

---

TALES MESQUITA MUNIZ

OS CIBERATAQUES NO CONTEXTO DAS GUERRAS VIRTUAIS: A APLICAÇÃO DO  
DIREITO INTERNACIONAL HUMANITÁRIO FRENTE A ESSAS CONDUTAS

Monografia apresentada ao Curso de Direito da Faculdade de Direito da Universidade Federal do Ceará, na qualidade de Trabalho de Conclusão de Curso, como requisito parcial para obtenção do título de Bacharel em Direito. Área de concentração: Direito Internacional Público.

Aprovada em 23/11/2022.

BANCA EXAMINADORA

---

Prof. D.r William Paiva Marques Júnior (Orientador)  
Universidade Federal do Ceará (UFC)

---

Prof.<sup>a</sup> M.<sup>a</sup> Fernanda Cláudia Araújo da Silva  
Universidade Federal do Ceará (UFC)

---

Lucas Salles Gazeta Vieira Fernandes (Mestrando)  
Universidade Federal do Ceará (UFC)

À minha família, que sempre primou por uma educação de excelência para mim, embora a vida tenha apresentado vários obstáculos para que se atingisse esse objetivo. Essa conquista é de todos que contribuíram com isso. Queria nomear, entretanto, os principais responsáveis por toda a formação do caminho da minha vida, meus pais: Dina Mesquita e Germano Muniz Filho. A influência, o amor e o suporte deles resultou neste trabalho e no fim de mais um ciclo. Portanto, esta monografia é dedicada a eles mais do que tudo.

Acredito que os filhos *pets* também mereçam reconhecimento. À Frida, à Pikachu, à Maria e ao Antônio por transmitirem amor e carinho mais que muitos humanos. Com certeza, foram um suporte emocional inesperado. Só posso torcer que eu esteja sendo um pai à altura.

À minha banca examinadora – em especial, ao orientador Prof. D.r William Paiva Marques Júnior –, cujos componentes merecem um espaço à parte para expressar minha gratidão com a devida dimensão. Minhas palavras sinceras estão presentes nos agradecimentos, onde reservei um lugar especial para elas.

Por último, mas definitivamente não menos importante, dedico este trabalho a todos os meus amigos. Descrever a relevância e o impacto de cada um na minha vida é uma ação impossível para esta dedicatória, visto que apenas abordaria uma parcela ínfima dessa influência e, por conseguinte, não faria jus ao significado de ninguém de maneira fidedigna. Afinal, os amigos são uma segunda família, e uma que você escolheu. Apesar disso, considero essencial escrever algumas palavras a fim de cravejar de joias este manuscrito bruto, da mesma forma que estas adornam e dão valor aos mais simples dos trabalhos humanos.

Começar do início, por mais pleonástico que seja, parece ser o melhor caminho a seguir e me parece um emprego legítimo nesse caso. Então, nada mais justo que recordar do Ensino Médio – ou, em outras palavras, dos amigos mais antigos que ainda mantenho contato e que me ensinaram o significado desse conceito de amizade prolongada, o que não é pouco. Não à toa, sempre há a vontade de não sair de certos grupos e reencontrar determinadas pessoas.

Na trajetória escolar, não tenho como raspar da memória a mentoria de Lorena Almeida, Stéffany Barbosa, Sarah Capelo, Letícia Medina e Isabel Gurjão. Essas pessoas cunharam a união de uma turma inteira e me fizeram sentir bem-vindo em um contexto institucional novo e desafiador e, assim, não querer desistir. Os estudos ao som de Amy Winehouse e Kate Bush são inesquecíveis.

Na mesma conjuntura, o Assemble surgiu, talvez com menos força que agora, mas cujas interações e receptividade também foram essenciais, à época, para me sentir seguro e chegar aonde estou. Aimée Berdine, Raquel Ferreira e Clara Menezes fizeram parte dessa história primeiro, para depois serem acompanhadas de Raissa Moraes e Luiza Soares – ou seria

Luisa? Uma verdadeira turma olímpica que nunca me deixou ser um ex do grupo. Muito obrigado!

Chegando ao fim dos grupos de Ensino Médio, ocupa também um espaço especial no meu coração o Bagaço da Laranja, que conta com Larissa Dornelles, Ana Flávia, Eduardo Austregésilo e Juliane Colares, além de reprisar os papéis de Lorena, Raissa e Stéffany. Meus ânimos sempre se levantaram em qualquer conversa ou situação quando éramos um grupo, e – em tempos de choro ou em tempos de riso – se tornaram uma âncora, impedindo-me de ficar à deriva (levado através do mar além-porto ou das dunas). Não tenho como retribuir o conforto e a segurança que me foram assegurados por tanto tempo. Espero que seja uma amizade que perdure por um período muito maior do que já vivenciamos e, quem sabe, tudo não seja só um “pré” de um auge que está por vir.

Não tão conectada a esses grupos, encontrei também uma amiga para toda hora, a Julia Sampaio, que fez parte de importantes momentos da minha vida. Teve que aturar minhas mudanças de humor e minhas chatices, mas nunca deixou de me tratar com carinho e cuidado pelos longos anos de pré-vestibulares. Além disso, apesar de a distância ter crescido entre nós, acabamos seguindo o mesmo caminho, e era um prazer revê-la pelos corredores da faculdade. Mal posso esperar para reencontrá-la na profissão – talvez não como parte contrária, contudo, porque é difícil competir com tamanha inteligência e afinco.

A faculdade, então, completou minha vida com mais pessoas inimagináveis. Nas salas de aula, fui agraciado com as pérolas Jeniffer Castro e Liliana Barboza, que tornaram muito mais palatáveis a sequência de aulas e atividades. Suavizaram o conceito de obrigatoriedade com maestria, sendo uma motivação para enfrentar o cotidiano universitário quando o Sol mal tinha irrompido no horizonte. Jeniffer, por sinal, pela dificuldade de aceitar uma saída presencial, fez questão de permanecer em contato virtualmente. Como sempre, tento prometer me atentar às redes sociais mais para respondê-la como ela merece (foco no tentar). Contudo, possuo fé até hoje que ela vai aparecer cara a cara mais vezes.

Ainda, as trajetórias pelos projetos de extensão – em especial, a Simulação da Organização das Nações Unidas e o Curso Pré-Vestibular Paulo Freire – marcaram-me não só pelas vivências e experiências, mas pelos colegas com que compartilhei esses momentos. Tanto é verdade que, até hoje, não consigo me distanciar d’Os Jovens: Gabriela Maria, Jéssica Dias, Júlia Cavalcante, Júlia Fé, Lucas e Nasla Gomes. Minha janela sempre estará aberta para eles, mesmo com os apagões que surjam, e não é *fake news*! Ainda que fiquem a quilômetros de distância, ou em um mundinho próprio na cabeça, sei que eles passam a tranquilidade de que

todos estão “logo ali” uns para os outros. Muitas histórias com pouco tempo; espero que novas aventuras venham para as risadas retornarem tanto quanto for possível.

Menção honrosa em todo esse caminho acadêmico também para quem aparecia recorrentemente, em diversos momentos, para abrilhantar esse percurso da universidade: Carol Farias, Laura Beserra, Mariana Aragão e Débora Alves. Em cada aparecimento e presença de vocês, na ocasião que fosse, meu coração se acalentava.

Como disse, as palavras – embora possuam um poder invejável – ainda não conseguem expressar com a exatidão necessária determinados sentimentos. Todavia, se elas transmitirem uma parcela deles e se ficou clara a contribuição de cada um no trajeto até desembocar nesta monografia, então creio que a presente dedicatória atingiu seu objetivo.

Se comecei com um pleonasmo, acredito que eu tenha licença de finalizar, assim, com mais uma estrutura não muito desejável em uma escrita – dessa vez, o clichê: que tudo de bom, sobretudo a felicidade, chegue a cada pessoa aqui mencionada. Muitos beijos e abraços!

## AGRADECIMENTOS

Em primeiro lugar, agradeço ao Prof. D.r William Paiva Marques Júnior, o orientador deste trabalho. Seu conhecimento transcende diversas áreas do Direito, tanto que suas produções constantes refletem essa qualidade, bem como demonstram seu peso e sua importância como ávido pesquisador e, conseqüentemente, como orientador. Ainda assim, como já lhe mencionei, a despeito de sua orientação ser excepcional e não merecer quaisquer deméritos, seu apoio, incentivo e sensibilidade diante das dificuldades relacionadas ou não com o desenvolvimento deste trabalho foram os fatores mais importantes para mim ao longo dessa trajetória. Sem eles, não sei se teria a energia e a vontade para seguir adiante com a presente produção acadêmica. Por essa razão, registro essa gratidão por escrito para ser eternizada, ao passo que seus conselhos estão guardados na memória.

Esta obra tampouco seria possível sem a Prof.<sup>a</sup> M.<sup>a</sup> Fernanda Cláudia Araújo da Silva. Além de seus gratos elogios e pertinentes comentários, mostrando sua sagacidade enquanto docente e acadêmica, é uma incrível pessoa, com uma disponibilidade e abertura aos discentes pouco vista em profissionais de hoje. Tanto como examinadora quanto como coordenadora, seu jeito de ser deixou mais leve minha passagem pela universidade.

Por fim, o mestrando Lucas Salles Gazeta Vieira Fernandes colaborou com esta produção aos poucos, desde o meu primeiro contato com ele na Simulação da Organização das Nações Unidas, um projeto de extensão de Direito Internacional. Seja por meio das discussões incutidas pelas experiências e vivências proporcionadas pelo projeto, seja mediante o incentivo e o apoio para tratar do assunto apesar de todas as dificuldades apresentadas pela vida, ele se tornou uma constante que seguiu o caminho do Direito Internacional e que, dessa forma, pôde me coroar com uma brilhante participação na banca.

Sendo assim, reforço meu sincero obrigado a todos os três.



## RESUMO

O Direito Internacional Humanitário salvaguarda, sobretudo, a dignidade da pessoa humana nos contextos de guerra, em que diversos direitos humanos são relativizados. Para isso, estabeleceu uma série de princípios com o objetivo de resguardar os não combatentes e mesmo os combatentes, quando fora de combate. Contudo, uma nova frente de combate surgiu com o advento e o aprimoramento da internet: o campo de batalha cibernético. Este trabalho visa a compreender a aplicação do Direito Internacional Humanitário em face do contexto atual de ciberataques, incentivados ou patrocinados por Estados em um esforço de guerra. A pesquisa possui natureza qualitativa e finalidade exploratória, além de se utilizar de uma metodologia de análise bibliográfica. Observa-se que as ofensivas virtuais ocorrem, em especial, por meio de derrubada de servidores e provedores de internet, bem como mediante a apropriação de dados e dinheiro. Esses ataques configuram constantes desrespeitos a princípios estabelecidos pelos diversos tratados internacionais humanitários, causando, sobretudo, a desvalorização da dignidade da pessoa humana, ao contrário do objetivo dos tratados em vigor, que é valorizá-la. Tendo em mente as principais consequências negativas provenientes desse novo âmbito de confronto, verifica-se a desatualização das normas humanitárias, que ficaram mais obscuras com a criação de novas tecnologias. Além disso, quando a legislação internacional consegue demonstrar um entendimento mais claro e assertivo, constata-se o desinteresse de vários países em se alinhar à proteção da dignidade e, como consequência, realizar ataques ou tolerá-los sem se atinar a qualquer limitação a que esteja submetido. Portanto, a fim de maximizar o valor do ser humano e da vida básica a que ele tem direito, defende-se que é essencial discussões de atualização, principalmente por meio das Nações Unidas, de novas diretrizes do Direito Internacional Humanitário, de modo a esclarecer quais são os entendimentos, as interpretações e as aplicações possíveis para o caso de guerra virtual. Ademais, nas questões mais incontroversas, urge-se o aumento de pressões – sejam políticas, sejam econômicas – para que os ciberataques indiscriminados cessem, adaptando-os às restrições previstas pelo ordenamento jurídico internacional em vigor.

**Palavras-chave:** Direito Internacional Humanitário; guerras virtuais; ciberataques; internet.

## ABSTRACT

International Humanitarian Law safeguards, above all, the human dignity in contexts of war, in which various human rights are relativized. To this end, it established a series of principles with the aim of protecting non-combatants, and even combatants when out of combat. However, a new front has emerged with the advent and improvement of the internet: the cyber battlefield. This work seeks to understand the application of International Humanitarian Law in light of the current context of cyberattacks, encouraged or sponsored by States in a war effort. The research has a qualitative nature and exploratory purpose, in addition to using a methodology of bibliographic analysis. It is observed that virtual offensives occur, in particular, putting servers and internet providers offline, as well as through the appropriation of data and money. These attacks constitute constant disrespect for the principles established by the various international humanitarian treaties, specially causing the devaluation of the human dignity, contrary to the objective of the treaties in force, which is to value it instead. Bearing in mind the main negative consequences arising from this new context of confrontation, it can be seen that humanitarian norms are outdated, which have become more obscure with the creation of new technologies. In addition, when international legislation manages to demonstrate a clearer and more assertive understanding, several countries are not interested in aligning themselves with the protection of dignity and, as consequence, carry out attacks or tolerate them without reaching any limitation that they are submitted to. Therefore, in order to maximize the value of the human being and the basic life to which he is entitled, it is essential to update discussions, mainly through the United Nations, of new guidelines of International Humanitarian Law, in order to clarify what are the understandings, interpretations and possible applications in cases of cyber warfare. Furthermore, on the most uncontroversial issues, there is an urgent need to increase pressure – whether political or economic – so that indiscriminate cyberattacks cease, adapting them to the restrictions provided for by the international legal system in force.

**Keywords:** International Humanitarian Law; cyber warfare; cyberattacks; internet.

## LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
Art.	Artigo
CIA	Agência Central de Inteligência dos Estados Unidos
CICV	Comitê Internacional da Cruz Vermelha
CIJ	Corte Internacional de Justiça
CISA	Agência de Cibersegurança e Infraestrutura de Segurança dos Estados Unidos
CONPEDI	Conselho Nacional de Pesquisa e Pós-Graduação em Direito
CSIS	Centro de Estudos Estratégicos e Internacionais
CSRC	Centro de Recurso de Segurança para Computador dos Estados Unidos
D.r	Doutor
DDoS	Negativa de Serviço Distribuída
DIH	Direito Internacional Humanitário
EUA	Estados Unidos da América
FUNAG	Fundação Alexandre de Gusmão
ICCO	Organização de Cultura e Comunicação Islâmica do Irã
ICJ	Corte Internacional de Justiça
IPRI	Instituto de Pesquisa de Relações Internacionais
MI-5	Serviço de Segurança do Reino Unido
NFT	<i>Tokens</i> não fungíveis
NSA	Agência Nacional de Segurança dos Estados Unidos
OFAC	Escritório de Controle de Ativos Estrangeiros dos Estados Unidos
OHCHR	Escritório do Alto Comissário sobre Direitos Humanos das Nações Unidas
OMPI	Organização Mundial da Propriedade Intelectual
ONU	Organização das Nações Unidas
OPCW	Organização para a Proibição de Armas Químicas
Prof.	Professor
TI	Tecnologia da Informação
UnB	Universidade de Brasília
UNESCO	Organização das Nações Unidas para Educação, Ciência e Cultura

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO.....</b>	<b>11</b>
<b>2</b>	<b>AS BASES DO DIREITO HUMANITÁRIO INTERNACIONAL.....</b>	<b>14</b>
<b>2.1</b>	<b>A aparente contradição da dignidade da pessoa humana aplicada aos contextos de guerra.....</b>	<b>16</b>
<b>2.2</b>	<b>O princípio da distinção (combatentes e não combatentes).....</b>	<b>18</b>
<b>2.3</b>	<b>A proteção especial a determinadas pessoas e propriedades.....</b>	<b>19</b>
<b>2.4</b>	<b>A vedação a métodos de guerra cruéis e desproporcionais.....</b>	<b>20</b>
<b>2.5</b>	<b>A boa-fé como corolário dos comportamentos e das estratégias de batalha .....</b>	<b>25</b>
<b>3</b>	<b>A GUERRA VIRTUAL: PRÁTICAS E ESTRATÉGIAS NO CAMPO DE BATALHA CIBERNÉTICO E SEUS IMPACTOS.....</b>	<b>27</b>
<b>3.1</b>	<b>A caracterização dos ataques virtuais como componentes da guerra .....</b>	<b>29</b>
<b>3.2</b>	<b>A derrubada de servidores-chave para a estrutura nacional .....</b>	<b>31</b>
<b>3.3</b>	<b>A apropriação de dados críticos e estruturais dos países.....</b>	<b>33</b>
<b>3.4</b>	<b>A apropriação de dinheiro em prol das Forças Armadas e da guerra .....</b>	<b>35</b>
<b>4</b>	<b>O DIREITO INTERNACIONAL HUMANITÁRIO DIANTE DE CIBERATAQUES NAS GUERRAS VIRTUAIS .....</b>	<b>40</b>
<b>4.1</b>	<b>Há direito humano à internet em tempos de guerra? .....</b>	<b>41</b>
<b>4.2</b>	<b>A inexistência de alvos bem definidos e delimitados nas investidas virtuais.....</b>	<b>44</b>
<b>4.3</b>	<b>A indefinição de combatente no âmbito virtual .....</b>	<b>47</b>
<b>4.4</b>	<b>A predominância da má-fé nas ofensivas bélicas <i>on-line</i> .....</b>	<b>49</b>
<b>5</b>	<b>CONSIDERAÇÕES FINAIS .....</b>	<b>51</b>
	<b>REFERÊNCIAS .....</b>	<b>55</b>

## 1 INTRODUÇÃO

Hoje em dia, o acesso à internet é essencial a uma parcela da população global e, ainda que exista uma importante quantidade de pessoas marginalizadas do desenvolvimento tecnológico, o número de indivíduos conectados só tende a aumentar. Muito provavelmente, a leitura deste trabalho ocorrerá por métodos digitais, por meio de dispositivos que se interligam ao ciberespaço, assim como ele também foi produzido virtualmente.

Dentro de um contexto em que há uma realidade cibernética desenvolvida e que, inclusive, se imiscui no mundo físico, as problemáticas surgidas no ambiente digital têm cada vez mais importância e impacto. Muito se vislumbra, ainda, as consequências dos momentos iniciais da internet, nos quais ela se desenvolveu à margem da lei, sem uma governança estatal para aplicar políticas públicas ao ciberespaço, a despeito de ele possibilitar diversos mecanismos positivos à sociedade.

Um desses efeitos se cristalizou como a falta de segurança, dadas as brechas presentes em um sistema de criação humana que permanece evoluindo. Mesmo depois de diversas atualizações, a rede mundial de computadores se tornou mais um meio de cometimento de crimes, em uma espécie de espelhamento das problemáticas encontradas na realidade material. Embora alguns *hackers* utilizem o conhecimento para objetivos benéficos, ajudando a construir uma internet melhor, outros aproveitam o anonimato e a globalização decorrentes da revolução comunicacional para realizar investidas nacionais e internacionais.

Essa estrutura vem sendo usada com vistas a não apenas atacar virtualmente particulares em face de intenções individuais, mas também a praticar ofensivas patrocinadas por Estados ou grupos paraestatais. O maior exemplo disso se viu com o irrompimento, em 2022, da guerra entre Rússia e Ucrânia. Já no início, a Ucrânia convocava voluntários, cidadãos ucranianos ou não, com o intento de distribuir tarefas a fim de atacar os sistemas russos (UCRÂNIA..., 2022a, *on-line*), enquanto, do lado da Rússia, *hackers* governamentais desafiavam a cibersegurança de Kiev e de outros países europeus ao provocar quedas de mecanismos *on-line* de políticas públicas e até do acesso geral à internet (UCRÂNIA..., 2022b, *on-line*). Em outras palavras, na prática, de modo evidente, definia-se uma frente de guerra cibernética.

Devido aos prejuízos generalizados, com a aparente inexistência de alvos militares delineados, essas constatações práticas levam a questionamentos teóricos a respeito da aplicação das normas de Direito Internacional Humanitário, cujo desrespeito às variadas determinações tratadas por esse ramo do Direito transparece durante a observação *a priori* das

condutas mencionadas. Afinal, já são bastante definidas e difundidas as proteções destinadas a diversos públicos, como civis, mesmo que o DIH conviva diariamente com variados problemas na sua execução (CICV, [2022]c, *on-line*).

A perspectiva futura, inclusive, antevê a continuação das atualizações tecnológicas e o aprofundamento da incorporação das relações sociais no ciberespaço. Porém, em vez de ser apenas um complemento à parte da realidade material – ou seja, um instrumento que aprimora o mundo físico, embora permaneça em um campo separado deste –, os prognósticos indicam a transformação do espaço cibernético em um metaverso. Neste, a realidade será duplicada, permitindo vivências semelhantes ao ambiente material sem sair do local físico (MACHADO, S., 2022, *on-line*). Além disso, a realidade estará completamente interconectada com a rede mundial de computadores, consoante se desenvolve a Internet das Coisas (ORACLE, [2022], *on-line*).

Tendo em vista a identificação da problemática citada, propõe-se o presente trabalho, de natureza qualitativa, com fins exploratórios e baseado em um método de pesquisa bibliográfico. Em primeiro lugar, a vertente qualitativa advém das análises e das percepções subjetivas decorrentes da realidade e da leitura de documentos. Em segundo lugar, a finalidade exploratória resulta da necessidade de obtenção, ao final, de uma visão geral dos comportamentos adotados pelos Estados diante do surgimento de um novo estilo de guerra e da maneira como se adaptaram em meio às normas já existentes, mas pensadas para o espaço material. Por último, o aspecto documental se deve à pesquisa se basear em conceitos de doutrinas literárias, periódicos e tratados internacionais de DIH, além da observação de fatos presentes nas narrativas jornalísticas mundiais.

Nesse sentido, no segundo capítulo, pós-introdução, o estudo se concentra na análise dos tratados internacionais humanitários e do direito consuetudinário que os estabeleceram, em especial as *Convenções de Genebra* e seus protocolos adicionais. Com a leitura da documentação legal e internacional vigente e com as considerações de estudiosos a respeito dos costumes de guerra, busca-se determinar os princípios e a base lógica que guiam a aplicação e a interpretação desse ordenamento.

Em seguida, no terceiro capítulo, adentram-se os ciberataques mais comuns, de modo a verificar a possibilidade de intervenção do DIH nesses casos e as práticas adotadas com maior recorrência pelos atacantes. Para isso, foi levada em consideração a quantidade de cada tipo de incidente cibernético, calculada com base tanto nos eventos noticiados e elencados por meio da busca em motores de pesquisa da internet quanto no relatório elaborado pelo Centro de Estudos Estratégicos e Internacionais (CSIS, da sigla em inglês). O capítulo foi dividido de

acordo com cada ofensiva rotineira identificada. Adotou-se, nessa parte, um viés mais descritivo, tendo em vista a importância de se considerar como cada ciberataque funciona para problematizar os respectivos comportamentos.

Por fim, no quarto capítulo, o último antes das considerações finais, continua-se a destrinchar as investidas digitais do terceiro capítulo, mas, nessa ocasião, abordando as problemáticas que elas causam na atualidade. Isso porque, após o detalhamento de cada ofensiva cibernética, chega-se às principais adversidades que acometem o contexto da frente de batalha virtual, com um tópico do capítulo destinado a cada obstáculo. Com isso, objetiva-se ponderar como aplicar as normas do DIH, de maneira a respeitar ao máximo os princípios por ele emanados nos contextos previstos pela legislação internacional.

Este trabalho visa a uma pesquisa mais pura, pois se vislumbra, ao final, a apresentação teórica dos problemas de aplicação, diante das condutas executadas na atualidade, relacionados com os dispositivos do ramo humanitário do Direito. Contudo, não se exige de elencar algumas sugestões de possíveis interpretações, além de eventuais ações a serem tomadas pelos atores globais para aumentar ou garantir, de fato, as proteções acordadas, o que acaba tendendo um pouco o trabalho à parte mais aplicada da pesquisa.

## 2 AS BASES DO DIREITO HUMANITÁRIO INTERNACIONAL

Pode-se dizer que o Direito Internacional Humanitário teve como marco o estabelecimento dos Direitos Humanos, notadamente com a *Declaração universal de Direitos Humanos* de 1948. No entanto, vale notar que diversas normas precedentes já explicitavam valores afins por meio do direito consuetudinário (RAMOS, 2017, *e-book*). Aliás, as raízes se remontam à Antiguidade e é tão antiga quanto a própria História – na *Bíblia*, inclusive, com a igualdade em relação a outros homens e mulheres e com a imagem de semelhança com Deus (MARQUES JÚNIOR, 2017, p. 31-32).

Considerando o contexto da Modernidade, trata-se de mais um mecanismo de limitação à atuação estatal, que já vinha ocorrendo desde os primórdios do capitalismo moderno, de modo que o Estado não intervisse na liberdade dos indivíduos. Afinal, para um efetivo funcionamento do sistema econômico vigente, as trocas proporcionadas deveriam ser livres, equivalentes e, na medida do possível, ilimitadas, fortalecendo os valores de igualdade e liberdade, ainda atuantes na realidade contemporânea. Não à toa, a *Declaração universal de Direitos Humanos* se centrou nesses princípios, ao mesmo tempo que Karl Marx criticava esses valores por se associarem justamente ao sistema econômico capitalista moderno (GOMES, 2018, p. 124-135).

Assim, dessa crescente tendência da redução da arbitrariedade estatal, somada aos horrores vislumbrados durante a ascensão de regimes autoritários pós-Primeira Guerra Mundial – sobretudo as práticas nazistas –, adveio a criação do Direito Internacional dos Direitos Humanos e do DIH. Tais ramos são intrínsecos à sociedade internacional que surgiu após a Segunda Guerra Mundial e se estabelecem mediante tratados, separando-se das normas consuetudinárias anteriores às Grandes Guerras em razão dessas características (RAMOS, 2017, *e-book*).

O conceito por trás da principal vertente humanitária é, em resumo, definir que até guerras possuem barreiras intransponíveis (CICV, 2022b, *on-line*). Em prefácio, o então presidente da Cruz Vermelha, Jakob Kellenberger, afirma que as demandas das civilizações – e a essência delas, portanto – é justamente restringir a violência, tanto que diversas normas foram criadas com o passar do tempo para atingir tal redução (HENCKAERTS; DOSWALD-BECK, [2017], p. 9-11). Ao analisar por essa ótica, percebe-se uma vertente valorativa mais moralista, pautada igualmente na ética, como fonte de justificação dos Direitos Humanos e, de modo tangente, do DIH. Entretanto, a construção histórica revela uma corrente que se inclina



para uma fundamentação jusnaturalista, com base, portanto, no Direito Natural (MARQUES JÚNIOR, 2017, p. 33).

Como parâmetro para essa limitação, o DIH se alicerça basicamente na salvaguarda da dignidade e do respeito à pessoa humana, desembocando no artigo que é comum às quatro *Convenções de Genebra*, o art. 3º. Embora o espírito da proteção à humanidade esteja presente ao longo de todos os documentos, tal disposição o resume e o evidencia ao asseverar, em parte de seu conteúdo:

Em caso de conflito armado de caráter não internacional que ocorra em território de uma das Altas Partes Contratantes, cada uma das Partes em conflito deverá aplicar, pelo menos, as seguintes disposições:

1) As pessoas que não participarem diretamente do conflito, incluindo membros das forças armadas que tenham deposto as armas e pessoas que tenham sido postas fora de combate por enfermidade, ferimento, detenção ou qualquer outra razão, devem **em todas as circunstâncias ser tratadas com humanidade, sem qualquer discriminação desfavorável** baseada em raça, cor, religião ou crença, sexo, nascimento ou fortuna, ou qualquer outro critério análogo.

Para esse efeito, são e permanecem proibidos, sempre e em toda parte, em relação às pessoas acima mencionadas:

- a) os atentados à vida e à integridade física, em particular o homicídio sob todas as formas, as mutilações, os tratamentos cruéis, torturas e suplícios;
- b) as tomadas de reféns;
- c) as ofensas à dignidade das pessoas, especialmente os tratamentos humilhantes e degradantes;**
- d) as condenações proferidas e as execuções efetuadas sem julgamento prévio por um tribunal regularmente constituído, que ofereça todas as garantias judiciais reconhecidas como indispensáveis pelos povos civilizados. [...] (CICV, 2019, p. 37, 38, 65, 66, 87, 88, 159 e 160, grifou-se)

Isto é, a repetição do dispositivo e a sua extensa aplicação esclarecem, sem sobre de dúvidas, o intuito de alçar esse princípio à condição de basilar e imprescindível durante qualquer período, seja em tempos de paz, seja em tempos de guerra. Não obstante essa consideração isolada, trata-se de objetivo extraído de toda a conjuntura dos textos, fixando-o por meio de diversos processos interpretativos, a exemplo do lógico e do sistemático, inclusive utilizando o elemento teleológico na exegese, de acordo com os ensinamentos de Carlos Maximiliano (2021, *e-book*).

## 2.1 A aparente contradição da dignidade da pessoa humana aplicada aos contextos de guerra

Em um primeiro momento, aparenta ser contraditório indicar que a dignidade da pessoa humana e o respeito a ela sejam questões centrais em tratados concernentes a conflitos, afinal vários direitos inerentes a tais valores são relativizados – para dizer o mínimo – nas situações de beligerância, mesmo nos textos legais que impõem várias restrições às atividades de guerra. Entretanto, é uma contradição aparente, a qual transparece a complexidade da sociedade e das relações humanas: elas raramente apresentam uma situação clara, separadas no espectro preto e branco de maneira apartada; assemelham-se mais com uma área cinzenta, de múltiplos entendimentos.

Embora a definição e o conteúdo normativo em si da dignidade da pessoa humana ainda registrem amplo dissenso entre doutrinadores e juristas, até porque a aplicação desse princípio é bastante inconsistente e muitas vezes frágil entre ordens constitucionais e legais dos vários países do globo, passou-se a identificar um forte vínculo entre a dignidade da pessoa humana e os direitos fundamentais das nações, incluindo no Brasil (SARLET; MARINONI; MITIDIERO, 2022, *e-book*). Expressando a concepção de Ricardo Soares (2019, *e-book*), o princípio da dignidade da pessoa humana é um âmbito tanto físico quanto moral a ser garantido a todos os seres humanos, sem distinção, apenas por existirem no mundo, independentemente de suas atitudes – se valorosas ou se temerosas –, possuindo associação com liberdade, valores espirituais, subsistência, valorização do trabalho, livre-iniciativa, igualdade, impedimento a degradar ou reificar o indivíduo, bem como todas as condições materiais referentes e necessárias a essas deferências.

Como exposto, o raciocínio que advém dessa lógica é que os direitos à vida e à liberdade, por exemplo, acabam tornando-se indissociáveis à garantia de uma vida digna aos indivíduos. Nesse sentido, a sensação de contradição em situações calamitosas de combate aparece justamente quando se tem à proteção ao direito à vida como essência geral do Direito Internacional, mas o qual é deixado de lado diante dos bombardeios e da morte de soldados inimigos, sendo uma situação reconhecida e, de certa forma, permitida pelo Direito Humanitário. Outra exemplificação aparece no direito à liberdade, em que surgem os prisioneiros de guerra, bem como diversas restrições de locomoção proporcionadas pelas Forças Armadas.

Vislumbra-se, então, que esse aparente contrassenso não chega a ser efetivamente uma novidade em ordenamentos jurídicos. No próprio Brasil, por exemplo, mesmo direitos

ressalvados pela Constituição e possuidores de *status* de fundamentais<sup>1</sup> são passíveis de limitação ou restrição, como asseveram Gilmar Mendes e Paulo Branco (2022, *e-book*). Nota-se que o Texto Constitucional de 1988 possibilita essa contenção em estados de defesa e de sítio, assim como em tempos de guerra, diante dos quais até a pena de morte pode ser estabelecida, apesar do direito à vida. Aliás, mesmo em tempos de paz e de ausência de outras excepcionalidades, a liberdade pode ser retirada em casos de crimes, mostrando que essa relativização, na verdade, é comum no dia a dia.

Portanto, os princípios de dignidade e de respeito humanos são adotados atualmente de acordo com a possibilidade, como se verifica nas normas vigentes acordadas entre os países. Essa é uma construção deveras moderna, visto que outrora as leis e os costumes da guerra eram estabelecidos por outros valores, bem como eram aplicados de forma inconstante, adequando-se a determinados inimigos e variando conforme a região.

Não obstante, pode-se indicar traços comuns, ainda que irregulares, a começar pelo apreço à honra do soldado. Os comportamentos ao longo do conflito deveriam evitar práticas consideradas cruéis e desonrosas que recairiam sobre os combatentes e manchariam a sua reputação. A caracterização de que condutas seriam imorais ou a indicação dos indivíduos contra os quais eram permitidas essas práticas eram definidas por vezes pelo exército e por vezes pela religião (CICV, [2022]c, *on-line*).

A evolução até os ditames humanitários contemporâneos, assim como diversos institutos correntes, passou por todo um processo histórico, inclusive por oscilações de ordem semântica. A polissemia da expressão, a qual lhe incumbia diferentes significados a depender do contexto histórico e cultural, permitiu a confusão da dignidade da pessoa humana com a evolução dos direitos humanos, por exemplo (SOARES, 2019, *e-book*). Com isso, a aplicação inconstante deu lugar à regularidade, e princípios começaram a aparecer, de maneira frequente e uniforme, ao redor do globo. Tendo isso em vista, aconteceu a adoção e a recepção de diversas ideias do direito consuetudinário dos conflitos por tribunais de guerra no período após 1945, que, inclusive, chegaram a inspirar a estrutura das *Convenções de Genebra* e documentos normativos afins, como as *Convenções e declarações de Haia* (CICV, [2022]c, *on-line*).

---

<sup>1</sup> Gilmar Mendes e Paulo Branco (2022, *e-book*) também afirmam que entram nesse bojo não só direitos, mas também liberdades, poderes e garantias, evidenciando a amplitude a que tal refreamento pode chegar, caso necessário e adequado ao contexto previsto para cada situação.

## 2.2 O princípio da distinção (combatentes e não combatentes)

Outro dos princípios basilares que busca organizar a guerra é a distinção entre combatentes e não combatentes, sobretudo os civis. A lógica por trás dessa norma emana do entendimento de que o meio de se ganhar a guerra é exaurir as forças militares do inimigo, não existindo interesse em englobar as destruições para os demais integrantes e as estruturas restantes do território. A ocupação, sem a resistência oficial armada, é iminente, e qualquer ataque se torna despropositado e desproporcional. Em decorrência disso, atacar ou bombardear ocupações indefesas já era uma conduta a ser evitada pelas forças conflitantes, por exemplo (CICV, [2022]c, *on-line*). Lembre-se de que, a despeito de não envolver direito à vida propriamente dito, a conservação de edificações e ambientes naturais reflete uma garantia às futuras gerações de utilizar os patrimônios por vezes inestimáveis e insubstituíveis, exprimindo um empobrecimento do povo a quem esse patrimônio pertence e da humanidade como um todo (UNESCO, 2021, p. 10-11).

Apesar de os governos chegarem à conclusão de que não combatentes e até estruturas desarmadas e não militares não devam ser atacados diretamente, definir combatentes não é uma tarefa fácil, mesmo porque esse termo se diferencia dos participantes das movimentações bélicas, sendo aquele um grupo ainda mais específico deste. É certo que todos os membros das Forças Armadas institucionais – com exceção do pessoal religioso ou sanitário, ainda que seja ligado a tais unidades e seja participante da guerra por causa disso – são considerados combatentes para os fins do DIH (CICV, [2022]e, *on-line*). Contudo, é perceptível que se trata de uma noção de um extremo mais claro da realidade.

Pessoas que possuam armas, alheias à vinculação ou às determinações das forças governamentais, já entram em um espectro mais obscuro e dependem da conceituação adotada por cada um para serem caracterizadas. No entanto, o DIH, de acordo com os tratados vigentes mais recentes, entende que nenhum indivíduo fora da organização das Forças Armadas ou de outros grupos paramilitares com organização e subordinação que não adentre as hostilidades pode ser englobado no grupo dos combatentes; ainda assim, se porventura alguém com essas características se inserir na guerra, só deve ser assim considerado enquanto durar sua participação, retornando à condição de não combatente tão logo cesse a perpetração das atividades bélicas (CICV, [2022]e, *on-line*).

Aliás, o dever das partes hostis extrapola a necessidade de se abster de ataques diretos: deve-se igualmente proteger os habitantes das áreas sob seu controle, na medida do possível, quando se souber que eles estão perto de objetivos militares, sobretudo os locais

sensíveis e essenciais à parte inimiga. Então, evacuações e realocações de estrutura militar são obrigações sempre que as condições permitirem (CICV, [2022]d, *on-line*).

Depreende-se de todas essas informações que se buscou preservar o direito à vida ao máximo<sup>2</sup>. Trata-se de um acerto evidente, não só pelo respeito à dignidade da pessoa humana. Afinal, a escolha de alvos, de forma indistinta, tanto afetaria eventualmente pessoas contrárias à beligerância quanto possibilitaria práticas de quase genocídio em casos extremos, ao se exterminar determinadas populações regionais. Era isso o que acontecia, por exemplo, na Roma Antiga, em que os enfrentamentos se puseram contra a população inteira das cidades inimigas, não só os soldados: além da morte das pessoas, havia o extermínio da natureza ao redor, dos animais e das estruturas de produção de alimentos. Conforme conta Numa-Denys Fustel de Coulanges (2021, *e-book*), “[...] uma guerra podia fazer desaparecer de um só golpe o nome e a raça de todo um povo, e transformar uma região fértil em deserto”.

### **2.3 A proteção especial a determinadas pessoas e propriedades**

Dentre os integrantes das Forças Armadas e da sociedade civil, as pessoas relacionadas com as atividades médicas, sanitárias, religiosas e humanitárias – incluindo nesse âmbito também as propriedades e os deslocamentos imprescindíveis para o desempenho de tal pessoal – foram reconhecidas para receber uma proteção ainda superior dos embates bélicos<sup>3</sup>. Esse amparo ocorre em razão do papel desses grupos, que atuam para socorrer e acolher indivíduos que se encontram em condições bastante precárias, além de cuidar dos mortos. A explicação advém da lógica de que não só a atuação deles são importantes para manter a dignidade de todos, como também correm mais riscos – apesar da proteção – por, às vezes, estarem próximos das batalhas, a exemplo de quando necessitam recolher e cuidar dos corpos das vítimas (CICV, 2016, *passim*).

O princípio da distinção, de certa maneira, já traz em sua essência a ideia de que algumas pessoas devem possuir um tratamento mais privilegiado que outras. Nesse caso, os não combatentes têm direitos superiores aos combatentes, já que mesmo os sistemas das forças em

---

<sup>2</sup> Embora saia um pouco do escopo deste trabalho, é válido ressaltar que, por esse mesmo motivo, se aplicam proteções especiais para os mortos e para os indivíduos que se voluntariam a ajudar doentes e enfermos, mesmo que não pertençam às organizações de socorro ou às potências protetoras, não se enquadrando como combatentes ainda que, desse modo, acabem participando do conflito. Não à toa, tem-se cuidado também com estabelecimentos hospitalares e sanitários (CICV, 2016, *passim*).

<sup>3</sup> À semelhança dos voluntários que ajudam enfermos e doentes, ainda que não estejam vinculados a organizações de socorro, o pessoal humanitário não é considerado combatente, embora se caracterize como partícipe do conflito. Isso ocorre mesmo se médicos, capelães e afins sejam membros das Forças Armadas, por exemplo.

conflito, em tese, trabalham para que aqueles não sofram os efeitos diretos da guerra, diferentemente destes. No entanto, o princípio das pessoas especialmente protegidas trabalha com uma preservação ainda maior.

Baseando-se na leitura dos tratados de DIH, note-se que os civis, em resumo, são protegidos, mas estão sujeitos a eventuais agressões e casualidades devido a interesses e objetivos militares justificáveis e proporcionais. Isso acontece sobretudo quando o alvo militar é atacado com mecanismos condizentes com seu porte e sem a antecipação da potência que defende o território, impossibilitando a evacuação ou realizando a defesa de modo ineficaz.

Por outro lado, as pessoas e os bens especialmente protegidos gozam de uma zona própria livre de ataques de qualquer tipo, embora esse direito os acompanhe até fora dela. É claro que existe uma série de requisitos a fim de que uma área, um conjunto de pessoas ou uma variedade de carregamentos sejam, enfim, reconhecidos como assegurados. Todavia, após estabelecida sua identificação, suas necessidades devem ser atendidas sempre que possível por quem detenha a responsabilidade factual pelo território, com poucas exceções que podem restringir a atuação desses socorros humanitários (CICV, 2016, *passim*).

#### **2.4 A vedação a métodos de guerra cruéis e desproporcionais**

Uma vez estabelecidos as pessoas e os objetos que não estão fora de combate, ou seja, passíveis de ser submetidos aos confrontos e, conseqüentemente, ser alvos das Forças Armadas e organizações afins de Estados em guerra, chega-se à seguinte pergunta: então, ao longo dos combates, toda e qualquer conduta pode ser aplicada aos soldados, visto que já se acertou que fazem parte dos embates?

Diante de toda a exposição até agora, a resposta consegue ser clara: não. Afinal, a dignidade da pessoa humana continua a prosperar e, acertadamente, não se limita aos não combatentes, embora a aplicação tenha falhas.

Apesar de a resposta negativa à indagação do início desta subseção ser clara, ela não é tão óbvia assim. Isso porque muitos atos questionáveis permanecem permitidos ou, no mínimo, tolerados. Um exemplo evidente disso é a utilização de bombas atômicas e explosivos a fissão nuclear afins e subsequentes, cuja destruição extrema e conseqüências posteriores não só já são previstas, como também são conhecidas diante da detonação desses artefatos no Japão, no fim da Segunda Guerra Mundial, bem como acidentes radioativos variados ao redor do globo.

Nos seres humanos, sem adentrar a questão dos mortos que pereceram instantaneamente pela destruição total das células e que poderiam ser poupados, houve sobreviventes submetidos a intenso sofrimento, chamados de *hibakusha*. Entre as lesões acometidas, estão a exposição de órgãos internos em razão do arrancamento da pele e de diversos tecidos, constantes sangramentos, quedas de cabelo, vômitos e náuseas, além da dor excessiva proveniente dessas e de outras causas advindas do impacto nuclear (SERRANO, 2020, *on-line*).

O meio ambiente também sofreu destruição imediata semelhante. Em primeiro lugar, têm-se os animais cujas lesões ocorreram de forma similar aos humanos, dado o modo de funcionamento do mecanismo da bomba, o qual leva todo organismo animal vivo a experiências de sangramento e dor excessivos por causa do impacto e do calor. Em segundo lugar, as cercanias passaram por incêndios de longa duração, de cerca de três dias (SERRANO, 2020, *on-line*), seguidos por uma chuva torrencial preta carregada de poeira, sujeira, fuligem e partículas bastante radioativas (ATOMIC ARCHIVE, [2022], *on-line*), a qual conseguiu degradar ainda mais a situação já precária pós-detonação, inclusive pelo risco aumentado de insuficiência respiratória aos sobreviventes iniciais (BIERNATH, 2020, *on-line*).

Não se deve esquecer das consequências latentes, passíveis de acometer até gerações posteriores. Isso porque a ionização decorrente da grande quantidade de radiação de alta frequência tem potencial de acarretar infertilidade e mesmo de mutar negativamente os genes, ocasionando cânceres e demais lesões e acometimentos genéticos tanto em pessoas quanto em animais (BIERNATH, 2020, *on-line*).

Então, se um equipamento promove tal tipo de destruição acentuada e horrenda, deveria ser evitada sua utilização a qualquer custo, inclusive por meio do DIH. Seria essa a conclusão a que se chegaria, uma vez que as explosões atingiram inclusive civis, feridos, construções diversas (como hospitais), ao mesmo tempo que os combatentes sequer tiveram a possibilidade de se defender ou se render em face do ataque iminente, e infligiram sofrimento desmedido aos atingidos, até indivíduos distantes do ponto de detonação (o marco zero). Contudo, a comunidade internacional ainda carece de uma vedação a esses dispositivos.

Pela contrariedade à lógica de todo o restante do arcabouço normativo do DIH, chegou-se a apelar à Corte Internacional de Justiça (CIJ), cujo mandato se alicerça nos direitos humanos, para declarar o impedimento ao uso de bombas atômicas, ainda que fosse uma decisão difícil de impor, dado os interesses geopolíticos notórios de grandes nações influentes. Contudo,

talvez até em razão dessa influência geopolítica marcante<sup>4</sup>, embora a CIJ reconheça que não há autorização específica para usar ou ameaçar utilizar armas nucleares, tampouco concluiu que existe proibição de tais condutas. A Corte mencionou, inclusive, sequer poder definir se essas ações caberiam em contextos de autodefesa nas quais o Estado atacado estivesse sob risco de existência (ICJ, 1996, p. 43-45), frustrando a identificação de características aptas a padronizar comportamentos estatais de risco e colocando a soberania territorial (autodefesa dos Estados) acima da dignidade e do respeito à humanidade em geral (destruição em massa de pessoas e terras de forma quase indiscriminada, ainda que a localização do marco zero seja justificável).

Logo, como consequência – porventura indesejada – desse tipo de posicionamento errático da comunidade e dos organismos internacionais, torna-se árduo conceituar quais são esses comportamentos vedados que seriam ou desumanos e cruéis, ou desproporcionais. Os caminhos a desembocar nessa espécie de rol a fim de facilitar o máximo possível a sistematização e a identificação desses atos são dois, discriminados melhor a seguir:

**a) Taxatividade** – Por meio dessa lógica, as condutas interditas são caracterizadas como aquelas que estão expressamente previstas nos tratados internacionais e documentos afins, além dos casos claros abrangidos pelos costumes do DIH. Os tribunais, a exemplo da CIJ, baseiam suas decisões com base nessa interpretação, como no posicionamento adotado no episódio das armas nucleares. Trata-se de uma lógica bastante vantajosa para as nações beligerantes, as quais conseguem proceder com o uso de inovações e atualizações de armamentos que só depois, talvez, sejam considerados ilegais, mantendo-se, dessa forma, sempre à frente da legislação ou utilizando sua influência até o último momento, sem serem punidas a tempo por falta de normatividade, por mais questionável que fosse a atuação levada a cabo.

**b) Generalidade com exceções** – Quanto a esse método, as ações banidas seriam simplesmente aquelas que afrontassem a dignidade da pessoa humana, por esta ser o princípio basilar do Direito Humanitário. Por exemplo, caso se desenvolvesse um projétil capaz de perfurar o inimigo e dar choques significativos no organismo em que se alojou de maneira

---

<sup>4</sup> Oficialmente, a CIJ baseia sua opinião na interpretação do Direito Internacional tanto em relação a costumes quanto no tocante a convenções legais padrões – escritas, codificadas – como se vê na opinião aludida no texto (ICJ, 1996, *passim*). Entretanto, ressalte-se que todo o estabelecimento desses costumes e toda a escrita e a codificação dessas normas são pautadas, de modo significativo, pela influência geopolítica de grandes nações. Afinal, como decorrência da importância e do tamanho delas, elas se caracterizam como grandes forças motrizes nas atuações militares e políticas e, por lógica, nos marcos legais e consuetudinários.



intermitente e prolongada, saber-se-ia de antemão a vedação à qual o projétil mencionado estaria sujeito, por infligir dor desnecessária e intensa a diversos combatentes feridos, que sofreriam descargas elétricas mesmo fora de combate.

Essa proposta tem como ponto negativo a própria ausência de delimitação clara, afinal, conforme explanado, o conceito da dignidade da pessoa humana ainda não encontra uma definição firme. Em contrapartida, por causa dessa amplitude, não se daria carta branca a nenhum indivíduo ou país para adotar quaisquer estratégias militares potencialmente danosas que surgissem, sendo esse o ponto positivo de tal interpretação. Em decorrência, tal opção é aquela a qual melhor se alinha com os objetivos do DIH.

Contudo, da forma como exposta acima, é perceptível o descompasso com a realidade. Voltando-se ao exemplo das armas nucleares, como justificar a permissão delas se é para a dignidade da pessoa humana se sobressair de toda maneira? Por conseguinte, é necessário colocar em pauta a existência de práticas excepcionais aceitas, embora criticadas, as quais não asseguram uma generalidade tão ampla assim. Entretanto, vale destacar que, nessa conjuntura, as exceções são as ações que devem ser expressamente declaradas com antecedência, e não o contrário.

Independentemente da proposta à qual alguém se filie, é importante discriminar os casos concretos que foram desautorizados pelo DIH após as devidas discussões por parte dos componentes da sociedade internacional. Desse modo, ter-se-á em mente quais ocorrências se adéquam seja ao conceito de atos especificamente proibidos – no caso da taxatividade –, seja ao conceito de excepcionalidade – no caso da generalidade com exceções.

Os armamentos com potencial de destruição em massa tal qual as bombas atômicas, só que vedados na maioria dos países, são as armas biológicas e químicas, cada uma com sua convenção legal que a condena (a *Convenção de 1972 sobre a proibição de desenvolvimento, produção e estoque de armas bacteriológicas e tóxicas e sobre sua destruição* e a *Convenção de 1993 sobre a proibição do desenvolvimento, produção, estocagem e uso de armas químicas e sobre sua destruição*, respectivamente). Assentam-se como justificativas do impedimento tanto a coação aos sofrimentos da guerra quanto o reconhecimento de que as partes em conflito não possuem o direito ilimitado de conduzir as hostilidades como quiserem<sup>5</sup> (CICV, 2004a, *on-line*).

---

<sup>5</sup> Vê-se na motivação novamente os elementos relacionados com a dignidade da pessoa humana sendo recurso de limitação à atuação militar no DIH.

O desarmamento concerne a várias práticas: desenvolvimento, estocagem, aquisição, conservação e transferência<sup>6</sup>. Além disso, pauta a destruição desses métodos de combate acaso já produzidas (CICV, 2004a, *on-line*). Em meio a todo esse consenso, no quesito de artefatos biológicos, somente Angola e Israel estão à margem desse acordo mundial, mas se comprometeram a utilizar métodos bacteriológicos e afins apenas em situações em que a parte inimiga os tenha empregado antes. Assim, eles se abstêm do chamado “primeiro uso” (CICV, [2022]i, *on-line*). Quanto a instrumentos químicos de destruição em massa, além dos angolanos e israelitas, norte-coreanos, iraquianos e líbios também conservaram o direito de retaliar (CICV, 2004b, *on-line*).

Apesar dessas reservas, beira a unanimidade a opinião de que o emprego de tais artifícios é maléfico à humanidade e deve ser evitada a todo custo. 98% da população global está sob a proteção das convenções, enquanto 99% das armas químicas foram destruídas de forma comprovada (só o estoque de Estados Unidos e Rússia conseguiria exterminar a maior parte da vida humana e animal do planeta). Dentre os artefatos coibidos, estão balas de veneno, bem como gases asfixiantes e deletérios (OPCW, [2022], *on-line*).

Permanecendo na mesma lógica de evitar o extermínio e o sofrimento em massa, ainda que se destine a combatentes, as partes conflitantes não devem buscar a vitória empregando a fome como método de confronto. Sem a caloria dos alimentos, o corpo começa a definhar, pois o organismo precisa obter energia e, se não a consegue via alimentação, retira-a das gorduras e dos músculos, exaurindo-os até a debilitação do cérebro e levando à morte ou a problemas de crescimento e de raciocínio, sobretudo em crianças e adolescentes. Nota-se o padecimento dos afetados ao longo de todo esse processo de esmorecimento, análogo à tortura (SIERRA, 2003, *on-line*).

Nesse tocante, os cercos e os bloqueios se mantêm autorizados, desde que o intuito deles não seja por si só impor um enfraquecimento pela fome e se tenha um objetivo militar justificável. Por esse mesmo motivo, o socorro humanitário pode se apresentar, sem qualquer impedimento, para reverter ou atenuar a situação de desnutrição e subalimentação (CICV, [2022]f, *on-line*).

Ademais, igualmente entram no rol de comportamentos proibidos aqueles que impeçam a aplicação ou o funcionamento dos dispositivos elencados nos tratados do DIH. O cerceamento de socorro humanitário se trata de um exemplo visível dessa condição, mas

---

<sup>6</sup> Dentre as condutas citadas, deixou-se de normatizar o **emprego** das armas bacteriológicas. Todavia, interpretou-se que o emprego também seria uma ação proibida, tendo em vista que, para fazer uso de tais artefatos, o armazenamento e a produção são necessários. A posse, ilegal, é presumida, portanto (CICV, 2004a, *on-line*).

também se vedam escudos humanos, ordens de extermínio de sobreviventes, assim como pilhagens ou destruições de bens particulares.

## 2.5 A boa-fé como corolário dos comportamentos e das estratégias de batalha

Em uma questão que permeia os ordenamentos jurídicos mundiais, incluindo o brasileiro, têm-se como essencial o respeito à boa-fé, ou seja, qualquer comportamento contrário a ela deve ser rechaçado por todos os partícipes do conflito. Aqui, são importantes tanto a boa-fé objetiva – em especial diante de um padrão de comportamento esperado para a situação concreta, a ser adotado ou ajustado pelas partes conflitantes, embora também se vise à sua faceta de retrato ideal das coisas – quanto a boa-fé subjetiva – a convicção pessoal de estar respeitando o Direito e os costumes, ou de confiar legitimamente na aparência de determinado ato –, em consonância com as acepções desenvolvidas por Judith Martins Costa (2018, p. 279-283).

Em outras palavras, evitam-se práticas traiçoeiras entre os envolvidos, porque são atividades ilegais e inesperadas em condições normais (boa-fé objetiva) e porque penaliza a confiança da parte contrária (boa-fé subjetiva) em ato por parte do inimigo que aparenta ser legítimo e que deve ser respeitado. Tal princípio abrange negociações, acordos, aplicações do DIH e estratégias militares, entre outras conjunturas possíveis antes, durante e depois das batalhas. Afinal, de acordo com os apontamentos do CICV ([2022]h, *on-line*), “Sem a boa-fé, a negociação no campo de batalha é perigosa e de pouca utilidade. As partes têm que ser capazes de confiar nas garantias dadas pelo outro lado [...]”.

Essa regra está expressa com melhor evidência no artigo 37 do *Protocolo Adicional I de 1977 relativo às Convenções de Genebra*, embora seja possível argumentar que o espírito do DIH já reprimia o mau uso da estrutura disponibilizada por ele. O dispositivo mencionado estipula, em seu parágrafo primeiro, a proibição da perfídia, de modo que:

É proibido matar, ferir ou capturar um adversário recorrendo à perfídia. Constituem perfídia os atos que apelem à boa-fé de um adversário, com a intenção de enganá-lo, fazendo-o crer que tem o direito de receber ou a obrigação de assegurar a proteção prevista pelas regras de direito internacional aplicáveis nos conflitos armados. São exemplos de perfídia os seguintes atos:

- a) simular intenção de negociar a coberto da bandeira de trégua, ou simular a rendição;
- b) simular uma incapacidade causada por ferimentos ou enfermidade;
- c) simular o estatuto de civil ou de não combatente;
- d) simular o estatuto protegido utilizando sinais, emblemas ou uniformes das Nações Unidas, de Estados neutros ou de outros Estados não Partes em conflito. (CICV, 2017, p. 32)

Vislumbra-se que a perfídia é diferente do ardil ou da artimanha de guerra, como inclusive assevera o parágrafo posterior ao transcrito, na medida em que aquela sinaliza à parte contrária que ela possui um *status* de direito inexistente (do qual decorreria a boa-fé objetiva). Isto é, deve-se conceder uma proteção ou uma garantia, cuja complacência (a boa-fé subjetiva) é subvertida em vantagem ao lado que se utilizou das prerrogativas do DIH e as desvirtuou e em detrimento do lado que respeitou as regras (CICV, [2022]g, *on-line*).

Por outra perspectiva, os ardis são meras estratégias de combate, que estimulam a confiança e a expectativa alheias, sem incorrer, contudo, em uma obrigação a ser respeitada por outrem. Por exemplo, a camuflagem de soldados cria uma confiança da ausência de inimigos na localidade, entretanto esse disfarce não impõe a necessidade do exército contrário de baixar a guarda. É por essa razão que, por mais que exista uma enganação, não se estabelece uma boa-fé a ser quebrada e se permite esse tipo de conduta. Além do mimetismo, informações falsas, operações simuladas e emboscadas também são exemplificações de comportamentos aceitáveis (CICV, 2017, p. 36).

### 3 A GUERRA VIRTUAL: PRÁTICAS E ESTRATÉGIAS NO CAMPO DE BATALHA CIBERNÉTICO E SEUS IMPACTOS

Umberto Gori (1998, p. 571-577) mostra que se depara, novamente, com outro termo de difícil definição: a guerra. Pela complexidade social desse acontecimento, ele não possui elementos que o identifiquem de forma clara, tampouco que deem azo a uma única interpretação. Assim, existem múltiplas definições versando sobre tal fenômeno.

Não bastasse essa dificuldade conceitual, a própria visão da sociedade sobre os conflitos sofre mutação ao longo da história humana. Da Antiguidade até a Idade Média, seja no campo da ética, seja no campo do Direito, não se falava em legitimidade da guerra, tampouco se seguiam critérios para iniciá-la. Com essa mesma visão das beligerâncias, assegurava-se a liberdade de eliminar todos os inimigos, sem restrições; assim, civis homens, crianças e mulheres não eram poupados do julgo do adversário. Em parte, esse entendimento vinha da inexistência de um Estado propriamente dito; já que não havia uma máquina a enfrentar, o papel de oponente recaía a toda a população (MORGENTHAU, 2003, p. 437-442).

Com a proliferação da adoção do Estado de Direito, a guerra começou a receber restrições, devido à necessidade de se observar os direitos inerentes às pessoas. A partir desse momento, a moralidade dos confrontos se intensificou e ascendeu a um valor de extrema importância, ao passo que, como consequência, a legitimidade dos confrontos entrou nos debates, inclusive com a categorização de guerras em justas ou injustas, proposta por Hugo Grotius<sup>7</sup> (1901, *passim*).

Usando classificação semelhante, Vattel (2004, p. 422) afirma ainda que “[...] se uma Nação pega em armas quando ela não recebeu nenhuma injúria<sup>8</sup>, e quando por injúria não está ameaçada, ela faz uma guerra injusta”, assim como acrescenta os motivos honestos, independentes do objetivo do embate, os quais se centram no bem-estar do Estado; os motivos viciosos são os contrários dos honestos. Depreende-se dos argumentos do autor que, então, iniciar um confronto injusto ou com motivo vicioso seria uma violação ao que ele denomina de “Direito das Gentes”.

---

<sup>7</sup> Conforme o entendimento de Grotius (1901, *passim*), esse atributo dos conflitos varia a depender de seu caráter (se público, privado ou misto). Evita-se adentrar essa classificação de forma pormenorizada, senão fugiria do escopo deste trabalho. Afinal, para entender se os ciberataques conseguem se configurar como guerra, pouco importa a motivação para o embate. O importante é compreender que a luta, de irrestrita, passou a ser passível de críticas e de justificativas.

<sup>8</sup> A injúria para Vattel (2004, p. 421) decorre de uma violação de algum dos direitos da Nação ou de um ataque a ela.

Atualmente, o posicionamento que vigora é o de condenar a guerra ao máximo, limitando o que seria um “direito ao ataque” a casos bastante excepcionais. Mesmo quando se tolera a força, prevê-se a intervenção por meio do Conselho de Segurança, em um esforço internacional conjunto, em detrimento da agressão de somente um país, a qual deve se limitar a uma legítima defesa imediata – isto é, de viés não prolongado (SERRA; SOUSA, 2021, p. 46-47). Entende-se, hoje em dia, que existe um direito à paz, o qual, inclusive, é direito humano, na medida em que a ONU expressa, em sua Constituição, a indispensabilidade da paz e aborda maneiras de alcançá-la mediante decisões coletivas sob a égide dos princípios internacionais. Trata-se de um direito que parte da quinta geração de direitos fundamentais, fase essa que inclusive apresenta preocupação com a jurisdição por meio da rede mundial de computadores (NARCISO; BORIN, 2015, p. 135-137).

Apesar desse desejo, a plena paz não foi atingida, e, pelo contrário, nota-se um acirramento das tensões mundiais. Nesse caso, reputa-se imprescindível dissecar as características do estado de beligerância, a fim de verificar se os ciberataques conseguem se enquadrar como elementos da dinâmica militar.

O conceito mais aceito historicamente<sup>9</sup> pautou como base os atos formais que levavam à declaração bélica; como consequência, fatores mais ligados à área do Direito eram o enfoque dos estudiosos. Todavia, trata-se de uma definição bastante problemática, visto que, com o passar do tempo, tais elementos não correspondem mais à realidade dos conflitos recentes pela ausência paulatina dessas formalidades. Por exemplo, embora venha a público a atuação de exércitos em várias frentes de batalhas, pouco se veem declarações de guerra formal por parte dos Estados, mesmo porque há uma tendência de os participantes diretos dos embates sequer chamarem os confrontos de guerra propriamente dita<sup>10</sup>, por causa da impopularidade de tais medidas.

Em consonância com o entendimento exposto, Hugo Grotius (1901, p. 317, traduziu-se) reforça o ato de formalidade como condição para tornar a guerra justa: “[...] ela [a guerra] precisa não só ser levada a cabo pela autoridade soberana em ambos os lados, mas necessita, do mesmo modo, ser devida e formalmente declarada, e declarada de maneira a ser conhecida por cada uma das potências beligerantes”.

---

<sup>9</sup> Note-se que a guerra só passou a ser estudada, de maneira sistemática, há pouco tempo. Maquiavel, em 1516, foi um dos primeiros a abordar o assunto, por exemplo (GORI, 1998, p. 571). Por isso, vê-se um apego à estrutura formal, escrita. Tendo em vista essa localização temporal, percebe-se quão recente foi o desenvolvimento de tais estudos, não se devendo apegar à sensação de Antiguidade que o termo “historicamente” traz.

<sup>10</sup> Nesse sentido, vislumbra-se o conflito curdo-turco, ao qual autoridades turcas e iranianas se referem como “luta contra organizações terroristas” (TURQUIA..., 2022, *on-line*) e a guerra russo-ucraniana, a qual o Kremlin denomina simplesmente de “operação militar especial” (PUTIN..., 2022, *on-line*).

Na mesma linha de raciocínio, Joseph Frankel (2022, *on-line*) esclarece que a guerra surge de uma situação conflituosa e conduzida por meio de métodos socialmente reconhecidos, também atribuindo ao verbete, de certo modo, o respeito a uma forma, pautada no costume e na lei, quando se escora no âmbito do “reconhecimento social”. Verifica-se, contudo, uma tentativa de ampliar o conceito, tendo em vista que essa identificação por parte da sociedade se expressa por meios bem mais diversos que atos oficiais direcionados, a exemplo de insatisfações, ordens orais e outros eventos mais atinentes à Sociologia e áreas de estudo afins do que ao Direito em si, embora nele resvale e nele se consiga englobar elementos marcantes para caracterizar a guerra.

Em outra perspectiva também antiquada, anteriormente, a característica primordial de uma guerra se centrava nos atos violentos de uma força armada organizada. No entanto, é perceptível o viés restritivo desse significado, com clara particularidade armamentista, em um mundo que hoje exhibe uma miríade de vertentes nas batalhas, como a psicológica e a econômica (GORI, 1998, p. 571-577).

Com o irrompimento dos conflitos modernos, a busca por uma definição que se oriente pelos demais aspectos conjunturais é essencial para uma análise atual das hostilidades. Diante disso, seriam os ataques virtuais, de fato, uma guerra, ainda que perpetrada por Estados, mas sem que tal situação de direito seja reconhecida pelos ritos apropriados?

### **3.1 A caracterização dos ataques virtuais como componentes da guerra**

Para responder ao questionamento proposto, deve-se debruçar muito mais sobre os aspectos factuais e contextuais de uma guerra, conforme exposto. Com esse objetivo, a conceituação de Umberto Gori (1998, p. 571-577) traz quatro características que parecem se adequar ao fenômeno de forma mais apropriada: atividade militar; tensão acentuada na opinião pública; aplicação de normas jurídicas incomuns, quando comparadas com os dispositivos aplicados em tempos normais, de paz; e uma integração política gradativa na estrutura interna, geralmente girando em torno do nacionalismo e do enfrentamento a um inimigo comum. Embora ainda sejam características imperfeitas, pois continuam deixando de fora outros métodos de pressão hostis, tais elementos se moldam melhor à conjuntura conflituosa da atualidade, sem se prender ao estilo de guerra passado – com violência e ritos no cerne da temática –, dada a amplitude proveniente do sentido de “atividade militar”.

Claro que, com a atuação individual de *hackers* que buscam proveito próprio (em geral, dinheiro), deve-se verificar caso a caso o intuito das invasões e, se visualizada a situação

de vantagem individual, atribui-la ao Direito Penal comum, ficando de fora do presente estudo. Entretanto, o uso de *hackers* como mecanismo estatal de imposição de força acontece e se subsume ao esforço de guerra.

Retomando as características pertinentes às hostilidades retratas por Umberto Gori, a batalha na internet consegue se compatibilizar com todas elas. A respeito da primeira característica, sabe-se que algumas nações – a exemplo dos Estados Unidos e da Coreia do Norte – possuem divisões nas Forças Armadas designadas para manejar ameaças cibernéticas, seja com vistas à inteligência e à contrainteligência, seja com vistas a mecanismos ofensivos (CAESAR, 2021, *on-line*). Do mesmo modo, a Ucrânia, em meio ao seu confronto com a Rússia, convocou nacional e internacionalmente indivíduos a integrar seu esforço tecnológico bélico, que chegou a ter mais de 400 mil pessoas (SCHECHNER, 2022, *on-line*).

É uma tendência por causa da crescente dependência, eficiência e influência da tecnologia na sociedade. Ainda que os Exércitos não mantenham uma estrutura destinada a esse campo entre sua organização, os governos já construíram órgãos e deles dispõem com programas avançados, capazes de interferir em sistemas ao redor do mundo<sup>11</sup> – como se observa na ABIN, na CIA, no MI-5, entre outros – e aptos a serem utilizados com fins bélicos. Portanto, os enfrentamentos virtuais podem, sim, ser entendidos como atividades de cunho militar.

Os outros três aspectos se relacionam mais com o caso concreto pelo qual a nação está passando, sem se ancorar em maiores definições. Assim, não faz sentido esclarecer se os métodos de combate no ciberespaço configuram uma tensão, um estado excepcional do ordenamento jurídico ou uma coesão nacional. Na verdade, devem-se sopesar esses três elementos não para afirmar se os ataques fazem parte da conceituação abstrata de cada um ou mesmo se a conglobam, mas sim para verificar se eles são decorrentes da presença de tais atributos àquele momento na sociedade em questão. Para isso, os comportamentos hostis precisam ser analisados em cada situação concreta, incluindo o comportamento e a configuração da sociedade naquele intervalo de tempo, de modo que seja possível identificar um estado de guerra<sup>12</sup>.

No tocante à ocorrência das ações no espaço cibernético, é importante frisar que ele constitui uma espécie de mundo abstrato construído em cima da internet em que há uma

---

<sup>11</sup> Essa capacidade é observada inclusive entre os particulares, *vide os hackers*, que hoje são um problema que afeta governos e cidadãos.

<sup>12</sup> Para tentar facilitar o entendimento, propõe-se a seguir a reconstrução da afirmação com outras palavras: a ocorrência de ataques virtuais não vai indicar a existência de tensão social, de aplicação excepcional de ordenamentos jurídicos alheios aos tempos de paz, tampouco de coesão nacional. São essas três características que vão indicar o estado de guerra, do qual as ofensivas serão meras consequências. Em contrapartida, tais ofensivas cibernéticas podem, sim, configurar uma atividade militar.



vivência ou uma experiência humana vinculada a uma interação semiótica e social. Essas vivências, inclusive, são tão completas que reproduzem relacionamentos e trocas concretas, longe da abstração e da simbologia do ciberespaço (LUCERO, 2011, p. 37-38).

Logo, apesar de construir um espaço à parte do mundo palpável, têm-se consequências diretas na realidade concreta. Não só isso, mas, em razão da necessidade de uma manifestação física – os dispositivos que acessam a rede mundial de computadores e nela se interligam –, consegue-se discernir tanto a ação que induz um ataque quanto a materialização do respectivo resultado. Chega-se a denotar, assim, um sentido de territorialidade(s), inclusive, na medida em que é possível afrontar a soberania política de um Estado devidamente organizado ao atingir um espaço sujeito a esse poder soberano – seja na localidade do ato, seja na área de repercussão da conduta, sem que se necessite averiguar os demais princípios concernentes à repressão a atividades criminosas, como o princípio de proteção ou o princípio da universalidade (BITENCOURT, 2022, *e-book*).

Então, considerando as delimitações, as concepções e as conjunturas mencionadas, percebe-se que, a depender da estrutura por trás dos ataques virtuais, é possível enquadrá-los como atos de guerra e, como decorrência, práticas a serem analisadas à luz do DIH.

### **3.2 A derrubada de servidores-chave para a estrutura nacional**

O principal tipo de ofensiva é a derrubada de *sites*, sistemas ou serviços em geral do governo que dependam da rede para se conectar, deixando-os fora do ar. A popularidade desse mecanismo provavelmente se deve por ser um ataque simples para quem tem poder de processamento de dados; contudo, em caso de sucesso, causa um empecilho considerável para a parte afetada. Afinal, uma ampla gama de comunicações está sendo impedida ou dificultada de acontecer.

A fim de obter tal resultado, os atacantes sobrecarregam os servidores-alvo com um imenso tráfego de dados – por isso, a necessidade enorme de processamento –, de forma que esses servidores não consigam lidar com o fluxo de informações e, conseqüentemente, não respondam a todos os acessos por sobrepujar a capacidade de resposta disponível. Essa transmissão massiva de dados, denominada de DDoS, é disparada por diversos computadores, seja porque estão infectados em razão da disseminação de vírus pelo invasor, seja porque os

usuários dos dispositivos concordaram com a utilização alheia destes de antemão – por meio de aplicativos, por exemplo<sup>13</sup> (GREENEMEIER, 2014, *on-line*).

As hostilidades russo-ucranianas demonstraram a utilização em escala nunca vista desse tipo de envolvimento bélico. *Hackers* de ambos os países já derrubaram vários endereços eletrônicos governamentais um do outro e se dividem entre agressores apoiados pelos Estados e amadores (CONGER; SATARIANO, 2022, *on-line*). O tamanho dessa espécie de enfrentamento pode ser mensurável ao se observar que milhares de europeus chegaram a ficar sem internet devido a tais ataques cibernéticos (UCRÂNIA..., 2022b, *on-line*).

Ao observar os registros mais recentes do CSIS (2022, *on-line*), que acompanha e lista os incidentes cibernéticos significativos, observa-se um envolvimento em peso de países europeus, em geral como vítima<sup>14</sup>. Albânia, Montenegro, Bósnia e Herzegovina, Reino Unido, Noruega, Itália, entre outros, em algum momento de 2022 – certas nações até mais de uma vez – sofreram com servidores e serviços fora do ar, sobretudo pelo método de DDoS.

Embora seja uma situação árdua de desvendar por completo, já que ou não se sabem os atacantes, ou não se consegue chegar aos patrocinadores e financiadores dos atos, a localização geográfica de vítimas e perpetradores deixa subentender que as condutas são uma reação à prática sancionatória adotada pelo Ocidente – em especial, pela Europa e pelos Estados Unidos. Isso ocorre porque a atividade de contrainteligência detecta que os comandos provêm de grupos iranianos e russos, ou de partidários favoráveis aos governos dessas duas nações, justamente os entes que mais sofrem com as sanções ocidentais, junto à Coreia do Norte, embora esta se concentre em outro tipo de ataque que será descrito mais à frente.

Devido a essa análise entre nacionalidades de agentes e vítimas, não se pode descartar também a motivação simplesmente ideológica, que subjaz toda a tensão sancionatória descrita (MAZEBOLT TECHNOLOGIES, 2021, *on-line*). Assim, a questão da represália e da ideologia podem andar tanto em separado, como reação a um ato específico de outro Estado, ou em conjunto, motivando ao mesmo tempo os ataques virtuais por serem incitamentos complementares, isto é, que não anulam um ao outro.

---

<sup>13</sup> É imprescindível ressaltar que, assim como nos outros casos de descrição de invasões virtuais, se almeja apenas realizar uma discriminação sucinta e resumida do modo de operação dos ataques, a fim de situar brevemente o leitor sobre o que se fala. O detalhamento minucioso desviaria o foco do tema e fugiria, por conseguinte, do escopo deste trabalho.

<sup>14</sup> É importante ressaltar que o conceito de vítima e atacante diz respeito unicamente à análise individual e específica de cada ofensiva cibernética. Assim, não se analisam questões de culpa e inocência – seja de governos, seja de indivíduos –, ainda mais quando se verifica a conjuntura de forma ampla, com suas causas e consequências políticas, históricas, sociais e econômicas, todas carregadas de enorme complexidade. Tampouco se afirma que os lados não se invertam eventualmente; por exemplo, o Irã foi alvo de um incidente que derrubou *sites*, imagens, banco de dados e computadores de sua ICCO, sendo vítima dessa vez, portanto (CSIS, 2022, *on-line*).

Deve-se ter em mente, entretanto, que não é só um incômodo, uma manifestação, um protesto ou mesmo uma interrupção de serviços e comunicações supérfluos que são preocupantes no contexto de tais ataques, visto que essas consequências servem apenas para demonstrar um posicionamento e causar descontentamento na população, tanto pela inconveniência das operações estarem *off-line* quanto pela simpatia à mensagem eventualmente transmitida ou subentendida. O problema aparece quando ocorre a suspensão de uma infraestrutura importante para o país, a exemplo de serviços de energia, água e saúde (incluindo seus respectivos bancos de dados), bem como a queda de mecanismos eleitorais *on-line*, como propagandas, campanhas, arrecadamentos e informações político-partidárias domésticas, comprometendo a democracia do país em detrimento da ideologia de que não se seja correligionário ou com que não se simpatize, como já há suspeitas desse tipo de interferência nos Estados Unidos (MAZEBOLT TECHNOLOGIES, 2021, *on-line*).

Trata-se de impactos preocupantes, dado que o impedimento à livre informação e à participação política são comportamentos que não só minam os institutos existentes, e, mesmo por isso, se configuram como antidemocráticos. Ora, a diversificação das fontes de conhecimento é uma característica intrínseca à democracia, pois permite a formação de consciência própria e a manifestação de um posicionamento construído sem enviesamentos. Por motivos similares, a negativa de acesso a determinadas fontes, ainda que temporariamente, afeta o princípio da normalidade das eleições, visto que suprime o debate de ideias (e, tangencialmente, a escolha e o posicionamento conscientes), assim como macula o princípio da igualdade, dados a possibilidade de prejuízos a certos políticos e partidos e o favorecimento aos demais que restaram intactos – mesmo que não tenham colaborado com os atos (MACHADO, R., 2018, *e-book*).

A verdade é que são impactos longe de serem desprezíveis caso se detenha a eles mais profundamente. Os efeitos das eventuais quedas, embora reversíveis, podem durar intervalos de tempo consideráveis e requerem constantes investimentos e atualizações para se evitar as consequências ao máximo. É um desafio a ser enfrentado pelas nações, em especial aquelas mais apegadas à democracia, valendo-se também de uma coesão entre todas as correntes político-ideológicas.

### **3.3 A apropriação de dados críticos e estruturais dos países**

A ofensiva contra a rede pode se destinar, ainda, a identificar dados e informações e enviá-los a outro servidor, por meio da conexão de internet, com a ajuda de um programa de

computador malicioso, chamado de *malware*<sup>15</sup>. Afinal, no mundo conectado de hoje, os dados são novos tipos de ativos. É uma conjuntura mais difícil de atuar, visto que envolve achar brechas no sistema ou obter acesso direto a ele mediante uma entrada interna<sup>16</sup>; além disso, para achar as informações e, enfim, transmiti-las a outro local, também é necessário utilizar e configurar os citados *malwares* (SHARMA, 2017, p. 62-64).

Apesar de todas as dificuldades, é possível a obtenção de dados sensíveis com esse método. No tocante às informações de nações, as tecnologias avançadas, os desenvolvimentos militares e as infraestruturas críticas são os materiais mais visados pelos atacantes, além da possibilidade de espionagem contínua. Desse modo, conhecimentos como a localização e a superioridades das defesas de um Estado, assim como o *design*, as configurações e as especificações de armas e, por fim, as plantas de edificações importantes conseguem chegar nas mãos dos adversários (SHARMA, 2017, p. 62-67).

Os Estados Unidos, por exemplo, já reconheceram sua posição como alvos de diversos países, dentre eles a China, nação com que disputa a hegemonia econômica e a influência geopolítica global. Os oficiais de inteligência disseram que os estrangeiros acessaram dados de infraestrutura, inclusive com a opção de desligar e prevenir a operação física, com foco em sistemas de água e combustível (NAKASHIMA, 2014, *on-line*). Mais recentemente, do outro lado, a China acusou os Estados Unidos, por meio da NSA, de roubar dados de redes de comunicação da Universidade Politécnica do Noroeste da China. O México também admitiu o prejuízo com vazamento de informações que revelaram comunicações internas do país, incluindo o monitoramento do embaixador estadunidense no território mexicano (CSIS, 2022, *on-line*).

Observa-se que tais ataques aumentam o nível de ameaça, que já eram relevantes, incrementando a sofisticação vista nos procedimentos de DDoS e afins. Porém, eles não se atêm somente à elucidação da movimentação militar e à alocação estrutural, as consequências mais evidentes de tais subtrações de dados. De fato, eles constituem uma gama importante do poderio estatal; porém, o enfoque nos entes privados – que estão igualmente na vanguarda tecnológica – se mostra tão danoso quanto uma atuação centrada na administração dos Estados, até porque,

---

<sup>15</sup> *Malware* é o gênero, dentro do qual os conhecidos vírus são uma das espécies de programas. Os programas maliciosos podem ser igualmente *trojans*, *spywares* e vermes, cuja diferenciação se baseia no intuito e no modo de atuação e replicação de cada um (HOSCH, 2022, *on-line*).

<sup>16</sup> Essa entrada interna pode ser ou não intencional. Isso quer dizer que a invasão consegue se dar ou por um ajudante com acesso privilegiado que permite ou facilita a entrada do programa malicioso no sistema – sendo partícipe do esquema, portanto –, ou por uma pessoa que transmite uma infecção por meio de mecanismos pessoais já comprometidos sem que se saiba, como cliques em *links* indevidos, assim como acontece com as infecções de dispositivos comuns de particulares, sendo este chamado de vítima comprometida, diante de seu desconhecimento perante a ameaça (SHARMA, 2017, *passim*).

em muitos países, a iniciativa privada ajuda a construção de toda a base de vertente militar, estrutural e tecnológica, entre outras.

A espionagem e o furto ou o roubo de dados da perspectiva das instituições privadas conseguem fortalecer o mercado nacional e podem levar à concorrência desleal e predatória, aqui prejudicando os alicerces estatais em um ponto de vista de guerra econômica, sobretudo, e, portanto, o enfraquecimento mais disfarçado e encoberto dos adversários (SCHARMA, 2017, *passim*). Não à toa, é um comportamento que, embora não esteja demarcado de maneira apropriada no cenário de Direito Internacional Público, é rechaçado por várias legislações locais, recaindo com maior força no Direito Internacional Privado, sobretudo em face da criação do conceito de propriedade intelectual<sup>17</sup>.

Ademais, não se pode deixar de lado as mesmas ameaças eleitorais e democráticas antevistas diante das ofensivas de derrubada de servidores e dispositivos semelhantes. Deve-se ter isso em mente porque, em meio ao acesso de sistemas internos, quaisquer informações são passíveis de serem adulteradas, o que reforça a necessidade de preocupação e atenção da comunidade global e a criação de mecanismos de proteção constantes em resposta a tais ameaças.

### **3.4 A apropriação de dinheiro em prol das Forças Armadas e da guerra**

Nos tópicos anteriores, vislumbraram-se comportamentos que, conquanto atribuíssem determinada vantagem aos atacantes, não eram tão palpáveis e auferíveis, mesmo porque, até o momento, fazem parte mais de uma estratégia de escalonamento de ameaças e de influências do que de ganhos diretos, provavelmente pela ausência de conflito aberto entre as potências com infraestrutura tecnológica ampla. Isso, porém, não significa que tais ataques não sejam temerosos.

Ainda assim, existem ofensivas que se direcionam a um lucro imediato, visando à obtenção de dinheiro. Essa transferência consegue ser mais danosa em razão da faceta universal desempenhada pela moeda. Segundo os ensinamentos de Bernardo Guimarães e Carlos Gonçalves (2017, *e-book*), a moeda exerce as funções de unidade de troca irrestrita, reserva de valor e unidade referencial de medida monetária. Em suma, com outras palavras, o dinheiro consegue ser permutado por qualquer outro bem ou serviço, além de guardado, mantendo-se o atributo da quantia nominal reservado a ele, ou, ainda, utilizado como comparação de valores

---

<sup>17</sup> Nesse tocante, pode-se verificar as considerações de Annabelle Bennett e Sam Granata (2019, *on-line*), além dos apontamentos de Fábio Condeixa (2015, p. 23-25).

entre as mercadorias. Não à toa, como bem expressa Márcio Braga (2019, *e-book*), a moeda é o ativo econômico de maior liquidez. Nesse sentido, o dinheiro é o ativo com maior capacidade de ser trocado por bens ou serviços, justamente por sua posição de universalidade na troca, sendo o bem mais provável de ser aceito em uma transação.

Todas essas características da moeda refletem a facilidade que uma parte em conflito possui ao angariar esse tipo de patrimônio. Assim que põe as mãos em valores, os líderes obtêm o poder de adquirir qualquer coisa que queiram, seja investir na infraestrutura nacional, seja aprimorar a máquina bélica. Por causa desse interesse universal no dinheiro – isto é, todo mundo o aceita – o investimento consegue ser aplicado tanto em pessoal, como em *hackers*, quanto em maquinário, a exemplo de armamentos, servidores ou outros equipamentos de conexão com a rede mundial de computadores.

O estilo aludido de ataque e, como decorrência, de financiamento é conhecido por ser posto em prática, em especial, pela Coreia do Norte, por meio de seu Escritório Geral de Reconhecimento<sup>18</sup>, embora não se restrinja a ele, visto que diversos outros países detêm arsenal tecnológico similar. Essa confirmação vem, inclusive, de fontes oficiais e governamentais, a exemplo do Departamento de Justiça dos EUA (THREE..., 2021, *on-line*), que chegaram a prender e indiciar três *hackers* militares norte-coreanos dessa unidade.

Da mesma forma que os russos e os iranianos, a Coreia do Norte é alvo de diversas sanções da comunidade internacional, as quais limitam o acesso do país a importações e exportações em geral, desde itens de luxo até comidas, produtos agrícolas e têxteis, minérios, maquinários e equipamentos elétricos, bem como restringem os deslocamentos de navios de bandeira norte-coreana (ARMS CONTROL ASSOCIATION, 2022, *on-line*). Além desses refreamentos impostos pelas Nações Unidas, são permitidos demais controles unilaterais de cada país, como se observa nas determinações do Departamento do Tesouro dos EUA (OFAC, 2016, *passim*), desde que não causem prejuízo à subsistência da população. Dentre todas essas restrições apontadas, existe também a interdição de deslocamento de dinheiro vivo.

Dessa forma, com o comércio decadente e a inoperância de qualquer fluxo de pagamento, a Coreia do Norte se vê diante de poucas opções de arrecadar e de manejar sua economia interna. A agricultura é voltada para abastecer o mercado interno, sobretudo em razão das colheitas fracassadas que afligem o plantio do território, e a importação de arroz e óleo de soja é necessária com vistas a complementar a necessidade alimentar básica (CIA, 2022, *on-*

---

<sup>18</sup> Essa agência de inteligência militar da Coreia do Norte também é conhecida, na comunidade de cibersegurança internacional, como Grupo Lázaro ou como Ameaça Persistente Avançada 38 (THREE..., 2021, *on-line*).

*line*). Juntando essa instabilidade de produtos com a inibição dos ganhos com exportações, o país se escora nos ataques cibernéticos como alternativa à situação em que se encontra.

Consequentemente, tornaram-se comuns ofensivas destinadas a apropriar dinheiro alheio, em especial os valores emanados no mundo virtual – quer sejam os próprios papéis-moedas com as respectivas quantias representadas em transações digitais, quer sejam as criptomoedas. Os métodos para atingir essas transferências de quantias no ciberespaço variam, podendo vitimizar cidadãos, empresas – estatais ou privadas – ou mesmo o próprio governo diretamente. A seguir, indicam-se os principais meios de se obter os valores de modo ilícito, fora os ataques já discriminados nos tópicos anteriores, baseado no próprio relatório do Departamento de Justiça dos EUA (THREE..., 2021, *on-line*) em que se baseou a persecução criminal de *hackers* norte-coreanos<sup>19</sup>.

**a) Golpes digitais contra bancos** – Invasão dos sistemas bancários a fim de emitir ordens de pagamentos (transferências) forjadas, o que possibilita depósitos em contas, inclusive com vistas a sacar o dinheiro em caixas de autoatendimento. Às vezes, a derradeira ação milionária ocorre após muito planejamento, de modo que o controle do sistema seja amplo e esteja certificado.

**b) Ransomware** – Uma espécie de extorsão virtual em que um programa malicioso é construído para criptografar os arquivos e os sistemas de determinado dispositivo, de modo que os tornem inutilizáveis. Assim, para reverter o processo, eliminar a criptografia e possibilitar o uso novamente, os criminosos demandam pagamentos (CISA, [2022], *on-line*).

**c) Campanhas de phishing** – O *phishing* possui em seu cerne o ato de ludibriar a vítima – passando-se por um terceiro com a maior fidedignidade possível – e de levá-la a fornecer dados e informações pessoais que serão utilizados para roubar dinheiro desse indivíduo ou para obter outra vantagem indevida por meio dos sistemas virtuais bancário e financeiro. Para conseguir essa enganação, os métodos utilizados são diversos, mas geralmente envolvem correios eletrônicos, sistemas de mensagens instantâneas ou *web sites* (CSRC, [2022], *on-line*).

**d) Roubo de criptomoedas** – Invasão dos sistemas de empresas relacionadas com moedas digitais, de forma a transferir os ativos a que essas companhias tivessem acesso. Assim

---

<sup>19</sup> Embora aqui se enfatize a atividade de grupos norte-coreanos, eles não são os únicos a adotar esse *modus operandi*. Eles apenas foram evidenciados aqui pela notória participação estatal da Coreia do Norte nesse tipo de esquema, forçando a aplicação do Direito Humanitário Internacional. Contudo, tal atividade criminosa pode ser perpetrada por qualquer nacional para qualquer país em estado belicoso.

como na invasão de golpes visando a transações digitais com os valores de moeda física, a transferência final decorre depois de se garantir o poder de controle da movimentação.

**e) Criação e publicação de aplicativos de criptomoedas** – Nesse caso, em vez de se infiltrar ativamente nos sistemas, os *hackers* se disfarçam como um empreendimento financeiro administrador de criptomoedas. A instalação do aplicativo pelo próprio usuário do dispositivo e o eventual preenchimento de dados bancários tornavam este passível de posterior invasão para movimentar financeiramente as contas desse usuário.

Vale a pena ressaltar que os métodos ora discriminados não precisam atuar de forma separada. Uma ou mais estratégias podem ser utilizadas em conjunto, o que, na verdade, são as ocorrências mais comuns. Por exemplo, as campanhas de *phishing* são mecanismos iniciais levados a cabo, a fim de que uma pessoa facilite o acesso não só para o furto de dados, mas de modo que se garanta o controle para proceder a golpes e encriptações direcionadas à prática de *ransomware*.

Diferentemente das condutas analisadas nos subtópicos anteriores, o enfoque está na apropriação do dinheiro em si, transformando-se em vantagem imediata. Ainda, apesar de o valor da movimentação financeira possa se destinar a qualquer setor da nação atacante, a capacidade de uso direto na estrutura da guerra é outro fator que pesa a essas ofensivas. Há fortes indícios que a receita de tal operação é designada aos programas de armamento nuclear e de mísseis balísticos, sem adentrar o prejuízo advindo da desconfiança do sistema financeiro global (CISA, 2020, *on-line*), tendo em vista que, na maioria das vezes, a movimentação de dinheiro afeta indivíduos do mundo inteiro, inclusive aqueles que estão completamente alheios às partes conflitantes.

Já em 2019, as Nações Unidas falavam na quantia de US\$ 2 bilhões levantados por ciberataques norte-coreanos e destinados aos programas de armamento de destruição em massa e ao esforço bélico em geral na Península Coreana, o que se comprova em razão do avanço sucessivo na área militar, mesmo em meio às sanções punitivas impostas (NICHOLS, 2019, *on-line*). Mais adiante, com o ano de 2022 ainda em andamento, as ofensivas cibernéticas roubaram US\$ 600 milhões de NFT<sup>20</sup> de um jogo vietnamita, além de outros US\$ 840 milhões

---

<sup>20</sup> O NFT é um criptoativo não fungível, que, em razão dessa ausência de intercambialidade entre si (cada NFT é único, por mais parecido que seja com outro), não é propriamente uma criptomoeda. Entretanto, trata-se de um patrimônio valioso que corresponde a objetos únicos e imutáveis manifestados no mundo digital e que consegue ser exprimido em valores – ou em papel-moeda oficial, ou em moedas digitais (COSSETTI, 2021, *on-line*). Assim, embora o conjunto de NFTs valha US\$ 600 milhões, não se tem uma quantidade de 600 milhões de NFT. Consoante as características de moedas elencadas por Bernardo Guimarães e Carlos Gonçalves (2017, *e-book*),



comprovados de outras fontes (a exemplos de bancos sul-africanos, paquistaneses e japoneses), mas cuja quantidade deve aumentar, visto que existem demais suspeitas ao qual não se pôde atribuir o autor ou a instituição responsável (BOOM, 2022, *on-line*).

Não só tais montantes milionários vinculados ao aprimoramento armamentista bélico são preocupantes, mas também porque a região peninsular coreana está próxima de territórios disputados entre as duas Coreias, o Japão e a Rússia (MINISTRY OF FOREIGN AFFAIRS OF JAPAN, [2022], *on-line*). Isso sem se concentrar na própria Guerra das Coreias, que está somente em trégua, ou seja, tecnicamente ainda estão com declarações de guerra vigentes uma contra a outra e em constante ameaça e tensão (LENDON, 2021, *on-line*).

Não à toa, o promotor de justiça estadunidense expressa a gravidade da situação ao relatar que:

O escopo das condutas criminais conduzidas pelos *hackers* norte-coreanos foi extenso e duradouro, e a amplitude dos crimes que eles cometeram é assombroso. As condutas detalhadas no indiciamento são atos estatais criminosos de uma nação que não parou por nada a fim de extrair vingança e de obter dinheiro para sustentar seu regime. (THREE..., 2021, *on-line*)

Por conseguinte, devido a essa sustentação da máquina de guerra, que pode vir a ser adotada por qualquer país diante de beligerâncias passíveis de serem irrompidas, é evidente a necessidade de tal contexto seja também analisado à luz do Direito Internacional Humanitário, compatibilizando essas ações ao assunto em questão deste estudo.

---

nota-se, então, claramente, que faltam, em especial, os aspectos de unidade de troca irrestrita e de valor referencial.

#### 4 O DIREITO INTERNACIONAL HUMANITÁRIO DIANTE DE CIBERATAQUES NAS GUERRAS VIRTUAIS

Depois de verificar as principais condutas praticadas no âmbito de ciberataques com estrutura estatal e de se constatar que essas ações atuam em um contexto de guerra, resta saber, enfim: como a estrutura atual vigente do DIH atua em toda essa conjuntura e, conseqüentemente, quais problemáticas surgem em meio a uma aplicação de um ordenamento já datado em comparação com os novos parâmetros e diretrizes de interações?

Diante de inovações tecnológicas cada vez mais constantes e surpreendentes, a internet tornou-se um campo tão difícil de se lidar quanto a realidade, mesmo quando ela ainda estava em seu estágio inicial. Então, questionamentos como os apresentados são naturais. Desde sua criação, questões a respeito da legislação e da soberania determinantes sobre a rede (ou se elas sequer existiam) circundavam as discussões, e ainda reflexos pontuais de tais debates permanecem, como a liberdade de expressão, o uso eleitoral da internet, a tributação da economia digital, entre outros (MENDES; ALVES; DONEDA, 2021, *passim*).

Hoje, sabe-se que as conclusões para algumas dessas ponderações foram definidas pouco a pouco, com o próprio desenvolvimento da governança da internet engatinhando a fim de entender o papel da comunidade internacional no cotidiano do ciberespaço. Em face de participações multissetoriais que ditam os rumos desse ambiente tecnológico, definiu-se que os papéis dos governos se dariam, essencialmente, com o objetivo de estabelecer e conservar seu poder e sua autoridade na rede, sobretudo em relação a matérias de políticas públicas, mediante a adoção de mecanismos que os façam prevalecer – entre eles, os ordenamentos jurídicos e demais ferramentas regulatórias (LUCERO, 2011, p. 113-115).

Portanto, é patente que os Estados, em geral, têm prerrogativa de fazer cumprir e sancionar indivíduos com base nas normas vigentes, nacionais ou internacionais, a exemplo daquelas englobadas pelo DIH. Como consequência, as ofensivas virtuais descritas no terceiro capítulo estão sujeitas aos princípios destrinchados no segundo capítulo, quando em contexto de guerra. Diante do raciocínio exposto, é necessário vislumbrar as brechas que se criam frente aos ataques mais recorrentes, de forma que se consiga realizar uma análise crítica sobre se é possível interpretar as normas internacionais, ainda que as adaptando, com base na nova realidade – ou seja, se são suficientes no atual momento – e quais partes podem ser aproveitadas e, a depender do caso, ensejam um maior comprometimento por parte dos atores governamentais do globo.

Observando o *modus operandi* das práticas e estratégias de beligerância cibernética mencionadas e discriminadas, depara-se com quatro problemáticas a serem enfrentadas pelo DIH que não encontram guarida – ao menos, de forma clara – na conjuntura normativa e consuetudinária atual, que são melhor abordadas nos subtópicos a seguir: a indefinição da amplitude do direito à internet como um direito humano; a inexistência de alvos bem definidos e delimitados; o aprofundamento da indefinição de combatentes, em especial no ambiente digital; e a predominância da má-fé como elemento dos instrumentos de guerra ante o anonimato relativo.

#### 4.1 Há direito humano à internet em tempos de guerra?

Reforçando a criação bastante recente da internet e os seus impactos sem precedentes, a rede mundial de computadores se desenvolveu à margem de marcos legais relativamente estáticos, fundamentados em eras passadas da sociedade humana. Se, por um lado, a comunicação é tratada como um direito humano pelo artigo 19 tanto da *Declaração universal dos Direitos Humanos* quanto do *Pacto internacional sobre direitos civis e políticos*, a essencialidade do ciberespaço como meio de comunicação, por outro lado, ficou em xeque, até porque se trata de mais um método comunicativo dentre os demais, sem exercer qualquer exclusividade.

Os artigos 19 de ambos os documentos, de âmbito internacional, exprimem a importância dessa interação e dessa interlocução aos seres humanos, conforme transcrito a seguir:

##### *Declaração universal dos Direitos Humanos*

Art. 19. Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de **procurar, receber e difundir**, sem consideração de fronteiras, **informações e idéias por qualquer meio** de expressão. (OHCHR, [2022], *on-line*, grifou-se)

##### *Pacto internacional sobre direitos civis e políticos*

Art. 19. Parágrafo segundo. Toda pessoa terá direito à liberdade de expressão; esse direito incluirá a **liberdade de procurar, receber e difundir informações e idéias** de qualquer natureza, independentemente de considerações de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou **por qualquer outro meio** de sua escolha. (BRASIL, 1992, *on-line*, grifou-se)

Nesse sentido, Frank La Rue, à época relator especial do OHCHR para a promoção e proteção do direito à liberdade de opinião e de expressão, em seu relatório às Nações Unidas,

argumenta, de maneira acertada, que a indicação em ambas as normas acerca da possibilidade de qualquer método de comunicação ser abarcado pela proteção à opinião e à expressão – isto é, tornando meramente exemplificativo o rol descrito no artigo – teve a intenção de englobar futuras inovações tecnológicas; portanto, a internet estaria inclusa em tal salvaguarda. Além disso, o relator também afirma, com muita clareza, que o espaço cibernético tem o condão de facilitar e possibilitar a aplicação de direitos humanos diversos, sendo, então, um instrumento para aumentar a aplicação e a eficácia da dignidade da pessoa humana (HUMAN RIGHTS COUNCIL, 2011, p. 6-9).

Em concordância a esse entendimento, Valério Mazzuoli (2021, *e-book*) expressa, de maneira contundente, que o acesso à *web* deve ser completamente livre a todos e, aprofundando mais tal posicionamento, caracteriza-o como “núcleo essencial dos direitos humanos”. Ainda, fala que o desrespeito aos direitos comunicativos decorre não só da censura desproporcional à publicação de ideias, mas também do impedimento de alcançar essas comunicações.

Diante dessas exposições, além da consideração de que a inclusão de direitos humanos, em detrimento das restrições a essas normas, é sempre bem-vinda para maximizar a dignidade de todos os indivíduos, a conclusão a que se chega é que o acesso livre à rede é, sim, um direito humano a ser respeitado em seu máximo.

Em contrapartida, não é rara a imposição de limitações à rede mundial de computadores por governos quando enfrentam inquietações sociais. Por exemplo, Mianmar bloqueou o acesso à internet depois de um golpe de Estado e revoltas subsequentes (MILITARES..., 2021, *on-line*). Além disso, o Irã também optou por restringir o alcance do espaço cibernético após o irrompimento de protestos na população a respeito da morte de uma jovem que usou um véu de maneira errada, segundo considerou a chamada “polícia da moralidade” (MOSHTAGHIAN, 2022, *on-line*).

Nota-se, então, que a interpretação dos estudiosos e, de certa forma, de parcela da ONU acaba se contrapondo com a prática oficial dos Estados, o que deixa o entendimento a respeito desse tema em uma espécie de limbo, mesmo em tempos de paz. Desse modo, é mais difícil ainda precisar a garantia dessa comunicação em tempos de guerra, visto que vários direitos humanos são relativizados tanto pela necessidade militar quanto pela imperatividade de proteção aos não combatentes, a exemplo do deslocamento compulsório.

Todavia, é interessante rememorar que a terceira e a quarta *Convenções de Genebra*, sobre prisioneiros de guerra e sobre civis, respectivamente, já previam a salvaguarda de correspondência e, por conseguinte, de interesses de comunicação dos indivíduos envolvidos.

A *III Convenção de Genebra relativa ao tratamento dos prisioneiros de guerra*, em seu artigo 71, garante o envio de correspondências, ainda que com limitação mensal e censura; já a *IV Convenção de Genebra relativa à proteção de civis em tempos de guerra*, em seus artigos 25 e 107, asseguram o envio e o recebimento de notícias familiares e, quanto a civis internados, também de correspondências. Em todos os casos, destaca-se a importância da rapidez e o rechaço à demora injustificada (CICV, 2016, p. 168 e 196-197).

Pode-se até argumentar que, dada a criação recente da internet, o DIH não foi idealizado a cobrir as comunicações pela rede e, portanto, não ensejaria tal proteção. Contudo, diante da integração profunda da tecnologia na sociedade – tornando a *web*, pois, um instrumento já convencional –, da imposição da rapidez nas normas humanitárias – com o artigo 71 supramencionado chegando a falar na utilização de “meios mais rápidos” – e, ainda, do resguardo dos direitos humanos a qualquer método de comunicação, defende-se que a utilização do ciberespaço para esse fim deve ser mantido pelas potências oponentes nos mesmos moldes vigentes para cartas e telegramas, sem a necessidade de qualquer complementação a fim de dar eficácia a essa interpretação.

Em outras palavras, a restrição ao uso da internet para interlocução pessoal, sobretudo familiar, só deve ocorrer em casos excepcionais, no interesse dos próprios prisioneiros, pelo menor tempo possível (assim como acontece com outras formas de correspondência), ou em situações cuja estrutura para o acesso digital esteja indisponível em virtude de consequências bélicas imprevistas ou imperiosas ou de deficiência estrutural prévia, contexto no qual outros meios devem ser empregados, a exemplo das próprias cartas e dos telegramas, visando a atender a esse direito comunicativo.

Portanto, não é mera liberalidade de quem ocupa o território e sobre quem recai essa responsabilidade decidir sobre tal disponibilização nos termos previstos e expostos, permitindo a discricionariedade somente para limitações mensais e censuras, restrição que já é considerada aceitável de acordo com os tratados humanitários. Cabe, então, à comunidade internacional e, ainda mais, às eventuais potências protetoras conclamadas a mediar e intervir na contenda forçar os governos e outras organizações envolvidas a assegurar tanto esse direito quanto a norma vigente no âmbito internacional.

Por outro lado, nas conjunturas que extrapolam os casos previstos – isto é, comunicação não pessoal, a exemplo de acesso livre a notícias de imprensa –, não há determinação que impeça a interdição. Isso ocorre porque, já que essa situação não está expressa no Direito Humanitário e permanece em um campo mais duvidoso, ela consegue adentrar a

restrição relativa de direitos humanos, tendo em vista as medidas excepcionais justificadas por causa de conflitos.

#### **4.2 A inexistência de alvos bem definidos e delimitados nas investidas virtuais**

Demonstrou-se que o DIH tanto normativo quanto consuetudinário estabelece, como um dos pontos basilares, que, em uma disputa, não será qualquer pessoa ou local capaz de ser alvo direto da guerra. Ressalta-se, novamente, a máxima de que o propósito maior para sobrepujar o adversário é derrotar as forças inimigas, somente. Frente às ofensivas virtuais, ainda que se realizem em um espaço cibernético, à parte da realidade, é incontroverso o reconhecimento de que as consequências repercutem no mundo físico, como já se discutiu.

Em meio a essa situação, o segundo capítulo demonstrou, em resumo, que os atos bélicos devem se reservar aos combatentes, evitando os civis à medida do possível. Ainda assim, os não combatentes acabam sujeitos a efeitos tangenciais de ataques considerados proporcionais, cujos alvos sejam militarmente importantes e justificáveis para a campanha.

Retira-se desse raciocínio a lógica de que os ciberataques não podem ter destino incerto e atingir um dispositivo a esmo. Aliás, não só se deve ter um destino certo, como também ele deve ser específico, com um propósito militar bem delineado. É importante, dessa forma, que as máquinas pessoais sejam salvaguardadas de ataques que são motivados simplesmente por pertencerem a uma pessoa cuja nacionalidade corresponda à de um adversário.

Ao considerar, ainda, todo o fundamento de que a interrupção do acesso à internet, mesmo em contexto de guerra, é uma violação dos direitos humanos, justificada apenas por situações imperiosas, argumenta-se, então, que esse tipo de ofensiva deve sofrer escrutínio, cada vez mais intenso, de todos os observadores.

Atualmente, observa-se certo desrespeito a esses parâmetros, tendo em vista que, na prática, se percebe bastante aleatoriedade<sup>21</sup> nos alvos escolhidos, mesmo porque englobam até Estados que não se encontram abertamente em batalha. Essa situação é verificada, em especial, nos ataques DDoS.

Averiguem-se, por exemplo, a derrubada do *site* do MI-5 por parte de *hackers* russos, a inacessibilidade do endereço eletrônico do Parlamento finlandês pretendida também por agressores pró-Kremlin e o roubo de dados de ativistas, acadêmicos e companhias privadas

---

<sup>21</sup> A aleatoriedade aqui referida diz respeito não a uma ausência de um alvo intencionado por parte do atacante, mas se alude à falta de correspondência entre o objetivo escolhido e um eventual ganho militar, sobretudo no tocante às investidas levadas a cabo no campo de guerra do mundo físico, palpável.

relacionados com vários países – incluindo Estados Unidos, Israel, Rússia e Canadá – realizado por ciberespões ligados ao Irã (CSIS, 2022, *on-line*). Embora nenhum desses atos tenha causado danos maiores às pessoas além do incômodo e da frustração, é patente a ausência denexo causal entre tais condutas e ganhos militares proporcionais e justificáveis, os quais são motivos plausíveis para afetar civis, entre outras estruturas e propriedades, ainda mais entre entes que sequer estão em estado de beligerância. Nesse sentido, são atitudes que já são repugnadas em embates, ou seja, que, em uma conjuntura de paz, devem ser obstadas de maneira mais veemente.

Além disso, constatam-se agressões direcionadas a grupos especialmente protegidos pela legislação humanitária. Conforme visto no subtópico 2.3, enfermos, prisioneiros de guerra (quando já rendidos, sob responsabilidade da potência inimiga) e funcionários médicos, sanitários e religiosos possuem proteção superior em relação a outros não combatentes. É importante se lembrar de que esse pessoal, inclusive, tem direito a locais fora da zona de combate, livres de quaisquer ameaças, caso se sigam os ritos determinados pelos tratados. Entretanto, estruturas digitais as quais auxiliam espaços e funcionários alinhados a esses objetivos também acabam atingidos pelos ciberataques, a exemplo do assalto ao sistema de saúde da Groenlândia, cujas consequências resultaram em uma limitação severa aos atendimentos no território (CSIS, 2022, *on-line*).

Nesse mesmo raciocínio, é imprescindível relembrar que é possível se apossar dos controles de infraestruturas básicas de atendimento à população, como o serviço essencial de distribuição de água (NAKASHIMA, 2014, *on-line*). É certo que nem toda investida contra sistemas estatais será proibida, já que se pode focar ferramentas exclusivamente militares e torná-las inoperantes, por exemplo. Porém, é visível a ofensa ao DIH quando se busca afetar os meios de sobrevivência dos habitantes de uma nação adversária. Apesar da tomada de controle e do comando de parada do sistema mencionado não terem ocorrido, a obtenção dos meios para possibilitar tal situação é suficiente para chamar a atenção e colocar todos os governos e as organizações em alerta.

Se ofensivas espaçadas, com impactos menores, já são passíveis de serem repelidos pelo ordenamento em vigor, a investida em servidores e provedores capaz de colocar *off-line* o acesso à rede mundial de computadores como um todo, então, deve ser contestada com mais força. Foi o que ocorreu com franceses, alemães e determinados europeus residentes no centro do continente; afinal, o ataque a provedores de internet é o mais visado, o que, como consequência, coloca em risco a acessibilidade citada (UCRÂNIA, 2022b, *on-line*). Não se deve

esquecer que a falha na *web* também consegue comprometer até os serviços essenciais citados de antemão, razão pela qual causa uma dupla afronta à dignidade da pessoa humana.

Não bastassem todas as preocupações levantadas, consegue-se indicar mais uma, cujo impacto já se chegou a dissertar previamente. Relembre-se de que se demonstrou o prejuízo à democracia quando se interfere em mecanismos eleitorais *on-line*. Aqui, não se refere apenas ao processo em si de votar e contabilizar os votos, mas também à simples derrubada de propagandas, endereços e informações de partidos políticos regularmente constituídos, bem como à adulteração de qualquer dado associado às instituições e aos procedimentos eleitorais.

Nem toda nação beligerante, no entanto, é necessariamente uma democracia, já que qualquer Estado, independentemente da sua organização política, pode se enveredar para um embate. A ênfase nas instituições democráticas se deve por ser esse o modelo adotado pelo Brasil e por ser o estilo de organização política escorada em múltiplos entes e processos, de forma que possuem alvos mais amplos. Contudo, tal inquietação recai, do mesmo modo, a outras espécies de governo, visto que se vislumbra a necessidade de proteção não somente aos princípios democráticos, como também à autodeterminação dos povos. Nessa perspectiva, destaque-se que ataques cibernéticos cujo objetivo seja minar a estrutura de poder existente, em um estilo de golpe de Estado, deve ser vedada de maneira especial, o que, infelizmente, ainda não acontece nos ditames atuais do DIH.

É bem verdade que é bastante árduo definir as ofensivas como atos de guerra, porque diversas condutas são executadas por criminosos com intuítos de ganhos individuais, sem ter uma máquina estatal por trás. Contudo, de acordo com as discussões já travadas, é notório que determinadas atitudes possuem, sim, um esforço nacional as impulsionando. Devido a uma rastreabilidade ainda falha, os países se escondem no anonimato relativo e brigam silenciosamente entre si.

Em resposta às problemáticas apontadas, mostram-se necessárias várias melhorias na condução das soluções desse assunto. Em primeiro lugar, é imprescindível diferenciar, na prática, justamente as investidas particulares e as patrocinadas por Estados ou por entes paraestatais. Apesar de se identificar o alinhamento ou a ideologia por trás dos ataques cibernéticos, ou mesmo a região geográfica aproximada do dispositivo de onde partiu a ordem central, pouco se sabe e se define com certeza acerca da estrutura e do comando que incentivam, financiam, orientam ou coordenam essa espécie de organização. Trata-se de uma perspectiva bastante problemática, inclusive, já que tal distinção é um aspecto determinante a respeito dos indivíduos, das empresas ou dos governos que serão acusados, bem como das espécies de responsabilização que incidirão sobre os eventuais inculpados.



Embora haja dificuldade de rastreamento, verifica-se que as nações interessadas – direta ou indiretamente – na continuidade dessas atuações, em geral, contrárias ao DIH se utilizam de tal obstáculo com vistas a se evadir. Tendo isso em mente, urge à comunidade internacional iniciar debates ligados à ampliação da responsabilidade estatal, de maneira que se consiga exercer pressão para a presença de uma investigação compulsória a cada ataque, com andamento adequado, ainda que se desconfie de investida cibernética de interesse particular, atrapalhando o funcionamento livre desse tipo de mancomunação incentivada por governos.

Ademais, mesmo que a interpretação das normas humanitárias já penda ao entendimento de que os ciberataques não devam ter destinação descomprometida, os Estados soberanos devem buscar meios, mediante força legal ou política, de esclarecer que o ordenamento jurídico internacional se aplica também às condutas bélicas no âmbito do campo de batalha digital. Isso, além de alinhar a aplicação do DIH, serve igualmente com o objetivo de repudiar a situação problemática a qual se vivencia, em outra espécie de pressão para obstá-la cada vez mais.

### **4.3 A indefinição de combatente no âmbito virtual**

Na discussão a respeito do princípio da distinção entre combatentes e não combatentes, já se afirmou a dificuldade e, por consequência, a existência de uma zona cinzenta de compreensão desses conceitos quando distantes de situações bem delineadas<sup>22</sup>. Diante, então, de um recrutamento para a frente virtual, essa definição fica mais distante de ser pacificada.

A maior complicação advém da conclamação pública sem precedentes recém-adotada pela Ucrânia, com o intento de se formar uma estrutura similar a um exército de *hackers* em meio à população civil (CONGER; SATARIANO, 2022, *on-line*). É importante destacar que essa mobilização partiu do próprio governo ucraniano, o qual, inclusive, distribuiu tarefas e comandos para os integrantes desse grupo de especialistas em tecnologia da informação executarem (UCRÂNIA, 2022a, *on-line*).

Esse tipo de ato possui o condão de levar ao limite a tolerância dos países oponentes quanto à configuração dos combatentes e, por conseguinte, aumentar a quantidade de indivíduos contra os quais podem retaliar. Em razão disso, trata-se de um contexto que carrega consigo bastante preocupação.

---

<sup>22</sup> Nesse sentido, conferir o estudo da definição de combatentes por parte do CICV ([2022]e, *on-line*) e as próprias *Convenções de Genebra* (CICV, 2016, *passim*), que levam a essa dificuldade de conceituação, embora consigam englobar, na definição, os partícipes mais visíveis na relação de combate.

O *Protocolo adicional I às Convenções de Genebra relativo à proteção das vítimas dos conflitos armados internacionais* assevera, de forma clara, no parágrafo terceiro de seu artigo 51, que “Os civis gozam da proteção concedida pela presente Seção [contra os perigos resultantes de operações militares], **salvo se participarem diretamente nas hostilidades** e enquanto durar essa participação” (CICV, 2017, p. 39, grifou-se).

Logo, ao considerar as ofensivas virtuais como operações bélicas, conforme se advoga para maximizar as garantias gerais à dignidade da pessoa humana em face da população mundial, atacar a estrutura adversária consoante a convocação do governo ucraniano, ou qualquer outro ente estatal ou similar, traria diversos civis e até demais grupos especialmente protegidos à condição de combatentes. Os resultados disso são a grande possibilidade de aumento de vítimas da guerra, a pulverização de alvos ao longo do território – visto que, provavelmente, os especialistas em TI estarão dispersos pela região, a depender do domicílio e do local da estação de trabalho –, bem como a precarização dos partícipes das hostilidades, pois o envolvimento deles se dá sem o suporte e a disposição direta das Forças Armadas, o que os deixa, de certo modo, à própria sorte. Torna-se evidente que tal contexto mina, em demasia, a proteção ensejada pelo DIH, sendo o oposto do que se espera.

Outra consequência jaz na dispersão desses agentes que atuam virtualmente nos embates, já que eles se encontram esparsos não só no território em conflito, como também em diversos Estados que sequer, *a priori*, participam da contenda ou mesmo coadunam com os ciberataques postos em prática por um nacional ou residente. Essa realidade, por enquanto, é ignorada, mas tem potencial de mudar a dinâmica de relações internacionais em hostilidades, sobretudo em caso de agravamento da relativa paz mundial e de uso crescente desse tipo de recurso no futuro. No mínimo, se mantida a diplomacia e a ausência de maiores deteriorações inter-relacionais, abre-se margem para o enfraquecimento do DIH, conforme exposto.

Portanto, defende-se que a resposta mais segura é que essa mobilização deva ser oficial, com integração dos voluntários aos quadros das Forças Armadas, de forma a melhorar a própria segurança dos envolvidos em caso de maiores acirramentos (e não sejam alvos à própria sorte) e de maneira a garantir e controlar o alinhamento de tais partícipes às normas internacionais. Veta-se, assim, a convocação geral e irrestrita, sob pena de desrespeito aos ditames do Direito Humanitário.

Ademais, como a normativa internacional humanitária ora vigente não acompanha essa realidade, recomenda-se um retorno às discussões sob a tutela da ONU. É notória a necessidade de atualização, com a devida complementação, da legislação global, de modo a considerar essa nova realidade digital.

#### 4.4 A predominância da má-fé nas ofensivas bélicas *on-line*

Por fim, adentra-se a última das principais problemáticas decorrentes dessa nova realidade mundial: a desconsideração da boa-fé nas investidas em ambiente cibernético. Aqui, não se fala da falta de vontade na interpretação do DIH, conforme já apontado nos tópicos anteriores, mas se debruça, sim, sobre a má-fé na atuação ou mesmo na construção da conduta, tendo-se consciência disso.

O principal ataque cibernético que se adéqua a essa situação é o roubo de valores para financiar Forças Armadas e esforços beligerantes afins, de acordo com as discussões do subtópico 3.4. Comportamentos criminosos incentivados ou patrocinados por Estados não são esperados por nenhum governo, até porque fogem de toda a ideia de cordialidade das relações internacionais. Não só isso, como também há uma verdadeira subversão do sistema financeiro e bancário, em especial.

Nesse ponto de vista, destrinchando melhor a atuação dos cibercriminosos, eles enganam o mecanismo de transferência ao fazê-lo acreditar que aquela movimentação seria o desejo do titular das quantias, deturpando a manifestação livre da vontade deste. Em outras palavras, o sistema crê estar respeitando a liberdade econômica de seu usuário.

Retorna-se, então, aos conceitos de boa-fé objetiva e subjetiva, de acordo com os apontamentos de Judith Martins Costa (2018, p. 279-283). Vislumbra-se a ofensa ao aspecto objetivo da boa-fé na medida em que o crime não é o padrão comportamental esperado na sociedade, tanto que os ordenamentos jurídicos ao redor do mundo preveem sanções, inclusive a segregação do indivíduo que compactue com o dano aos bens jurídicos tutelados. No tocante ao aspecto subjetivo, a agressão a ele advém, justamente, da crença de se respeitar o direito alheio de liberdade de movimentação financeira.

Infelizmente, há pouco a se fazer em relação a essa problemática, além de aperfeiçoar a segurança de tais recursos. Isso porque a questão esbarra em uma das maiores deficiências que afeta o DIH: a falta de vontade de respeitar as normas humanitárias somada à ausência de meios para impô-las (CICV, [2022]c, *on-line*). Como abordado, esse método de apropriação de dinheiro é levado a cabo pela Coreia do Norte, sobretudo, e já há uma ampla pressão sob a perspectiva sancionatória no país, sendo que não há quaisquer prognósticos que indiquem o arrefecimento de tal prática; talvez, as sanções até a motivem mais.

Por outro lado, saindo do âmbito de apropriação indevida de financiamento ao esforço de guerra e se direcionando ao apoderamento de informações e dados sensíveis, conduta parecida, mas com enfoque em ativos distintos, nota-se um contexto duvidoso, o qual necessita

de maiores esclarecimentos por parte daqueles que constroem a legislação e o entendimento internacionais. Essa incerteza paira em razão da relativa aceitação da utilização da espionagem<sup>23</sup>, tendo em vista que as convenções não a apontam como ilícito e, dessa forma, é considerada um instrumento de guerra válido.

Claro que um espião, se descoberto, se sujeitará a pesadas punições do país prejudicado. Aliás, o espreitador possui salvaguardas ainda mais restritas que combatentes ostensivos, apesar de aquele não causar nenhuma lesão direta como estes. Por isso, a nação a quem o espião serve, muitas vezes, tenta lhe atribuir cobertura diplomática para que ele receba certas imunidades e passe despercebido mais facilmente (CONDEIXA, 2015, p. 21-25).

Com isso, por analogia, embora englobe a má-fé por meio de *e-mails* mal-intencionados, por exemplo, os ciberataques que se destinam exclusivamente à obtenção de informações e dados são permitidos. Trata-se de uma exceção estabelecida pelo costume e, mesmo que não escrita, é considerada clara por todos os atores do cenário global.

Todavia, é essencial ressaltar que esse entendimento evidente vigora entre entes em combate. A aplicação dessa interpretação analógica quando configurada a espionagem entre Estados com relações de paz plenamente estabelecidas é duvidosa e requer maior atenção da comunidade internacional, sobretudo porque existem, sim, diversos registros de tais roubos nessa conjuntura pacífica, a exemplo de Estados Unidos e China (CSIS, 2022, *on-line*).

Advoga-se pela possibilidade de uso desse mecanismo apenas quando essa obtenção de dados acontece sem a utilização de vítimas comprometidas, segundo apontamento de Munish Sharma (2017, p. 66-67). A posição referenciada é a que melhor maximiza o respeito à boa-fé, visto que se evita a enganação de terceiros no processo de preparação prévia ao ataque. Contudo, reconhece-se que é um entendimento difícil de ser adotado, pela restrição que ocorrerá nas agências de inteligência, sobre as quais vários atores internacionais se apoiam.

---

<sup>23</sup> O roubo de valores não é considerado espionagem, motivo pelo qual essa prática não pode ser associada ao contexto duvidoso mencionado. Nos conceitos desenvolvidos que determinam os atributos de espiões, é claro o objeto da espionagem: informações, dados e serviço de inteligência em geral, ou seja, nada se diz sobre a obtenção de moeda, ainda mais em grandes montantes (CONDEIXA, 2015, p. 21-23).

## 5 CONSIDERAÇÕES FINAIS

Com base em toda a conjuntura descrita e em todos os argumentos expostos, conclui-se que o Direito Internacional Humanitário é um conjunto de normas que, junto com os Direitos Humanos, ascendeu no cenário internacional para proteger, sobretudo, a dignidade da pessoa humana. O DIH, em particular, é utilizado em contextos de guerra e, por salvaguardar um bem jurídico tão caro à sociedade pós-Segunda Guerra Mundial, deve ter seus princípios aplicados e maximizados tanto quanto possível.

A fim de proceder a essa aplicação, é necessário compreender, justamente, quais são os princípios norteadores da atuação do DIH. Em primeiro lugar, tem-se a dignidade da pessoa humana, conceituada como um âmbito físico e moral garantido a todos os seres humanos, incluindo as condições necessárias para que se atinja essa garantia. Por isso, ela se associa com diversos outros valores relacionados com a liberdade dos indivíduos.

Em segundo lugar, deve-se ter em mente a necessária distinção entre combatentes e não combatentes, de modo que se consiga determinar adequadamente os alvos válidos em meio aos confrontos. Assim, reconhece-se a existência de uma parcela da população que não deve ser visada diretamente, isto é, os civis. Da mesma forma, acorda-se a existência de pessoas especialmente protegidas, as quais têm direito, sem qualquer embaraço, a se estabelecerem em uma zona fora do confronto, livre de ataques; nesse quesito, ainda que pertençam às Forças Armadas, adentram-se enfermos, náufragos, prisioneiros de guerra, equipes sanitárias e humanitárias e pessoal religioso, além das propriedades e espaços de deslocamento intrínsecos ao objetivo deles.

Dentro desse raciocínio, não são só estruturas essenciais e pessoas que detêm proteção contra determinados tipos de ofensiva. Localidades indefesas também são albergadas pelo resguardo contra ataques desproporcionais e despropositados, já que patrimônios históricos, culturais e naturais são um direito da humanidade.

Chega-se, ainda, ao princípio da vedação a métodos bélicos cruéis e desproporcionais. Parte-se do pressuposto de que mesmo combatentes têm a guarida da dignidade da pessoa humana, ainda que mais relativizada em comparação com o restante da população.

Por último, estabelece-se a boa-fé como norteadora dos comportamentos e das estratégias de batalha, de maneira a evitar a perfídia como instrumento da conjuntura de beligerância. Apesar disso, estão liberadas as artimanhas de guerra, como camuflagem de soldados, espionagem, emboscadas, informações falsas e operações simuladas.

Tendo em mente todo esse arcabouço principiológico delimitado, verifica-se que o surgimento da internet criou um ambiente no qual a aplicação das normas e, como consequência, dos princípios do DIH se tornou desafiadora. Pela novidade de uma realidade à parte do mundo físico, as condutas no cenário cibernético cresceram, em um primeiro momento, com a ausência de governança e com muitas questões em aberto.

Contudo, diante do crescimento da conexão entre ciberespaço e realidade palpável, as práticas cibernéticas começaram a afetar bastante o mundo material. Assim, proliferaram-se os ciberataques e, paulatinamente, tornaram-se instrumentos da atividade bélica e, portanto, atos de guerra. Isso ficou evidente quando as estruturas militares e o financiamento estatal incorporaram e incentivaram essa conduta entre seus subordinados ou apoiadores.

Os principais tipos de ofensivas cibernéticas são a derrubada de servidores e de provedores da internet, em especial pelo método DDoS, o roubo de informações e de dados nacionais sensíveis e a apropriação indevida de dinheiro em prol das Forças Armadas do país a que o *hacker* é alinhado.

A ênfase em deixar *off-line* os servidores e os provedores que servem o adversário atrapalha os serviços e as comunicações do país. Além disso, causam frustração e incômodo na população e deixam uma mensagem de protesto, ambos capazes de minar o apoio dos cidadãos ao governo e à operação de guerra, embora possam acirrar ainda mais os ânimos. Uma problemática maior aparece quando a inoperância afeta o sistema eleitoral em democracias, com o desaparecimento, mesmo que temporário, de propagandas e informações político-partidárias, por exemplo. Esse comportamento fere a isonomia e abala os princípios democráticos.

Quanto ao contexto de obtenção de dados sensíveis, há o espalhamento de programas maliciosos que conseguem angariar conhecimentos de estruturas, armas e tecnologias importantes à nação oponente. Ainda, é possível tomar o controle de sistemas, inclusive aqueles de valia básica aos seres humanos, como a distribuição de água.

Finalmente, no tocante à apropriação de quantias em favor dos esforços bélicos, há movimentações de vultosas quantias – seja de dinheiro transacionado digitalmente, seja de criptomoeda – aos cofres públicos dos Estados que incentivam as investidas. Os valores são utilizados para manter as atividades militares e obter outras formas de patrimônio, o que vira uma espécie de ciclo vicioso.

Logo, diante de ciberataques que se favorecem em meio à atuação quase irrestrita por ocorrerem na brecha do âmbito virtual pouco normatizado, urge se empenhar e se concentrar na interpretação e na aplicação do DIH a fim de atualizá-lo frente a essa conjuntura.

Para isso, é necessário identificar que o abuso mais evidente da conduta dos *hackers* e dos Estados apoiadores provém de quatro ofensas notáveis às normas humanitárias internacionais: a inobservância da internet como um direito humano comunicativo; a inexistência de definição ou delimitação nos alvos dos ciberataques; a convocação indevida de civis com o conseqüente aumento exacerbado de combatentes; e a predominância da má-fé em diversas ofensivas.

Ao visar à derrubada de servidores e de provedores, os *hackers* têm o potencial de restringir, de maneira substancial, o acesso à internet. Contudo, entende-se que o ciberespaço é um instrumento de comunicação albergado pelos Direitos Humanos, motivo pelo qual não cabe quaisquer tentativas de suprimir esse direito, de modo total, quando utilizado para interlocução pessoal, a não ser em casos extremos, com opção suplementar de envio de cartas e telegramas. Não obstante, tal restrição não é só indevidamente adotada por adversários, mas também pelos próprios governos em momentos de inquietação social.

Com isso, defende-se que o DIH é claro nesse quesito e possui aplicabilidade imediata. É necessária, então, a pressão de nações e organizações para priorizar o cumprimento das normativas internacionais e, por conseguinte, vigorar e normalizar tal direito basilar.

Além disso, em que pese a demonstrada proteção atribuída a civis, a propriedades e patrimônios indefesos e a outros grupos sob guarida especial, as ofensivas virtuais atingem alvos de forma indiscriminada, sem respeitar as diretrizes estabelecidas pelo DIH. Tais agressões alcançam estruturas de saúde e de saneamento básico, dispositivos de civis e endereços eletrônicos alheios às forças militares. É visível a falta de justa causa entre o ataque e o ganho com o resultado, sobretudo na frente de batalha material.

Devido à rastreabilidade ainda falha, responsabilizar os Estados é uma tarefa árdua, visto que é bastante difícil identificar quais ataques foram praticados por criminosos com intuítos de ganhos individuais e quais foram efetivamente perpetrados pelas entidades estatais. Nesse sentido, advoga-se pela obrigação dos governos em investigar, de modo adequado e compulsório, as ofensivas cujas ordens de execução partiram de seu respectivo território, sob pena de responsabilização, nesse caso, pela omissão. Objetiva-se dificultar o encobrimento de atividades bélicas cibernéticas que infrinjam o Direito Humanitário.

Considerando também que os ciberataques com alvos indiscriminados são recorrentes, a comunidade internacional deve se reunir a fim de complementar os tratados já existentes. Busca-se, assim, uma maior segurança jurídica e maior clareza com vistas a pressionar as nações a adequar seu *modus operandi* de agressões digitais.

Outro problema irrompido pelas novas modalidades de estratégias de batalha é a convocação de civis para trabalhar, em suas estações de trabalho particulares, nas investidas

digitais. Sob coordenação estatal, com participação direta no conflito, essa situação dá margem para considerar essa parcela de especialistas como combatentes. Com isso, esses indivíduos ficam aptos a sofrer embates diretos por parte do grupo adversário.

Não bastasse a referida constatação, o exército de *hackers* pulverizaria os alvos ao longo de todo o território nacional e internacional. Desse modo, uma maior área se sujeita, inclusive, a bombardeios físicos, já que eliminar os componentes do esforço de guerra cibernético se torna um objetivo militar da outra parte. Ademais, como alguns atacantes podem residir em países alheios ao conflito, tem-se o condão de deteriorar diversas relações pacíficas entre nações do globo. Portanto, trata-se de razões suficientes para estabelecer em uma nova norma a proibição desse tipo de conclamação voluntária à luta virtual e, caso ela ocorra, seja com integração ao quadro das Forças Armadas do respectivo Estado.

Para finalizar, os ciberataques também não estão considerando a observância da boa-fé. A prática de crime contra civis, com envio de *e-mails* e outras ferramentas enganosas, além de ignorar a proteção destinada a esse grupo e ferir a boa-fé objetiva por não ser o padrão social esperado e adequado, subverte os sistemas financeiro e bancário, que acreditam estarem obedecendo à vontade e à liberdade econômica de um usuário legítimo, atingindo a boa-fé subjetiva. Trata-se de flagrante desrespeito a tal princípio do DIH, que deve ser rechaçado por todas as nações, mantendo-se pressões sancionatórias a países que se utilizam dessa conduta.

Continuando a lógica, a espionagem poderia ser enquadrada como violação do DIH, já que também usa, de certo modo, a má-fé para angariar informações e vantagens. Todavia, esclarece-se que os atores internacionais consideram tal recurso como exceção e o permitem como ferramenta de guerra. Como a espionagem é igualmente adotada em tempos pacíficos, o que já não é um uso incontroverso, é de bom tom que os mesmos atores se reúnam para esclarecer como esse contexto se situa em tempos de paz. Por atividades de inteligência serem parte do cotidiano, sustenta-se o entendimento de que, ao menos, se proíba o uso de vítimas comprometidas, deixando os demais métodos como válidos.

Adotando-se os posicionamentos e as soluções indicadas, a aplicação do DIH se torna mais uniforme e clara. Além disso, as sugestões maximizam a proteção dos Direitos Humanos e da dignidade da pessoa humana, sobretudo por observar os princípios essenciais que a comunidade internacional buscou preservar ao estabelecer os tratados humanitários. Frise-se a recomendação de mais debates sob a tutela da ONU, com o objetivo de normatizar novas medidas diante dessa realidade inovadora e disruptiva, já que, assim, se conseguem adotar ações mais impositivas.



## REFERÊNCIAS

ARMS CONTROL ASSOCIATION. **UN Security Council resolutions on North Korea**. 2022. Disponível em: <https://www.armscontrol.org/factsheets/UN-Security-Council-Resolutions-on-North-Korea>. Acesso em: 7 nov. 2022.

ATOMIC ARCHIVE. **Immediate aftermath**. [20 set. 2022]. Disponível em: <https://www.atomicarchive.com/history/atomic-bombing/hiroshima/page-9.html>. Acesso em: 20 set. 2022.

BENNETT, Annabelle; GRANATA, Sam. Quando o Direito Internacional Privado e a Lei da Propriedade Intelectual se encontram. **Revista da OMPI**, [Geneva], n. 6, Dec. 2019. Disponível em: [https://www.wipo.int/wipo\\_magazine/pt/2019/06/article\\_0007.html](https://www.wipo.int/wipo_magazine/pt/2019/06/article_0007.html). Acesso em: 11 out. 2022.

BIERNATH, André. Quais são os efeitos da radiação no corpo? **Veja Saúde**, [S. l.], 4 maio 2020. Disponível em: <https://saude.abril.com.br/medicina/efeitos-radiacao-corpo/>. Acesso em: 20 set. 2022.

BITENCOURT, Cezar R. **Tratado de Direito Penal: parte geral – arts. 1º a 120**. 28. ed. São Paulo: SaraivaJur, 2022. v. 1. *E-book*.

BOOM, Daniel. North Korea's crypto hackers are paving the road to nuclear armageddon. **CNET**, [S. l.], Oct. 9, 2022. Disponível em: <https://www.cnet.com/culture/features/north-koreas-crypto-hackers-are-paving-the-road-to-nuclear-armageddon/>. Acesso em: 8 nov. 2022.

BRAGA, Márcio B. **Princípios de economia: abordagem didática e multidisciplinar**. São Paulo: Atlas, 2019. *E-book*.

BRASIL. **Decreto nº 592, de 6 de julho de 1992**. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Brasília, DF: Presidência da República, 1992. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/decreto/1990-1994/d0592.htm](http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm). Acesso em: 12 nov. 2022.

CAESAR, Ed. The incredible rise of North Korea's hacking army. **The New Yorker**, [S. l.], Apr. 19, 2021. Disponível em: <https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army>. Acesso em: 3 out. 2022.

CIA. North Korea. *In*: CIA. **The world factbook**. Nov. 3, 2022. Disponível em: <https://www.cia.gov/the-world-factbook/countries/korea-north/summaries>. Acesso em: 8 nov. 2022.

CICV. **A guerra e o direito**. [23 jun. 2022]. Disponível em: <https://www.icrc.org/pt/guerra-e-o-direito>. Acesso em: 23 jun. 2022.

CICV. **Até mesmo as guerras têm limites**. [23 jun. 2022]. Disponível em: <https://www.icrc.org/pt/normas-da-guerra>. Acesso em: 23 jun. 2022.

CICV. **Convenção de 1972 sobre a proibição de armas bacteriológicas e sobre sua destruição**. 23 abr. 2004. Disponível em: <https://www.icrc.org/pt/doc/resources/documents/misc/5yblc9.htm>. Acesso em: 22 set. 2022.

CICV. **Convenção de 1993 sobre a proibição das armas químicas e sua destruição.**

23 abr. 2004. Disponível em:

<https://www.icrc.org/pt/doc/resources/documents/misc/5yblcz.htm>. Acesso em: 22 set. 2022.

CICV. **Convenções de Genebra de 12 de agosto de 1949.** Genebra: CICV, 2016.

CICV. **DIH consuetudinário:** normas: introdução. [28 jun. 2022]. Disponível em: [https://ihl-databases.icrc.org/customary-ihl/por/docs/v1\\_rul\\_in#Fn\\_9983C1FD\\_00001](https://ihl-databases.icrc.org/customary-ihl/por/docs/v1_rul_in#Fn_9983C1FD_00001). Acesso em: 28 jun. 2022.

CICV. **DIH consuetudinário:** normas: norma 24. [29 ago. 2022]. Disponível em: [https://ihl-databases.icrc.org/customary-ihl/por/docs/v1\\_rul\\_rule24](https://ihl-databases.icrc.org/customary-ihl/por/docs/v1_rul_rule24). Acesso em: 29 ago. 2022.

CICV. **DIH consuetudinário:** normas: norma 3. [29 ago. 2022]. Disponível em: [https://ihl-databases.icrc.org/customary-ihl/por/docs/v1\\_rul\\_rule3](https://ihl-databases.icrc.org/customary-ihl/por/docs/v1_rul_rule3). Acesso em: 29 ago. 2022.

CICV. **DIH consuetudinário:** normas: norma 53. [23 set. 2022]. Disponível em: [https://ihl-databases.icrc.org/customary-ihl/por/docs/v1\\_rul\\_rule53](https://ihl-databases.icrc.org/customary-ihl/por/docs/v1_rul_rule53). Acesso em: 22 set. 2022.

CICV. **DIH consuetudinário:** normas: norma 65. [26 set. 2022]. Disponível em: [https://ihl-databases.icrc.org/customary-ihl/por/docs/v1\\_rul\\_rule65](https://ihl-databases.icrc.org/customary-ihl/por/docs/v1_rul_rule65). Acesso em: 26 set. 2022.

CICV. **DIH consuetudinário:** normas: norma 66. [22 set. 2022]. Disponível em: [https://ihl-databases.icrc.org/customary-ihl/por/docs/v1\\_rul\\_rule66](https://ihl-databases.icrc.org/customary-ihl/por/docs/v1_rul_rule66). Acesso em: 22 set. 2022.

CICV. **DIH consuetudinário:** normas: norma 73. [22 set. 2022]. Disponível em: [https://ihl-databases.icrc.org/customary-ihl/por/docs/v1\\_rul\\_rule73](https://ihl-databases.icrc.org/customary-ihl/por/docs/v1_rul_rule73). Acesso em: 22 set. 2022.

CICV. **Protocolos adicionais às Convenções de Genebra de 12 de agosto de 1949.**

Genebra: CICV, 2017.

CISA. **FASTCash 2.0:** North Korea's BeagleBoyz robbing banks. Aug. 26, 2020. Disponível em: <https://www.cisa.gov/uscert/ncas/alerts/aa20-239a>. Acesso em: 8 nov. 2022.

CISA. **Stop ransomware.** [7 nov. 2022]. Disponível em:

<https://www.cisa.gov/stopransomware>. Acesso em: 7 nov. 2022.

CONDEIXA, Fábio de M. S. P. Espionagem e Direito. **Revista Brasileira de Inteligência**, Brasília, DF, n. 10, dez. 2015, p. 21-40. Disponível em:

<https://rbi.enap.gov.br/index.php/RBI/article/view/123/99>. Acesso em: 11 out. 2022.

CONGER, Kate; SATARIANO, Adam. Hackers voluntários atuam em conflito na Ucrânia sem ninguém no comando. **Folha de S.Paulo**, Nova York, 4 mar. 2022. Disponível em: <https://www1.folha.uol.com.br/mercado/2022/03/hackers-voluntarios-atuam-em-conflito-na-ucrania-sem-ninguem-no-comando.shtml>. Acesso em: 3 out. 2022.

COSSETTI, Melissa C. O que é NFT? Entenda a relação dos *tokens* com jogos, arte e mais. **Tecnoblog**, [S. l., 10 mar. 2013]. Disponível em: <https://tecnoblog.net/responde/o-que-e-nft-non-fungible-tokens/>. Acesso em: 8 nov. 2022.

COSTA, Judith M. **A boa-fé no direito privado**. 2. ed. São Paulo: SaraivaJur, 2018. *E-book*.

COULANGES, Numa-Denys F. de. **A cidade antiga**: um estudo da religião, do direito e das instituições da Grécia e Roma. São Paulo: Montecristo Editora, 2021. *E-book*.

CSIS. **Significant cyber incidents**. 2022. Disponível em: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incident>. Acesso em: 6 out. 2022.

CSRC. **Glossary**: phishing. [7 nov. 2022]. Disponível em: <https://csrc.nist.gov/glossary/term/phishing>. Acesso em: 7 nov. 2022.

FRANKEL, Joseph. War. *In*: ENCYCLOPAEDIA Britannica. Aug. 24, 2022. Disponível em: <https://www.britannica.com/topic/war>. Acesso em: 28 set. 2022.

GOMES, David F. L. Sobre o conceito moderno de Constituição: proposta de uma nova abordagem. **Cadernos do Programa de Pós-Graduação em Direito/UFRGS**, Porto Alegre, v. 13, n. 1, 2018, p. 124-148. Disponível em: <https://seer.ufrgs.br/index.php/ppgdir/article/view/77922/49962>. Acesso em: 22 jun. 2022.

GORI, Umberto. Guerra. *In*: BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco (org.). **Dicionário de Política**. 11. ed. Brasília, DF: Editora UnB, 1998. p. 571-577.

GREENEMEIER, Larry. How hackers take down web sites. **Scientific American**, [S. l.], Feb. 11, 2014. Disponível em: <https://blogs.scientificamerican.com/observations/how-hackers-take-down-web-sites-video/>. Acesso em: 3 out. 2022.

GROTIUS, Hugo. **The rights of war and peace**. New York: M. Walter Dunne, 1901. Disponível em: [http://www.dominiopublico.gov.br/download/texto/0138\\_Bk.pdf](http://www.dominiopublico.gov.br/download/texto/0138_Bk.pdf). Acesso em: 20 nov. 2022.

GUIMARÃES, Bernardo; GONÇALVES, Carlos. **Introdução à Economia**. 2. ed. Rio de Janeiro: Elsevier, 2017. *E-book*.

HENCKAERTS, Jean-Marie; DOSWALD-BECK, Louise. **Direito Humanitário Internacional consuetudinário**. [Genebra]: CICV, [2017].

HOSCH, William L. Malware. *In*: ENCYCLOPAEDIA Britannica. Sept. 30, 2022. Disponível em: <https://www.britannica.com/technology/malware>. Acesso em: 6 out. 2022.

HUMAN RIGHTS COUNCIL. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue**. 16 May 2011. Disponível em: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement>. Acesso em: 12 nov. 2022.

ICJ. **Legality of the threat or use of nuclear weapons (advisory opinion)**. 8 July 1996. Disponível em: <https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf>. Acesso em: 20 set. 2022.

LONDON, Brad. Entenda por que a guerra entre as Coreias não terminou em 1953. **CNN Brasil**, Hong Kong, 30 dez. 2021. Disponível em:

<https://www.cnnbrasil.com.br/internacional/entenda-por-que-a-guerra-entre-as-coreias-nao-terminou-em-1953/>. Acesso em: 8 nov. 2022.

LUCERO, Everton. **Governança da internet**. Brasília, DF: FUNAG, 2011.

MACHADO, Raquel C. R. **Direito Eleitoral**. 2. ed. rev., atual. e ampl. São Paulo: Atlas, 2018. *E-book*.

MACHADO, Simone. Metaverso: como participar do “futuro da tecnologia”? Saiba tudo. **Tilt Uol**, [S. l.], 28 abr. 2022. Disponível em: <https://www.uol.com.br/tilt/faq/metaverso-o-que-e-como-entrar-e-mais.htm>. Acesso em: 22 nov. 2022.

MARQUES JÚNIOR, William Paiva. Reflexos do Direito Internacional dos Direitos Humanos na proteção aos refugiados: análise do caso brasileiro. *In*: TOLEDO, Cláudia M. Q. de; ARNAUD, Wanda M. de L.; CANOTILHO, Mariana R. (coord.). **[Coletânea do] VII Encontro Internacional do CONPEDI: Direito Internacional dos Direitos Humanos I**. Florianópolis: CONPEDI, 2017.

MAXIMILIANO, Carlos. **Hermenêutica e aplicação do Direito**. 23. ed. Rio de Janeiro: Forense, 2021. *E-book*. Coleção Fora de Série.

MAZEBOLT TECHNOLOGIES. 5 reasons DDoS attacks are the biggest threat to governments worldwide. **[Blogue de] MazeBolt Technologies**, Ramat Gan, Dec. 9, 2022. Disponível em: <https://blog.mazebolt.com/reasons-why-ddos-attacks-governments>. Acesso em: 9 out. 2022.

MAZZUOLI, Valerio de O. Direitos comunicativos como direitos humanos: abrangência, limites, acesso à Internet e direito ao esquecimento. *In*: MENDES, Laura S.; ALVES, Sérgio G.; DONEDA, Danilo (coord.). **Internet & regulação**. São Paulo: SaraivaJur, 2021. Série IDP – Linha Pesquisa Acadêmica.

MENDES, Gilmar F.; BRANCO, Paulo G. G. **Curso de direito constitucional**. 17. ed. São Paulo: SaraivaJur, 2022. *E-book*.

MENDES, Laura S.; ALVES, Sérgio G.; DONEDA, Danilo (coord.). **Internet & regulação**. São Paulo: SaraivaJur, 2021. Série IDP – Linha Pesquisa Acadêmica.

MILITARES de Mianmar bloqueiam internet após golpe de Estado no país. **Veja**, [S. l.], 6 fev. 2021. Disponível em: <https://veja.abril.com.br/mundo/militares-de-myanmar-bloqueiam-internet-apos-golpe-de-estado-no-pais/>. Acesso em: 12 nov. 2022.

MINISTRY OF FOREIGN AFFAIRS OF JAPAN. **Perguntas & respostas sobre o território japonês**. [8 nov. 2022]. Disponível em: <https://www.br.emb-japan.go.jp/territory/question-and-answer.html#q4>. Acesso em: 8 nov. 2022.

MORGENTHAU, Hans. **A política entre as nações: a luta pelo poder e pela paz**. Brasília, DF: Editora UnB: IPRI, 2003.

MOSHTAGHIAN, Artemis *et al.* Irã restringe internet em meio a protestos por morte de jovem por mau uso de véu. **CNN Brasil**, [S. l.], 24 set. 2022. Disponível em: <https://www.cnnbrasil.com.br/internacional/ira-restringe-internet-em-meio-a-protestos-por-morte-de-jovem-por-mau-uso-de-veu/>. Acesso em: 12 nov. 2022.

NAKASHIMA, Ellen. Foreign powers steal data on critical U.S. infrastructure, NSA chief says. **The Washington Post**, [S. l.], Nov. 20, 2014. Disponível em: [https://www.washingtonpost.com/world/national-security/nsa-chief-foreign-powers-steal-data-on-critical-us-infrastructure/2014/11/20/ddd4392e-70cb-11e4-893f-86bd390a3340\\_story.html](https://www.washingtonpost.com/world/national-security/nsa-chief-foreign-powers-steal-data-on-critical-us-infrastructure/2014/11/20/ddd4392e-70cb-11e4-893f-86bd390a3340_story.html). Acesso em: 6 out. 2022.

NARCISO, Késia R.; BORIN, Roseli. A paz internacional como direito humano e o efeito borboleta. In: ARAUJO, Bruno M. V. de; BIZAWU, Kiwonghi; LEISTER, Margareth A. (coord.). **[Coletânea do] XXIV Congresso Nacional do CONPEDI: Direito Internacional dos Direitos Humanos II**. Florianópolis: CONPEDI, 2015.

NICHOLS, Michelle. North Korea took \$2 billion in cyberattacks to fund weapons program: U.N. report. **Reuters**, [New York], Aug. 5, 2019. Disponível em: <https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX>. Acesso em: 8 nov. 2022.

OFAC. **North Korea sanctions program**. Washington, D.C.: OFAC, 2016. Disponível em: <https://home.treasury.gov/system/files/126/nkorea.pdf>. Acesso em: 7 nov. 2022.

OHCHR. **Declaração universal dos Direitos Humanos**. [12 nov. 2022]. Disponível em: <https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por>. Acesso em: 12 nov. 2022.

OPWC. **History**: looking back helps us look forward. [22 set. 2022]. Disponível em: <https://www.opcw.org/about-us/history>. Acesso em: 22 set. 2022.

ORACLE. **O que é IoT?** [22 nov. 2022]. Disponível em: <https://www.oracle.com/br/internet-of-things/what-is-iot/>. Acesso em: 22 nov. 2022.

PUTIN diz que relações Rússia-Ucrânia se normalizarão após “operação militar especial”. **CNN Brasil**, [S. l.], 17 jun. 2022. Disponível em: <https://www.cnnbrasil.com.br/internacional/putin-diz-que-relacoes-russia-ucrania-se-normalizarao-apos-operacao-militar-especial/>. Acesso em: 9 out. 2022.

RAMOS, André de C. **Curso de direitos humanos**. 4. ed. São Paulo: SaraivaJur, 2017. *E-book*.

SARLET, Ingo W.; MARINONI, L. G.; MITIDIERO, D. **Curso de direito constitucional**. 11. ed. São Paulo: SaraivaJur, 2022. *E-book*.

SCHECHNER, Sam. Ukraine’s ‘IT Army’ has hundreds of thousands of hackers, Kyiv says. **The Wall Street Journal**, [S. l.], Mar. 4, 2022. Disponível em: <https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX>. Acesso em: 3 out. 2022.

SERRA, Gabriel V. H; SOUSA, Monica T. C. A legitimidade do uso da força no direito internacional: os limites dos princípios da soberania e da não intervenção frente aos Direitos Humanos. In: DEL OLMO, Florisbal de S; GLITZ, Frederico E. Z (coord.). **[Coletânea do] III Encontro Virtual do CONPEDI: Direito Internacional I**. Florianópolis: CONPEDI, 2021.

SERRANO, Carlos. Hiroshima e Nagasaki: como foi o ‘inferno’ no qual morreram milhares por causa das bombas atômicas. **BBC News Mundo**, [S. l.], 6 ago. 2020. Disponível em: <https://www.bbc.com/portuguese/resources/idt-a05a8804-1912-4654-ae8a-27a56f1c2b8a>. Acesso em: 20 set. 2022.

SHARMA, Munish. Data theft: implications for economic and national security. **Journal of Defence Studies**, New Delhi, v. 11, n. 1, Jan./Mar. 2017, p. 61-80. Disponível em: [https://www.researchgate.net/profile/Munish-Sharma-7/publication/327498043\\_Data\\_Theft\\_Implications\\_for\\_Economic\\_and\\_National\\_Security/links/5b9208c44585153a53002aca/Data-Theft-Implications-for-Economic-and-National-Security.pdf](https://www.researchgate.net/profile/Munish-Sharma-7/publication/327498043_Data_Theft_Implications_for_Economic_and_National_Security/links/5b9208c44585153a53002aca/Data-Theft-Implications-for-Economic-and-National-Security.pdf). Acesso em: 6 out. 2022.

SIERRA, Guilherme. Como a fome afeta o organismo? **Superinteressante**, [S. l.], 31 mar. 2003. Disponível em: <https://super.abril.com.br/saude/como-a-fome-afeta-o-organismo/>. Acesso em: 22 set. 2022.

SOARES, Ricardo M. F. **Hermenêutica e interpretação jurídica**. 4. ed. São Paulo: SaraivaJur, 2019. *E-book*.

THREE North Korean military hackers indicted in wide-ranging scheme to commit cyberattacks and financial crimes across the globe. **Justice News [of the United States Department of Justice]**, Washington, D.C., Feb. 17, 2021. Disponível em: <https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and>. Acesso em: 7 nov. 2022.

TURQUIA reitera intenção de continuar operações militares contra curdos na Síria. **G1**, [S. l.], 19 jul. 2022. Disponível em: <https://g1.globo.com/mundo/noticia/2022/07/19/turquia-reitera-intencao-de-continuar-operacoes-militares-contr-curdos-na-siria.ghtml>. Acesso em: 9 out. 2022.

UCRÂNIA convoca “exército de TI” para batalha cibernética. **G1**, [S. l.], 26 fev. 2022. Disponível em: <https://g1.globo.com/mundo/noticia/2022/02/26/ucrania-convoca-exercito-de-ti-para-batalha-cibernetica.ghtml>. Acesso em: 15 nov. 2022.

UCRÂNIA sob ataque incessante de *hackers* russos; internet cai na Europa. **Tilt UOL**, São Paulo, 5 mar. 2022. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2022/03/05/ucrania-sites-estao-sob-ataque-incessante-de-hackers-russos.htm>. Acesso em: 3 out. 2022.

UNESCO. **Orientações técnicas para aplicação da Convenção do Patrimônio Mundial**. Lisboa: UNESCO, 2021.

VATTEL, Emer de. **O direito das gentes**. Brasília, DF: Editora UnB: IPRI, 2004.