Universidade Federal da Paraíba – UFPB
Centro de Ciências Humanas, Letras e Artes – CCHLA
Núcleo de Cidadania e Direitos Humanos – NCDH
Programa de Pós-Graduação em Direitos Humanos, Cidadania e Políticas Públicas – PPGDH

MARCELYNNE ARANHA ALMEIDA

GUERRAS CIBERNÉTICAS E A PROTEÇÃO HUMANITÁRIA DE SUAS VÍTIMAS: ENTRE CONTROVÉRSIAS CONCEITUAIS E O ENSEJO POR POLÍTICAS PÚBLICAS INTERNACIONAIS

JOÃO PESSOA – PB

2022

MARCELYNNE ARANHA ALMEIDA

GUERRAS CIBERNÉTICAS E A PROTEÇÃO HUMANITÁRIA DE SUAS VÍTIMAS: ENTRE CONTROVÉRSIAS CONCEITUAIS E O ENSEJO POR POLÍTICAS PÚBLICAS INTERNACIONAIS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direitos Humanos, Cidadania e Políticas Públicas da Universidade Federal da Paraíba – UFPB, como requisito final para a obtenção do título de Mestre em Direitos Humanos, Cidadania e Políticas Públicas.

Linha 1: Direitos Humanos e Democracia: Teoria, História e Política

Orientador: Prof. Dr. Sven Peterke

JOÃO PESSOA – PB

2022

A447g Almeida, Marcelynne Aranha.
Guerras cibernéticas e a proteção humanitária de suas vítimas: entre controvérsias conceituais e o ensejo por políticas públicas internacionais / Marcelynne Aranha Almeida. - João Pessoa, 2022.
153 f.

Orientação: Sven Peterke.
Dissertação (Mestrado) - UFPB/CCHLA.

1. Conflitos Armados Internacionais. 2. Direito Internacional Humanitário. 3. Novas Tecnologias de Guerra. 4. Operações Cibernéticas. I. Peterke, Sven. II. Título.

UFPB/CCJ CDU 34

MARCELYNNE ARANHA ALMEIDA

GUERRAS CIBERNÉTICAS E A PROTEÇÃO HUMANITÁRIA DE SUAS VÍTIMAS: ENTRE CONTROVÉRSIAS CONCEITUAIS E O ENSEJO POR POLÍTICAS PÚBLICAS INTERNACIONAIS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direitos Humanos, Cidadania e Políticas Públicas da Universidade Federal da Paraíba – UFPB, como requisito final para a obtenção do título de Mestre em Direitos Humanos, Cidadania e Políticas Públicas.

Linha 1: Direitos Humanos e Democracia: Teoria, História e Política

Orientador: Prof. Dr. Sven Peterke

Data de aprovação: 23/08/2022

BANCA EXAMINADORA

Sven Peterke
Prof. Dr. Sven Peterke (Orientador)

Gustavo B. H. Batista
Prof. Dr. Gustavo Batista (Membro Interno)

Prof. Dr. Henrique Lenon Guedes (Membro Externo)

Prof. Dr. Paulo Kuhlmann (Membro Externo)

JOÃO PESSOA – PB

2022

Dedico este trabalho à **Dona Isabel** e aos meus amados pais.

AGRADECIMENTOS

Ao meu Deus, que nunca me abandonou. Em meio às tempestades, a fé permitiu que pudesse seguir... vou a Cristo por Maria.

Aos meus pais, Conceição e Marcelino, que sempre me deram suporte inesgotável. Por serem meus exemplos de fé, de vida, minha base.

Ao meu noivo, Matheus, pelo apoio ininterrupto, e pelo amor a mim dedicado. Esteve ao meu lado diariamente na reta final desta pesquisa, partilhou da minha angústia e lágrimas quando tanto queria avançar academicamente, e não conseguia por motivos de saúde. Não poderia ter escolhido pessoa melhor para passar o resto da vida.

Ao Prof. Dr. Sven, ao qual eu já nutria bastante admiração durante a graduação, e tive o prazer de ter como orientador nesta pós-graduação. Tornou esse processo de autoconhecimento e de crescimento mais leve, e, com sua sabedoria, incentivou e acreditou nesta pesquisa. Meu profundo agradecimento pelo olhar crítico e humano.

Aos professores do PPGDH e aos membros da banca, Prof. Dr. Gustavo Batista, Dr. Henrique Lenon e Dr. Paulo Kuhlmann, pelas análises e sugestões para que a pesquisa crescesse – e eu também.

À UFPB e à CAPES, pelo apoio sem o qual essa pesquisa não teria alçado voo.

A todos familiares e amigos que me incentivaram durante esses anos de aprofundamento acadêmico. Em especial, à minha sogra, Niédja, e à minha tia Jocelina, pelas orações, visitas e incentivos para que eu jamais desistisse dos meus sonhos e mantivesse a minha fé.

Humanitarianism consists in never sacrificing
a human being to a purpose.
(Albert Schweitzer)

RESUMO

A presente dissertação analisa as possíveis situações de guerra cibernética sob a ótica da proteção de vítimas pelo Direito Internacional Humanitário (DIH). Numa tendência de digitalização e de dependência global do espaço cibernético, que pode ter sido acelerada pelo cenário de pandemia da COVID-19, as vulnerabilidades do ambiente virtual foram afloradas, ressaltando este como potencial zona de operações militares. Os ataques realizados no ciberespaço podem ter diversas origens, desde Estados, organizações terroristas, ativistas, cidadãos comuns, etc., e por vezes podem ser utilizados por governos para auxiliar estrategicamente os tradicionais domínios bélicos e/ou coadunar como "atos de guerra". Enquanto ambiente complexo, incerto e de difícil fiscalização, propiciam-se violações, especialmente de direitos humanos e de normas de direito internacional. Nessa perspectiva, esta pesquisa parte da delimitação das situações denominadas como guerra cibernética enquanto matéria de preocupação humanitária, perpassando a identificação de conceitos como os de espaço cibernético, operações cibernéticas, ataques cibernéticos, etc., de modo atento às consequências e vitimizações dessas guerras para os fins jurídicos. Cada vez mais Estados têm desenvolvido capacidades cibernéticas ofensivas, levando a questionamentos quanto ao grau de dano humano oferecido pelas ações de natureza não cinética e à possível avaliação destas segundo a convencional regulamentação de conflitos armados de caráter internacional. Com vistas a isso, objetiva-se discutir até que ponto operações cibernéticas inseridas ou equivalentes a conflitos armados internacionais – guerras cibernéticas – podem receber o tratamento jurídico humanitário correspondente à sua essência protetiva. A hipótese levantada é de que as situações de guerra cibernética aqui circunscritas não ocorrem em um vácuo jurídico, e que as operações em seu escopo estão, em parte, regulamentadas pelo DIH, embora de modo insuficiente, sobretudo sob um viés operacional. Utiliza-se do método dialético para compreensão do fenômeno, e abordagem qualitativa para investigar as informações e interpretações atinentes aos ataques cibernéticos e ao DIH. A partir de procedimento de revisão bibliográfica e pesquisa documental, observam-se discussões doutrinárias sobre eventos da praxe internacional que permeiam os riscos de operações cibernéticas e a possibilidade de adaptação de preceitos do *jus in bello*, bem como os posicionamentos e pareceres emitidos por Estados, organizações internacionais e pelo Comitê Internacional da Cruz Vermelha. Conclui-se que os princípios humanitários podem oferecer uma elucidação à "zona cinzenta" que lastreia o comportamento dos Estados no ciberespaço em contexto de segurança internacional. Contudo, o potencial custo humano que as operações cibernéticas têm assumido faz notar que outros impasses – como a atribuição de autoria estatal – exibem a necessidade de melhor balizamento e de adoção de políticas públicas internacionais para cooperação sobre seu uso, com atenção às possíveis vítimas e para posterior responsabilização internacional.

Palavras-chave: Conflitos Armados Internacionais. Direito Internacional Humanitário. Novas Tecnologias de Guerra. Operações Cibernéticas.

ABSTRACT

This dissertation analyzes the possible situations of cyber warfare from the perspective of the protection of victims by International Humanitarian Law (IHL). In a trend of digitalization and global dependence on cyberspace, which may have been accelerated by the COVID-19 pandemic scenario, the vulnerabilities of the virtual environment were highlighted, showing this as a potential zone of military operations. Attacks carried out in cyberspace can have different origins, such from States, terrorist organizations, activists, ordinary citizens, etc., and can sometimes be used by governments to strategically assist traditional warfare domains and/or coadunate as "acts of war". As a complex, uncertain and hard to monitor environment, it is conducive to violations, especially of human rights and international law. In this perspective, this research starts from the delimitation of the situations called cyberwarfare as a matter of humanitarian concern, going through the identification of concepts such as cyberspace, cyber operations, cyberattacks, etc., in an attentive way to the consequences and victimizations of these wars for legal purposes. Many States have developed offensive cyber capabilities, leading to questions about the degree of human damage offered by actions of a non-kinetic nature and the possible evaluation of these under the conventional regulation of international armed conflicts. In view of this, it is aimed to discuss to what extend cyber operations amounting to, or conducted in the context of, an international armed conflict – cyber wars – can receive the humanitarian legal treatment corresponding to its protective essence. The hypothesis is that the cyber warfare situations described here do not occur in a legal vacuum, and that the operations within its scope are partly regulated by IHL, although insufficiently, especially from an operational perspective. It uses the dialectical method to understand the phenomenon, and qualitative approach to investigate the information and interpretations regarding cyberattacks and IHL. Based on the literature review procedure and documentary research, the doctrinal discussions on events in international practice that permeates the risks of cyber operations and the possibility of adapting the precepts of *jus in bello* are observed, as well as the positions papers and opinions issued by States, International organizations, and by the International Committee of the Red Cross. It is concluded that humanitarian principles can offer an elucidation of the "gray zone" that underlies the States behavior in cyberspace in the context of international security. However, the potential human cost that cyber operations have taken on points out that other impasses – such as the attribution of State authorship – show the need for better guidance and adoption of international public policies for cooperation on its use, with attention to possible victims and for subsequent State responsibility.

Keywords: International Armed Conflicts. International Humanitarian Law. New Technologies of Warfare. Cyber Operations.

LISTA DE ILUSTRAÇÕES

FIGURAS

QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AGNU – Assembleia Geral das Nações Unidas

AI – Artificial Intelligence (Inteligência Artificial)

Art. – Artigo

CCDCOE – Cooperative Cyber Defence Centre of Excellence (Centro de Excelência em Defesa Cibernética Cooperativa da OTAN)

CICV – Comitê Internacional da Cruz Vermelha

CIJ – Corte Internacional de Justiça

CJI – Comissão Jurídica Interamericana

COVID-19 – Corona Virus Disease (Doença do Coronavírus – 2019)

CSNU – Conselho de Segurança das Nações Unidas

DHI – Direitos Humanos Internacionais

DIH – Direito Internacional Humanitário

DDoS – Distributed Denial of Service

DoS – Denial of Service

ECS – Estratégia de Cibersegurança da União Europeia

EUA – Estados Unidos da América

GGE – Group of Governmental Experts (Grupo de Peritos Governamentais das Nações Unidas)

I CG – I Convenção de Genebra de 12 de agosto de 1949 para a melhoria das condições dos feridos e dos enfermos das forças armadas em campanha

IV CG – IV Convenção de Genebra de 12 de agosto de 1949 relativa à proteção dos civis em tempo de guerra

IP – Internet Protocol (Endereço de Protocolo de Rede)

OEWG – Open-Ended Working Group (Grupo de Trabalho Aberto das Nações Unidas)

OI – Organização Internacional

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado do Atlântico Norte

PA I – Protocolo Adicional I às Convenções de Genebra de 1949, relativo à proteção das vítimas dos conflitos armados internacionais, de 8 de junho de 1977

PA II – Protocolo Adicional II às Convenções de Genebra de 1949, relativo à proteção das vítimas dos conflitos armados não internacionais, de 8 de junho de 1977

PoA – Programme of Action for advancing responsible State behaviour in cyberspace (Programa de Ação para promover o comportamento responsável do Estado no ciberespaço).

RAM – Revolução nos Assuntos Militares

SCADA – Supervisory Control and Data Acquisition (Sistemas de Supervisão e Aquisição de Dados)

SQL – Structured Query Language

SPAM – Sending and Posting Advertisement in Mass

TIC – Tecnologia da Informação da Comunicação

UE – União Europeia

SUMÁRIO

INTRODUÇÃO

As fronteiras geográficas tradicionais foram relativizadas ainda mais pelo ciberespaço, possibilitando que informações e dados pudessem se difundir entre Estados, organizações e indivíduos em ritmo acelerado graças a redes digitais em infraestrutura interconectada. Com o aumento da capacidade tecnológica, governos e populações se tornaram dependentes de conexões confiáveis e de dados colocados apenas no espaço cibernético. Nesse cenário, operações cibernéticas se tornaram uma realidade nos conflitos armados da contemporaneidade, inclusive implicando em potencial custo à humanidade. Eventos recentes têm demonstrado os riscos que as operações cibernéticas, estejam inseridas ou não em contexto de conflito armado, oferecem à infraestrutura civil e à prestação de serviços essenciais à população, sobrelevando o papel de políticas públicas e da discussão internacional sobre a aplicabilidade, suficiência e adaptação do Direito Internacional Humanitário (DIH) às denominadas guerras cibernéticas.

Em 13 de março de 2020, em plena pandemia do novo coronavírus, um hospital de Brno, cidade da República Tcheca, foi atingido por um ataque cibernético que forçou o adiamento de intervenções cirúrgicas urgentes, a transferência de pacientes e a redução de atividades essenciais. Outros incidentes cibernéticos direcionados ao setor de saúde durante a pandemia foram relatados em diversos países, incluindo França, Espanha, Tailândia e Estados Unidos (MAČÁK; RODENHÄUSER; GISEL, 2020). O incidente em Brno é apenas um dos exemplos fáticos de como ataques cibernéticos podem implicar em custos humanos.

Em situações de conflito armado, o DIH, especialmente pelas previsões das Convenções de Genebra de 1949 e seus Protocolos Adicionais de 1977, oferece proteção normativa às vítimas das hostilidades, sejam elas combatentes ou não. Atenta ao incremento dos meios ou métodos de guerra pelas Tecnologias da Informação e da Comunicação (TIC), esta pesquisa analisa o uso bélico de operações cibernéticas, que, dadas as abstrações oferecidas pelo espaço cibernético – dissimulação de autoria, violência não cinética, danos indiretos, etc. – podem ser maiormente utilizadas nas relações internacionais com vistas a obtenção de certas vantagens, de modo alheio à salvaguarda das vítimas pelo DIH.

Tendo em vista os pequenos passos que entidades da sociedade internacional e da academia têm dado para averiguar o alcance das normas de proteção em conflitos armados internacionais às operações cibernéticas, a presente pesquisa problematiza se as situações às quais podem ser denominadas guerras cibernéticas de fato têm o potencial de causar danos humanos, e em que medida essas situações conseguem ser avaliadas pelo DIH. De modo

particular, como a essência protetiva do DIH enfrenta a novidade tecnológica e a viabilidade de atribuição e responsabilização por operações cibernéticas com qualidade bélica – sobretudo a atores estatais.

Diante da repercussão internacional do emprego de operações cibernéticas para fins militares e os impasses e riscos à segurança humana ocasionados pela névoa que permeia a aplicabilidade das normas que limitam as hostilidades dos conflitos armados àquelas, inicialmente exibe-se o problema de se aproximar a uma noção de "guerra cibernética" apta aos estudos do DIH, não obstante tratar-se de tema essencialmente interdisciplinar. A partir disso, e à luz de uma realidade emergente, a discussão sobre a ciberguerra é realizada observando os desafios de visualização de ações no ciberespaço como "atos de guerra", e a evolução de políticas internacionais que promovam a defesa dos direitos humanos e diminuição dos riscos humanitários é examinada.

O trabalho faz uma opção por estudar o tema especialmente sob a perspectiva dos conflitos armados de caráter internacional, com atenção às potenciais vítimas de operações cibernéticas. A hipótese articulada aponta que as situações de guerra cibernética aqui circunscritas não estão em um vácuo jurídico, mas que as ações em seu escopo estão parcialmente regulamentadas pelo DIH, porém de modo insuficiente, maiormente do ponto de vista operacional.

Para os fins deste estudo, faz-se mister identificar conceitos como os de espaço cibernético, operações cibernéticas, ataques cibernéticos e, por fim, de guerra cibernética, para que sejam observadas as possíveis consequências e vitimizações dessas guerras e, então, para que se investigue a aplicabilidade das normas dos conflitos armados e o que organismos internacionais têm estimulado nesse sentido. Avalia-se se a aplicabilidade das normas protetivas humanitárias pode ocorrer de maneira não meramente declarativa, mas operacional, a partir dos princípios do DIH e da elaboração de instrumento de *soft law* como reforço delineador de políticas públicas de segurança cibernética e cooperação internacional no que tange ao uso de operações cibernéticas e à responsabilização estatal.

Das imprecisões que perpassam as guerras cibernéticas, e da possível brecha para ilícitos, tendo em vista a potencial (in)suficiência normativa humanitária para regular atividades militares no ciberespaço, a pesquisa parte da discussão sobre até que ponto o surgimento de um novo padrão de conflito pautado em atividades no meio cibernético pode implicar em "uso de força" e em "ataque armado" pela Carta das Nações Unidas e, de forma mais factível, em "ato de guerra" ou em "ataque" para as normas do DIH. Os "ataques" para o ordenamento

humanitário, vide art. 49 (1) do Protocolo Adicional I (PA I) às Convenções de Genebra, importam em atos de violência (precipuamente física) contra um adversário, e é com base nesses que os princípios que fundamentam a proteção de direitos humanos em conflitos armados são empregados.

Questiona-se se a condução de operações cibernéticas com qualidade de ou inseridas em conflitos armados alteraria a "lógica cinética" de uso da força e de atos de violência física que as Leis da Guerra, o *jus ad bellum* e o *jus in bello*, estavam acostumadas. Afinal, a dependência das ferramentas digitais e do funcionamento ininterrupto das tecnologias ligadas ao ciberespaço para acesso de informações críticas e prestação de serviços essenciais – como acesso à saúde, fornecimento de energia elétrica, acesso a bancos, sistemas de saneamento e distribuição de água à população de um país – poderia demonstrar que um "ataque" não mais precisa corresponder a danos físicos diretos. Uma operação cibernética capaz de manipular sistemas, desativar serviços ou desligar computadores, por exemplo, seria capaz de repercutir na liberação de águas de barragens, inativação de hospitais, apagões elétricos, etc., afetando civis de forma indistinta e sem necessariamente resultar em mortes ou destruição de objetos.

Alicerçada em procedimentos de natureza qualitativa, a pesquisa trabalha a interpretação e tratamento de informações sobre operações cibernéticas com vistas a atender interesses políticos e estratégicos, e suas potenciais vitimizações para o DIH. O método de abordagem é dialético, posto que se compreende a totalidade do fenômeno do ciberespaço como potencial ambiente bélico, fato social que recebe influências políticas, econômicas, etc., que ultrapassam a ciência jurídica. Parte da complexidade de se delimitar e de estabelecer parâmetros para o que viria a ser a guerra cibernética, e, então, sob o prisma humanitário, analisa o evento com vistas à realidade dos conflitos armados internacionais contemporâneos. Por vezes confrontando o acolhimento e regulamentação de operações cibernéticas pelo DIH, a partir de diferentes interpretações doutrinárias acerca dos perigos do fenômeno guerra cibernética, propõe-se a observar tal como questão de natureza humanitária que merece atenção de políticas públicas internacionais voltadas à proteção de suas vítimas, em que pese as abstrações inerentes.

Dentre as referências utilizadas para a pesquisa bibliográfica e documental, destacam-se obras de divulgação, publicações periódicas de pesquisadores do DIH, além de pareceres e declarações emitidas pelo Comitê Internacional da Cruz Vermelha (CICV) e por organismos internacionais como a ONU e OTAN acerca de ataques cibernéticos, advento da ciberguerra, aplicabilidade das normas já existentes para a proteção da infraestrutura básica e dos civis, e

políticas públicas de segurança e defesa cibernética. São sobrelevadas as publicações no escopo do CICV para desenvolvimento do tema, como as oferecidas pela *International Review of the Red Cross*, e os Manuais de Tallinn como instrumentos elaborados por pesquisadores que melhor têm enfrentado os problemas do direito internacional aplicável ao espaço cibernético.

O trabalho é composto por três capítulos. No primeiro, busca-se definir o que é a guerra cibernética para os fins da pesquisa. Para isso, é iniciado com uma breve apresentação do que seria a guerra para Carl von Clausewitz, teórico bastante utilizado por pesquisadores como pontapé para conceituar a guerra cibernética. Na parte seguinte do capítulo, é contextualizado o espaço cibernético como possível novo domínio de guerra, donde surgem novos meios e métodos de condução de hostilidades. Posteriormente, destina-se à discussão de uma definição de guerra cibernética a partir das Leis da Guerra e de diferenciações em relação a outras ameaças e ataques no ciberespaço. Para fins de melhor visualização dos impactos à nível global de operações cibernéticas, são citados, de forma breve, alguns exemplos da praxe internacional corriqueiramente interligados a conflitos de interesse entre Estados.

O segundo capítulo é desenvolvido de maneira a examinar a dimensão em que as operações cibernéticas seriam regidas pelo DIH, possivelmente representando a transgressão de "limites cinéticos" a disposições pertinentes aos escopos do *jus ad bellum* e do *jus in bello*, como "uso da força", "ataque armado" e "força armada". É observado quem são as vítimas de ciberguerras à luz do potencial lesivo de operações cibernéticas; em especial, as populações civis como mais afetadas por conflitos armados. A partir da discussão sobre o que viria a ser "ataque" para o DIH e sobre quais ações seriam reguladas pelas normas humanitárias, inicia-se a reflexão sobre o nível de proteção oferecido às vítimas de operações cibernéticas em curso de conflitos armados internacionais.

O terceiro capítulo investiga tal salvaguarda oferecida pelo DIH às vítimas, balizada pelos Princípios da Humanidade, da Distinção, da Proporcionalidade e da Necessidade Militar. Estes são explorados com base em debates bibliográficos sobre os desafios de adaptação frente à novidade bélica. O capítulo aborda, ainda, a evolução do tratamento das operações cibernéticas pela sociedade internacional, sobretudo como matéria de proteção humana que enfrenta impasses jurídicos: a atribuição de autoria e a viabilidade de responsabilização internacional são analisadas sob a ótica da jurisdição no ciberespaço e do dever de *due diligence* dos Estados, e é feito um breve acompanhamento sobre como organismos internacionais – CICV, ONU, OEA e OTAN – têm se movimentado para desenvolver o direito internacional frente ao espaço cibernético, mormente em prol da proteção de vítimas em guerras cibernéticas.

Após as considerações finais e referências bibliográficas, consta um glossário onde alguns dos termos discutidos estão organizados para facilitar a consulta sobre o significado maiormente acatado para os fins da pesquisa. Além de todos os motivos retromencionados que justificam a pesquisa como de relevância corrente na agenda global, nota-se a escassez de produção científica nacional sobre o fenômeno da ciberguerra e suas vitimizações como matéria do DIH. No mais, vinculando a nova dinâmica estratégica e bélica do uso do espaço cibernético e os efeitos nocivos que tal oferece, o presente trabalho oferece um olhar contemporâneo sobre a “nova guerra” e os valores humanitários até então estabelecidos.

1. GUERRA CIBERNÉTICA: UM CONCEITO CONTROVERSO

A guerra é um fenômeno mutável e complexo. Dessa premissa, este primeiro capítulo é desenvolvido de maneira a introduzir o tema chave da pesquisa: a guerra cibernética. Antes de quaisquer indagações sobre os caminhos que serão percorridos pelo direito e pelas políticas públicas internacionais para a tratativa do assunto, cumpre distinguir e compreender o uso do domínio cibernético como uma nova tecnologia de guerra e, portanto, como matéria de segurança humana. A ênfase da presente pesquisa atravessa as transformações tecnológicas e a evolução das denominadas "Leis da Guerra[1]" e, para tanto, o faz à luz das potenciais vítimas e dos riscos humanitários da cibernética na esfera militar. Não obstante o espaço cibernético, elemento que será examinado neste capítulo, apresentar seus inquestionáveis benefícios à humanidade, na medida em que é visto e utilizado como tecnologia de guerra (*stricto sensu*), passa-se a questionar os limites e proporções que as guerras (*lato sensu*) da informação podem atingir nos dias atuais.

O conceito de guerra cibernética não é uniforme e bem delimitado – e dificilmente o será, tendo em vista todos as abstrações e inovações inerentes ao ambiente onde ocorre. Contudo, para compreendê-la, diversos autores[2] tentam interpretar sua essência a partir de axiomas clausewitzianos. Por tal razão, para alcançar uma definição de espaço cibernético e de guerra cibernética para o intuito dos estudos do Direito Internacional Humanitário aplicável ao novo domínio que se mostre atenta às possíveis vitimizações em contexto de conflito armado[3], inicialmente, e de forma breve, será abordado o paradigma clausewitziano e suas rasas[4] contribuições, sobretudo metafóricas, para os estudos jurídicos e para a predileção de regramentos voltados às constantes alterações e à diversidade dos fenômenos da guerra.

Em seguida, a partir de discussões interdisciplinares, é apresentado o espaço cibernético como domínio em que ocorre a guerra cibernética, o novo cenário fruto das transformações das últimas décadas que implicou numa renovação dos assuntos militares e, diante disso, em preocupação para o direito internacional. Ao final do capítulo, é discutido o conceito de guerra cibernética a partir da distinção entre outras ameaças cibernéticas e ataques que se inserem no

[1] O *jus ad bellum* e o *jus in bello*, aqui, o direito de recorrer à guerra pela Carta das Nações Unidas de 1945 e o direito na guerra, o Direito Internacional Humanitário.
[2] Vide Danny Steed (2016), John Arquilla e David Ronfeldt (1993), Paulo Shakarian *et al*. (2013), P. W. Singer e Allan Friedman (2014), Rafael G. Mota (2018), Thomas Rid (2013), dentre outros.
[3] Serão abordados nos capítulos seguintes.
[4] Não é contestada a relevância de Carl von Clausewitz e de sua clássica doutrina de guerra, todavia, é patente a limitação histórica à realidade do final do século XVIII e início do século XIX, quando vigorava um sistema internacional bastante diverso, sem limitações ao uso da força, e a ênfase no poder militar dos Estados-Nações.

contexto de conflito armado, para então se atingir a noção de guerra cibernética[5] – atrelada à perspectiva jurídica – que será adotada ao longo desta pesquisa.

1.1 A guerra em Clausewitz

"A guerra é uma simples continuação da política por outros meios", definiu Carl von Clausewitz (1780-1831) em sua renomada obra *Vom Kriege*, Da Guerra (2010, p. 27). O escritor e soldado prussiano iniciou a carreira militar ainda muito jovem, na Confederação do Reno entre 1793 e 1794, e o contexto histórico-intelectual que levou à sua obra remete à virada de séculos e período que perpassa as guerras da Revolução Francesa e guerras napoleônicas.

Esse contexto histórico, por si só, revela bastante da formação e vida daquele que pode ser considerado um dos maiores teóricos da guerra. Falecendo aos 51 anos, em 1831, Clausewitz colecionou em sua carreira militar a participação em diversos conflitos armados, e estima-se que tenha começado a escrever Da Guerra em 1818, logo após o fim das guerras napoleônicas. Apesar de ter batalhado em oposição a Napoleão Bonaparte, Clausewitz admirava o estadista, inclusive denominando-o como "o próprio Deus da Guerra" em sua obra (CLAUSEWITZ, 2010, p. 835).

Ocorre que o fascínio por Napoleão se mostrou muito mais ligado ao estudo sobre a técnica e habilidade em se fazer a guerra, o que proporcionou a escrita de oito livros que refletem uma teoria da guerra inacabada, dada a morte do então general prussiano e a publicação do conjunto de textos em Da Guerra por sua esposa em 1832, com o indicativo de que apenas o primeiro capítulo do livro I, relativo à natureza da guerra e definição da mesma, havia sido integralmente redigido. Na obra consta a advertência do próprio general de que se uma morte precoce viesse a interromper seus trabalhos, "o material existente só poderia sem dúvidas ser considerado como um amálgama de ideias informes expostas a incessantes mal-entendidos, que suscitará uma quantidade de críticas prematuras" (CLAUSEWITZ, 2010, nota II, p. XCII).

O propósito de Clausewitz não era de apresentar uma teoria para explicar o que leva às guerras. Antes disso, o prussiano desenvolveu uma teoria sobre a estratégia na guerra. Nessa

[5] Como se verá, conceito controverso, sem uma definição universal ou largamente aceita. Os estudos para uma delimitação são bastante polêmicos e por vezes contraditórios, perpassando desde a inexistência ou invalidação de guerras cibernéticas até a visualização destas como uma ameaça existencial (ASHRAF, 2021, p. 274). Compreende-se que para alguns pesquisadores, sobretudo dos Estudos Estratégicos e Relações Internacionais, o conceito encontra impasses éticos e políticos; como em Thomas Rid (2013), Marco Cepik; Diego R. Canabarro; Thiago B. Ferreira (2015), etc. Mas a posição que esta pesquisa adota é voltada à praxe internacional e ao risco humano presente na possível inconsistência alegada por partes beligerantes quanto a regulamentação internacional de operações cibernéticas e posterior responsabilização dos envolvidos em conflitos armados. Logo, filia-se a um raciocínio maiormente jurídico e condizente com os fundamentos do DIH.

toada, seus textos possuem comparações com a história militar para que se analise a complexidade na condução das guerras e, apesar de ter rompido paradigmas para a arte da guerra no século XIX, gozam de generalizações e abstrações bastante pertinentes para a compreensão crítica da relação entre política e conflitos armados, que repercutem nas relações internacionais e no pensamento militar contemporâneo.

Clausewitz observa o fenômeno guerra como um instrumento de política nacional, que racionalmente seria empreendido para alcançar o objetivo de satisfação dos interesses nacionais. Não mero ato político, mas instrumento político, em que se resguarda a intenção política por meio de ato de violência onde se almeja forçar o adversário a submeter-se à vontade do outro, a guerra é apontada pelo soldado como "um verdadeiro camaleão", pois sua natureza é modificada a cada caso concreto, seguindo um conjunto de tendências provenientes da trindade intermediada pelo povo, exército e governo (CLAUSEWITZ, 2010, p.7, 27-30).

A acepção de guerra como política por outros meios lembra a filosofia política maquiavélica, em que os fins justificam os meios e na qual, observa Thales Castro (2012, p. 94), se assume uma maximização do poder na operacionalização do cenário internacional pelos atores da política internacional, numa relação de causa-efeito que explica a dinâmica dos Estados como atores políticos racionais do sistema internacional. De fato, ambos adotam perspectivas finalísticas pautadas no conflito bélico e na busca pelo poder, onde guerra e política são temas indissociáveis, proporcionando a qualificação como teóricos realistas nas Relações Internacionais[6]. Contudo, os indícios de apropriação ou de diálogo crítico entre o general prussiano e Nicolau Maquiavel são vagos, outrossim, a análise clausewitziana da guerra detém um estatuto epistemológico distinto, em que o fenômeno guerra guarda caráter histórico e social, para além do político, e se mostra estrategicamente flexível e aberto às transformações sociais, políticas e econômicas (PASSOS, 2014, p. 149-150).

Enquanto tema central nos estudos das Relações Internacionais, o intuito de se explicar a guerra e a paz entre as nações tem origem bastante anterior ao surgimento da cátedra e foi preocupação de diversos filósofos, historiadores e juristas[7]. Apesar de lastreada por múltiplas orientações teóricas em que o fenômeno é analisado sob diferentes perspectivas, as Relações Internacionais estão alicerçadas pela dicotomia entre as teorias realista e liberal para

[6] Maquiavel e Clausewitz por vezes são rotulados como teóricos do *realpolitik*, "realismo político" na Ciência Política e nas Relações Internacionais, tendo em vista a instrumentalidade política adotada e a relevância atribuída ao poder para se defender e para manutenção do Estado frente às ameaças à segurança nacional (JATOBÁ, 2013, p. 18-20; PASSOS, 2014, p.145).

[7] Desde a antiguidade, sob distintos contextos culturais, podem ser citados Cícero, Sun Tzu, etc., e até mesmo Santo Agostinho.

interpretação e desenvolvimento do problema guerra. Se, por um lado, a filosofia da guerra por vezes representada e embasada pelos clássicos Nicolau Maquiavel e Thomas Hobbes desvela uma essência negativa e belicosa do homem, onde a política internacional é permeada pelo estado de guerra e pela natureza egoística dos indivíduos, por outro, defende-se a ação transformadora da condição humana e a idealização de uma comunidade internacional, onde À Paz Perpétua de Immanuel Kant inspira a eliminação da violência da guerra entre as nações por princípios éticos e morais que levam ao surgimento do direito internacional clássico.

Nessa seara, cabe ponderar que assim como o pensamento de Maquiavel, no seu tempo, rompeu paradigmas e trouxe conceitos relevantes para a relação guerra, poder e política, Clausewitz proporcionou uma apreciação abrangente e mutável do fenômeno, próxima dos elementos sociais e do reconhecimento das relações humanas complexas, a qual gerou releituras teóricas como interpretações neoclausewitzianas[8].

Antes de descrever a guerra como instrumento de política nacional, contudo, Clausewitz (1989, p. 75, tradução nossa[9]) a define como "um ato de força destinado a forçar o adversário a submeter-se à nossa vontade". A percepção de imposição da vontade ao inimigo em razão da intenção política, sob a ótica do contexto histórico de supremacia da violência organizada vivida pelo general prussiano, demonstra que o uso da força seria um dos instrumentos mais úteis da política – já que a guerra é a continuação da política por outros meios. A guerra como "ato de força" sobreleva a violência física ou a ameaça do uso da força[10] entre "forças vivas" que se encontram em choque em meio às incertezas (CLAUSEWITZ, 2010, p. 11, 25).

Ao mesmo tempo que sobreleva os Estados como principais atores das relações internacionais, diante da conjuntura bélica que permeava a soberania desde os tratados de

[8] Anatole Rapoport (2010, p. LXV) observa o ponto de vista neoclausewitziano fortemente defendido pela nova escola americana de relações internacionais: "Nos detalhes, o ponto de vista neoclausewitziano difere da clássica doutrina clausewitziana, mas concorda com ela no essencial. A divergência é devida aos aspectos radicalmente diferentes, tanto políticos como tecnológicos, da guerra do século XX. Os neoclausewitzianos assumem uma posição realista; daí considerarem importantes as mudanças fundamentais do meio político e tecnológico. A semelhança essencial entre as formas modernas e clássicas da filosofia clausewitziana da guerra está enraizada na concepção básica da guerra como instrumento político e na admissão tácita de que os interesses nacionais de um Estado são facilmente discerníveis e, em grande parte, identificáveis com o poder de um Estado em comparação com outros". O filósofo francês Raymond Aron figura como um dos principais teóricos neoclausewitzianos, mormente por sua obra Paz e Guerra Entre as Nações, que reveste de modernidade a filosofia clausewitziana (RAPOPORT, 2010, p. LXX).

[9] War is thus an act of force to compel our enemy to do our will (CLAUSEWITZ, 1989, p. 75). Em parte, utiliza-se da versão brasileira, cuja tradução com o termo "violência", no lugar de "força", não raramente é considerada inadequada: "A guerra é pois um ato de violência destinado a forçar o adversário a submeter-se à nossa vontade" (CLAUSEWITZ, 2010, p. 7).

[10] Naturalmente, à sua época, a força cinética, ou física, a qual remete ao conflito à punho, uso de espadas, pólvora, bombas, etc., que causam danos materiais e têm efeito direto (SINGER; FRIEDMAN, 2014, p. 68).

Vestfália[11] e o período entre os séculos XVIII e XIX em que viveu, o realismo clausewitziano reconhece o "cálculo de probabilidades", ou a inteligência e estratégia, como instrumento para se obter a paz e se realizar o combate tão somente voltado ao atendimento de sua finalidade: o objetivo político (CLAUSEWITZ, 2010, p. 33-46). Logo, as forças militares serviriam à política.

A guerra, portanto, é vista sob o ponto de vista predominantemente militar, em que as forças armadas são cabalmente necessárias para manutenção do Estado soberano, entidade que não reconhece autoridade superior, e que exerce a força em nome da nação. Função própria aos interesses do Estado, a guerra é vista como fase normal das relações internacionais, coadunando com o pensamento de anarquia entre Estados, quer sejam civilizados ou não[12], e como arte do Estado que está subordinada à política e que não vai além do que a própria natureza violenta da política já apregoa. Nessa vereda, o pensamento clausewitziano bastante se aproxima do pessimismo e estado de natureza hobbesiano.

A noção estratégia e finalística da guerra de Clausewitz almejava consagrar uma teoria universal do que a guerra deveria ser, idealizando o rol de ações permissíveis ao "soldado profissional" (KEEGAN, 1993, p. 17), em uma "cegueira epistêmica" frente às guerras que ocorriam ao seu tempo; com efeito, sua teoria conscientemente arquitetava os comportamentos desejáveis em combate, como conteúdo propedêutico à ética do comportamento na guerra, e ao *jus in bello*, em que pese sua intensa preocupação com as funções intelectuais e morais do "bom combatente" (CINELLI, 2016, p. 119-120) estar vinculada ao máximo alcance dos objetivos da guerra à serviço da nação[13].

Seu ideal de organização da força militar reverbera suas vivências e reflexões como homem que viveu nos campos de batalha num período no qual o recurso à força não era restrito,

---

[11] O ideal vestfaliano de controle exclusivo do Estado sobre a aplicação da legítima força coercitiva, o "monopólio da violência" e o protagonismo nos campos de batalha recaíam sobre as forças armadas regulares do Estado-nação, e era sob tal premissa que Clausewitz visualizava a guerra como mero recurso da política que "se limitava basicamente à combinação entre diplomacia coercitiva e aplicação do poderio bélico convencional" (VISACRO, 2019, p. 117-118).

[12] Clausewitz (2010, p. 8-9) traz que "as guerras das nações civilizadas são bem menos cruéis e destruidoras do que as das nações não civilizadas [...] entre os selvagens prevalecem as intenções inspiradas pela sensibilidade; entre povos civilizados prevalecem as que são ditadas pela inteligência. [...] mesmo as nações mais civilizadas podem ser arrebatadas por um ódio ferroz. Por aqui se vê quanto estaríamos longe da verdade se reduzíssemos a guerra entre povos civilizados a um ato puramente racional dos governos, que nos pareceria cada vez mais isento de toda e qualquer paixão, de tal modo que, afinal de contas, o peso físico das forças armadas já nem seria necessário e que bastariam relações teóricas entre elas – uma espécie de álgebra da ação". Nota-se a visão realística de anarquia nas relações internacionais, em que a política é veementemente violenta.

[13] Até certa medida, as interpretações de Clausewitz mostram que este "acabou por ratificar a importância e a relevância de se ter, no âmbito da razão de Estado, uma clara orientação quanto à aplicação do jus in bello, ou seja, quanto à ética do comportamento na guerra. Normas para a ação despidas de caráter cogente, cuja eficácia não fosse perseguida e fiscalizada pelo Estado, seriam despropositadas" (CINELLI, 2016, p. 120).

e que exaltava as capacidades estratégicas no combate, apesar das referências iluministas do século XVIII e dos ideais pacifistas kantianos que migravam do campo religioso para o político à época[14]. O que leva à guerra, suas motivações e o desejo humano de se buscar a vitória e eminência do poder militar e político também são consideradas pelo prussiano, mas o seu racionalismo instrumental da guerra como fase normal nas relações entre nações e o fato de querer ser um teórico universal da arte da guerra, o tornam referência na frequente tentativa de conceituação do fenômeno. Esta teorização, todavia, é elementar tendo em vista a complexidade e mutabilidade inerentes aos cenários de hostilidades e a necessidade de se formular regras e princípios que diminuam o peso das controvérsias sobre o destino do conflito (MOTA, 2018, p. 87).

Ademais, a partir da perspectiva clausewitziana, há notória influência nas ciências militares, na estratégia e tática das forças armadas nacionais da atualidade[15]. Este é motivo, inclusive, de se contextualizar, ainda que brevemente e de modo restrito, o pensamento clausewitziano de "guerra" antes de adentrar às novas tecnologias bélicas da Era da Informação. Por sua teoria da guerra voltada ao comportamento militar, seus conceitos abstratos são bastante utilizados como ponto de partida para se compreender as novas configurações complexas, incertas e amorfas advindas da tecnologia cibernética.

Dessarte, de modo apartado das demais acepções da sua obra e do seu contexto histórico, das metáforas apresentadas por Clausewitz e suas utilizações como "conceito", a guerra como "camaleão"[16] provavelmente é a mais oportuna para se aplicar aos conflitos bélicos atuais e à conjuntura aqui trabalhada. Adquire diversas versões conforme as características gerais da época em que ocorra, sejam políticas, econômicas, tecnológicas, intelectuais e/ou sociais (PARET, 1989, p. 22); possui uma intrínseca maleabilidade de seus componentes.

---

[14] A filosofia kantiana de antes de 1806, destaca Peter Paret (1989, p. 15) instruiu-o intelectualmente, mas não em seu conteúdo; ao começar a pensar em escrever um estudo que iria explorar toda a guerra, o general teria escolhido como modelos intelectuais as obras O Espírito das Leis, de Montesquieu, e Crítica da Razão Pura, de Kant. Clausewitz também teria seguido influências metodológicas de Hegel para compreensão da História, numa utilização modificada da tese e antítese para se explorar características específicas de um fenômeno particular com maior exatidão. Bernard Brodie (1989, p. 48), ao analisar a importância de Da Guerra, também destaca que naquela época À Paz Perpétua (1795) de Kant e a ideia de que a guerra era inerentemente maléfica já repercutiam significativamente, mas que a visão pacifista gozava imensuravelmente de menos aceitação do que na atualidade.

[15] Anatole Rapoport (2010, p. LXV-LXVII) fala sobre isso ao dizer que na militarização norte-americana passou a adotar um ponto de vista neoclausewitziano, com divergências em relação à teoria clássica naturalmente devido a aspectos políticos e tecnológicos das guerras do século XX. Além disso, sem muita dificuldade é possível encontrar referências a Clausewitz em diversos documentos acadêmicos e doutrinários das escolas militares da atualidade. O prussiano é corriqueiramente citado como teórico da guerra, como elementar para se compreender os princípios em situações de conflito armado (CINELLI, 2016, p.114-115).

[16] "A guerra, então, não é apenas um verdadeiro camaleão, que modifica um pouco a sua natureza em cada caso concreto, mas é também, como fenômeno de conjunto e relativamente às tendências que nela predominam (...)" (CLAUSEWITZ, 2010, p. 30).

A natureza mutante da guerra, nas décadas recentes, tem sido explicitada por diversos elementos que trazem à tona a tese das "novas guerras", que vão além dos conflitos nomeadamente interestatais e da força militar por meios tradicionais. Os Estados perderam o monopólio da guerra, emergiram atores paraestatais e privados[17], e a característica principal das "novas guerras" passou a ser a assimetria – "de forças, tamanho, armas, estratégias, recursos, legitimidade, etc.[18]" entre as partes em conflito, o que por vezes pode suscitar a dificuldades de emprego de normas humanitárias e ao crescente número de vítimas civis (THÜRER, 2011, p. 245-247).

1.2 Novas tecnologias de guerra e o espaço cibernético

A guerra passa por atualizações. Sempre passou, acatando transformações nas suas condutas diante da dinâmica social. É observando essa premissa que o historiador John Keegan (1993, p. 10) descortina a noção clausewitziana ao dizer que a guerra não é a continuação da política por outros meios, pois a guerra precede o Estado, a diplomacia e a estratégia, e se concretiza ao longo da história como expressão de culturas[19]; onde as tecnologias de guerra refletidas na criação e aprimoramento de armas e estratégias implicavam em superioridade em relação ao adversário[20]. À parte dos infindáveis debates filosóficos sobre o que é a guerra, sua origem, e sobre por que o homem recorre a ela, a guerra mostra-se sujeita às condições sociais e situa a tecnologia como "processo de adaptação ao ambiente por novos produtos e processos atinentes aos meios de força" (DUARTE, 2012, p. 30).

A tecnologia é relevante para a tática e estratégia bélica sob o prisma de seus efeitos. Assim, há uma natureza e essência na guerra que a tecnologia não é capaz de alterar, mas apenas influir. É sob esse olhar que a guerra deve ser compreendida como expressão social e instrumento da política (DUARTE, 2012, p. 31-32) ou, da inversão do aforismo clausewitziano

[17] Daniel Thürer (2011, p. 246) detalha: "Para-State and private actors, completely detached from State structures, now occupy the stage: local warlords, rebel groups, private military and security companies, international terror and criminal networks are only the most prominent among them. These non-State actors develop their own military and economic structures and, as a result, enjoy a great deal of autonomy".

[18] Fundamental inequalities in force, size, weapons, strategies, resources, legitimacy, etc. are an attribute of virtually all new wars. (THÜRER, 2011, p. 246).

[19] Vitelio Brustolin (2019, p. 653), por sua vez, ao analisar a definição de guerra baseada em Clausewitz, alega que não importa se a guerra provém da cultura, pois a política, pelo soldado prussiano, engloba a cultura, já que aquela é a "representante de todos os interesses da comunidade" (CLAUSEWITZ, 2010, p. 873); a guerra, logo, é um fenômeno de natureza social, e não há como falar em guerra antes de se falar em comunidades.

[20] Keegan (1993) faz um percurso da história da guerra, donde cita desde instrumentos de pedra preliminarmente como arma de caça, o trabalho do homem com metais, o advento da pólvora, a utilização de cavalos, etc., e o desenvolvimento de armas nucleares, assim como a tendência tecnológica no modo de guerrear.

trazida por Michel Foucault (2005, p. 22), em que "a política é a guerra continuada por outros meios", enquanto controle da violência pelos Estados frente às relações de poder que se manifestam pela política[21]. Ademais, Clausewitz[22] já delineava a (des)informação – ou inteligência[23] – como elemento de poder, que possui grande importância para a condução das operações nos campos de batalha, aliada à obtenção de vantagens e superioridade geral em detrimento do inimigo.

Sob o olhar tecnológico, e adentrando aos tempos hodiernos, o processo de globalização iniciado no último quartel do século XX incrementou o desenvolvimento de novas tecnologias em nível acelerado e evidenciou ainda mais a lógica de "informação como poder" deslindada desde a criação da cibernética pelo cientista Norbert Wiener (1894-1964) em meados da década de 1940, ao fim da Segunda Guerra Mundial. Ao estudar as ramificações da teoria das mensagens enquanto meios de dirigir a sociedade e a maquinaria, e o desenvolvimento das máquinas a partir da psicologia, do sistema nervoso e do método científico, Wiener (1965, p. 15) cunhou o termo "cibernética[24]" a partir das pesquisas sobre controle e comunicação entre animal e máquina[25] e possibilitou o surgimento do que hoje se tem nas ciências da tecnologia da informação.

As últimas décadas do século XX marcaram o início da difusão das novas tecnologias e representaram o cerne da Revolução da Tecnologia da Informação (CASTELLS, 2011, p. 76), que atingiu proporções ainda maiores quando da criação e desenvolvimento da *internet* a partir da década de 1970 e tem se manifestado e se desenvolvido sobremaneira ao longo do século vigente. Fruto da "fusão singular de estratégia militar, grande cooperação científica, iniciativa tecnológica e inovação contracultural" (CASTELLS, 2011, p. 82), a difusão da *internet*

---

[21] "Portanto: a política é a guerra continuada por outros meios. Há nessa tese – na própria existência dessa tese, preliminar a Clausewitz – um tipo de paradoxo histórico. Com efeito, pode-se dizer, de modo esquemático e um pouco grosseiro, que, com o crescimento, com o desenvolvimento dos Estados, ao longo de toda a Idade Média e no limiar da época moderna, viram-se as práticas e as instituições de guerra passarem por uma evolução muito acentuada, muito visível, que se pode caracterizar assim: as práticas e as instituições de guerra de início se concentraram cada vez mais nas mãos de um poder central [...]" (FOUCAULT, 2005, p. 55); em alusão à guerra como instrumento do poder estatal.

[22] Seja a informação obtida por meio do povo – os habitantes – em cooperação voluntária (CLAUSEWITZ, 2010, p. 493), ou a informação proveniente de diversas fontes, como "mapas, livros, memórias" (Ibidem, p. 68), etc.

[23] Aqui, outra possível diferenciação entre a obra traduzida para o português e a obra em língua inglesa: "A informação na guerra" (CLAUSEWITZ, 2010, p. 79) e "Intelligence in War" (CLAUSEWITZ, 1989, p.117).

[24] A palavra "cibernética" foi escolhida por derivar do grego *kubernetes*, que significa "piloto" ou "controle", aquele que assume a função de governar e corrigir o rumo frente às influências externas (WIENER, 1948, p. 15-16).

[25] O matemático norte-americano possibilitou o pontapé do pensamento sistêmico da complexidade na cibernética ao aproximar a mecânica e a neurologia, traçando o estudo do controle e da comunicação nos animais e nas máquinas e dando especial atenção ao princípio de realimentação na engenharia, o *feedback*, o qual permite o acompanhamento do sistema de informações de uma máquina, seus desvios e desempenho desejado, e suas semelhanças com o processo circular do sistema nervoso central humano (WIENER, 1948, p.112-114).

notabilizou um novo domínio que já era sintomático do início da Era da Informação: o espaço cibernético, ou ciberespaço.

O estudo do espaço cibernético não comporta tão somente a noção de ambiente virtual e suas relações em rede pelo uso da *internet*, mas por vezes alcança a percepção de "domínio global[26]" em que a rede de computadores e as conexões pela *internet* nele estão inseridos. Com olhar panorâmico, pode compreender

> [...] um domínio global dentro do ambiente da informação, cujo caráter distinto e único é moldado pelo uso da eletrônica e do espectro magnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas usando tecnologias de informação e comunicação.[27] (KUEHL, 2009, p. 27, tradução nossa)

E por vezes pode ser simplificado como um ambiente de informação composto por dados digitalizados que são criados, armazenados e compartilhados, onde a virtualidade se faz como continuação do físico, das ações provenientes de comandos a computadores, sistemas e infraestruturas que permitem o fluxo das informações (SINGER; FRIEDMAN, 2014, p. 13-14).

Fato é que o advento desse novo domínio e suas novas formas de comunicação alteraram a sociedade tanto positivamente quanto negativamente. As facilidades oferecidas são inúmeras, e repercutem nas inovações e avanços na saúde, no fornecimento de água, energia, na prestação de serviços essenciais diversos, no fortalecimento de instâncias democráticas, etc., dentro da lógica da sociedade em rede[28]. Entretanto, as áreas cinzentas que permeiam o espaço cibernético e os riscos que se nutrem pelo surgimento de ameaças em um domínio tão incerto têm demonstrado proporções que atravessam os fundamentos da soberania estatal vestfaliana e que urgem por novas considerações à luz de uma sociedade internacional cada vez mais complexa[29].

---

[26] À ideia de *global domain*, pode ser debatido o questionamento feito por alguns pesquisadores sobre o ciberespaço ser uma nova espécie de *global common*, ou seja, um bem comum, área ou domínio que não é governado por nenhuma jurisdição política ou Estado específico (CHERTOFF, 2014, p. 10); essa problemática é comentada, inclusive, no Manual de Tallinn 2.0, ao tratar da soberania dos Estados, territorialidade e jurisdição diante de atividades cibernéticas (SCHMITT, 2017, p. 12). Contudo, tal discussão será melhor abordada a *posteriori*, quando nesta pesquisa estiver sendo analisada a atribuição de autoria de ações no espaço cibernético – terceiro capítulo.

[27] […] cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies. (KUEHL, 2009, p. 27).

[28] Manuel Castells (2011) aborda as diversas dimensões da globalização e seus efeitos, positivos e negativos, no que na atualidade se tem por "sociedade em rede".

[29] Uma das características do espaço cibernético e sua difusão é a potencialização da complexidade da sociedade internacional pela constatação da gama de sistemas legais e da heterogeneidade de atores globais, que se relacionam de forma interativa no ambiente virtual (BARROS, 2015, p. 163). O ciberespaço evidencia como a tradicional lógica vestfaliana de soberania estatal e dos Estados como únicos atores das relações internacionais não é suportada na contemporaneidade.

O termo "domínio" é largamente usado nas discussões sobre segurança e defesa dos Estados e nas produções acadêmicas das Relações Internacionais em alusão à competência estratégica e ao lugar em que ocorre o conflito, como o "campo de batalha", ou domínio bélico. A diferenciação entre os domínios existentes decorre da maneira como podem ser utilizados pelo homem, de como são explorados para operações e atividades com intuitos diversos, militares, econômicos, políticos ou sociais. Nesse sentido, Daniel T. Kuehl (2009, p. 24-25) explica a existência de quatro domínios: terrestre, marítimo, aeroespacial e geoespacial, que foram explorados e se difundiram ao longo da existência humana. Mais recentemente passou-se a adicionar o quinto domínio[30], o cibernético, o ciberespaço.

Na atualidade, o espaço cibernético é amplamente utilizado pelos indivíduos, Estados, organizações internacionais, grupos criminosos, etc. Há uma gama de atores com fácil acesso ao ambiente e, sobretudo após o cenário de isolamento social ocasionado pela pandemia da COVID-19, quase todas as atividades exercidas pelos cidadãos são permeadas pelo espaço cibernético. Também palco de manifestações políticas, sociais, etc., a exemplo das mobilizações da Primavera Árabe impulsionadas pelas mídias sociais, na última década o espaço cibernético tem sido bastante utilizado como instrumento de persuasão social e psicológica, de divulgação de *fake news*, e de expressão do poder de influência na opinião pública.

A influência estratégica que pode ser exercida pelo espaço cibernético transformou não só a forma como se atua nos demais domínios, como trouxe à tona a existência do "poder cibernético", *cyberpower*, enquanto "capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em todos os ambientes operacionais e entre os instrumentos de poder"[31] (KUEHL, 2009, p. 38, tradução nossa). Dessa forma, o ciberespaço e o *cyberpower* mostram-se dimensões de um instrumento informacional de poder que tem sido utilizado por diversos atores com vistas aos objetivos político, militar, econômico, etc., num cenário de transição e de difusão de poder[32] que marca a Revolução da Informação no século XXI e seu impacto no sistema internacional (NYE JR., 2011, p. 113-114).

---

[30] Sobre a existência de um quinto domínio, apartado dos demais, são tecidas ponderações. Os argumentos no sentido de assim qualificá-lo, observam Cepik, Canabarro e Ferreira (2015, p. 25), podem implicar no risco de ofuscar a maleabilidade inerente de seus componentes. Entretanto, os autores reconhecem que tem se tornado comum nos últimos anos designar os incidentes cibernéticos como ocorrendo no "quinto domínio", o novo teatro de operações, como se vê na Estratégia de Defesa Nacional dos EUA, de 2005, e como tem sido difundido por intelectuais, militares, mídia, etc. (CEPIK; CANABARRO; FERREIRA, 2015, p. 22).

[31] [...] the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power. (KUEHL, 2009, p. 38).

[32] O cientista político Joseph Nye Jr., na obra *The Future of Power,* discute o poder nas relações internacionais diante da Revolução da Informação que tem se manifestado no século XXI, e também manifesta a tendência para o declínio da soberania vestfaliana: "Two types of power shifts are occuring in this century: power transition and

O poder cibernético, como fruto do desenvolvimento tecnológico informacional que alcança públicos em proporções antes inimagináveis, levou à mudança significativa do conceito de uma guerra clássica, e adentrou às ferramentas de guerra híbrida. Quando se reflete sobre as interferências de informações nas plataformas sociais e sobre o potencial estratégico de ações no meio cibernético como ferramenta para a consecução de objetivos, é notória a tendência de exploração do espaço cibernético, quer seja por atores estatais ou por atores não-estatais. Da compreensão de guerra híbrida como termo que descreve "guerra" em amplo espectro, e que emergiu após as tensões geopolíticas da Guerra Fria, o espaço cibernético tem sido amplamente utilizado para se exercer influência e obter vantagens unindo meios convencionais e não convencionais (ABDYRAEVA, 2020, p. 12-13).

Dentro da lógica de guerras híbridas, o espaço cibernético pode servir em prol de pressão comercial ou financeira entre os atores; pode servir como palco de campanhas de propaganda ou de desinformação (espalhando *fake news*, teorias conspiratórias, etc.); pode colaborar para manipulação de psicológica e social de indivíduos e povos; assim como pode ser teatro de ataques cibernéticos onde se almeja modificar, obter, interromper, destruir, etc., dados ou informações dispostas no ambiente para fins diversos, geralmente coadunando com ilícitos (ABDYRAEVA, 2020, p. 14-15).

De toda sorte, por mais que o espaço cibernético proporcione uma nova visão sobre os conflitos geopolíticos, quando é direcionada atenção especial à segurança humana, há que se ponderar sobre a gravidade das ações em seu escopo, até certo ponto diferenciando o que pode ser artifício de uma "guerra" da informação em sentido amplo – como o que se vê pela influência, por exemplo, exercida pelas redes sociais, na atualidade um dos instrumentos mais importantes de guerra híbrida devido ao seu poder de construir crenças e compreensão pública, e também de moldar as percepções e atitudes públicas em relação a questões políticas e sociais –, e o que pode ser um ataque cibernético de altas proporções que devidamente justifique o emprego do termo "guerra cibernética" invocando as Leis da Guerra do direito internacional.

Quando considerado como novo domínio bélico por atores e autoridades internacionais[33], contudo, assume-se que o espaço cibernético está sendo visualizado como

power diffusion. [...] The problem for all states in today's global information age is that more things are happening outside the control of even the most powerful states. […] States will remain the dominant actor on the world stage, but they will find the stage far more crowded and difficult to control. A much larger part of the population both within and among countries has access to the power that comes from information" (NYE JR., 2011, p. 113-114).

[33] Também podem ser citados o Ministério da Defesa da Holanda, a Organização do Tratado do Atlântico Norte, além de documentos do Departamento de Defesa dos Estados Unidos da América, etc., como aqueles que já descreveram o espaço cibernético como o quinto domínio bélico, após os domínios terrestre, marítimo, aéreo e espacial. (SCHMITT, 2017, p. 12).

aspecto de inovação nos conflitos armados, como ambiente onde se verificam novos meios e métodos de se travar um conflito bélico. Ou seja, é visto enquanto espaço em que a utilização intensa de instrumentos cibernéticos – computadores, dispositivos diversos ligados à tecnologia da informação, às redes, etc. – se mostra cada vez mais militar, implicando em modificações no viés estratégico e tático, e nas estruturas de defesa e segurança dos Estados para lidar com possíveis guerras.

Há quem conjecture que os meios e métodos que levam a consubstanciar a guerra cibernética constariam como vertente da Revolução nos Assuntos Militares[34] (RAM), em conjunto com o advento da Informação Artificial (AI) e outras inovações científicas, levando à lógica das "novas guerras" ou das "guerras do futuro" (PINHEIRO, 2018; CINELLI, 2016, p. 131-136; MOTA, 2018, p. 89-98; GAMA NETO, 2017). É o que se imagina com o desenvolvimento de armas autônomas[35], armas hipersônicas[36], operações cibernéticas[37] e aplicações militares da biotecnologia, que figuram como as preocupações mais recentes na matéria dos riscos de segurança global e de controle de armas pelo direito internacional (SOSSAI, 2021, p. 325).

A introdução de novas tecnologias e técnicas de guerra exige a revisitação das normas de direito internacional contemporâneas que visam limitar a condução de hostilidades, por vezes invocando debates mais aprofundados sobre o papel e uso da tecnologia em questão. Isso é notado, por exemplo, pelas discussões articuladas a partir do espaço cibernético como domínio bélico e com a criação de armas autônomas; duas novas tecnologias que têm sido

---

[34] Observa Carlos Cinelli (2016, p. 131-132) que a Revolução dos Assuntos Militares reflete a transformação militar instigada sobretudo ao término da Guerra Fria, com mudanças organizacionais importantes que justificam o advento do "pós-modernismo militar", caracterizado pela interdisciplinaridade de áreas do conhecimento humano e pela execução de tarefas, na seara das forças armadas dos Estados, que não seriam tradicionalmente consideradas militares. Todavia, a temática da RAM é bastante controversa, como se vê pelas análises de Leandro Gonçalves (2015); o historiador defende que a transformação da guerra ocorre de maneira gradual, lenta e cumulativa, em oposição à tese de mudanças abruptas e onde a tecnologia é condicionante da transformação. Asseverar que somente a tecnologia basta para reconhecer o cenário de mudanças, de "novas guerras" ou a tese de RAM como subproduto do progresso tecnológico, por vezes mostra-se insuficiente: "não há rupturas revolucionárias na história da guerra, há sim uma longa história evolutiva dinamizada pelos enfrentamentos nos que prevalece o lado beligerante que melhor consiga adaptar sua estratégia, tática e empregos dos meios na arte da guerra" (GONÇALVES, 2015, p. 32).

[35] Qualquer sistema com autonomia em suas funções críticas, como aqueles que podem selecionar (procurar, detectar, identificar, rastrear, selecionar) e atacar (usar força contra, neutralizar, danificar ou destruir) alvos sem intervenção humana (CICV, 2016).

[36] Antiga ambição armamentista da Guerra Fria, as armas hipersônicas são veículos propulsores que ultrapassam a velocidade do som, e possuem trajetória considerada imprevisível quanto ao alvo. Da dificuldade de se vincular a uma rota, os sistemas de defesa antimísseis por vezes não conseguem interceptar esse tipo de arma, que pode ser equipado com ogivas atômicas e implicar numa nova ameaça nuclear. Rússia, EUA e China estariam em uma "corrida" para desenvolvimento da tecnologia. (BOYD, 2019).

[37] A noção de operações cibernéticas e a qualificação como "ataque" ou "arma" para o direito internacional é introduzida ao longo do item 1.3 e melhor abordada no segundo capítulo.

bastante abordadas academicamente e que estão em ênfase na agenda global[38], dados os impasses na aplicação das normas existentes e os riscos à proteção humana frente a conflitos em que o contato físico humano tem se tornado cada vez mais raro.

Historicamente, as tecnologias, como conjunto de técnicas e habilidades, sempre estiveram presentes nos conflitos, e suas inovações por uma das partes frequentemente implicavam na superioridade em relação ao adversário. Contudo, o que as novas tecnologias que têm emergido desde o século anterior explicitam é a busca de "guerras mais limpas", em contraposição aos conflitos sanguinários que marcaram a Primeira e Segunda Guerras Mundiais. O advento da tecnologia nuclear e a possibilidade de um "holocausto planetário[39]", que paradoxalmente teve o efeito de "cancelar" conflitos armados globais de grande escala entre grandes potências – condição que marcou a primeira metade do século XX –, exibe bem a perspectiva de guerras instantâneas a que as novas tecnologias se propõem (CASTELLS, 2011, p. 547).

Nesse ínterim, por mais que categoricamente vigore a proibição ao uso da força e a ilicitude da guerra de agressão nas relações internacionais desde o advento da Carta das Nações Unidas de 1945, o aprimoramento da capacidade militar pelas novas tecnologias é uma realidade, e espelham uma visão estratégica de esforços para se encontrar meios de ainda se fazer a guerra, dessa vez em versões que sejam mais "aceitáveis para a sociedade[40]": *a priori* não envolvendo civis, logo, com a prevalência de exércitos profissionais e qualificados; sendo o mais breve possível, com vistas a evitar consumir recursos humanos e econômicos e a desviar-se de questionamentos sobre a justificativa da ação militar ao longo do tempo; e devendo ser supostamente limpa, cirúrgica, "com destruição até mesmo do inimigo, mantida dentro de limites razoáveis e escondida o máximo possível da visão pública, com a consequência de ligar intimamente manuseio de informações, formação de imagem e prática da guerra" (CASTELLS, 2011, p. 548).

Todas essas características parecem se manifestar pelo aprimoramento da capacidade tecnológica militar, maiormente em relação às armas autônomas e ao uso de operações

[38] O Comitê Internacional da Cruz Vermelha, enquanto organização internacional que tem como uma de suas funções desenvolver o Direito Internacional dos Conflitos Armados (ou DIH), bastante tem promovido discussões sobre sistemas de armas autônomas e sobre operações cibernéticas como novas tecnologias de guerra. No escopo da Assembleia Geral das Nações Unidas também têm sido estabelecidos *Groups of Governmental Experts* (GGE) para as temáticas que permeiam o ciberespaço e os sistemas de armas autônomas letais (KELLENBERGER, 2021, p. 269). Atenção maior a esses colóquios sobre operações cibernéticas será dada no capítulo 3.

[39] Termo utilizado pelo próprio Manuel Castells, em alusão ao Holocausto, Segunda Guerra Mundial.

[40] Manuel Castells (2011, p. 548) enumera três conclusões em relação às condições que tornam a guerra mais aceitável pela sociedade, conforme o pensamento dos "países democráticos desenvolvidos" e seus interesses geopolíticos.

cibernéticas. Corriqueiramente, entende-se que "operações cibernéticas" englobam aquelas ações contra ou via computadores, sistemas de computadores ou da informação e outros meios de fluxo de dados. Tais poderiam ter intuitos diversos, desde a infiltração em um sistema alheio para coletar, exportar, destruir, alterar, criptografar, etc., dados, até para se acionar, alterar ou, de algum modo, manipular processos controlados pelo sistema infiltrado. O objetivo dessas operações (ou ataques cibernéticos, em amplo aspecto) pode, conforme o contexto, conotação e os efeitos que se deseje atingir[41], estar vinculado a motivações econômicas, culturais, políticas, militares, etc. (ISLAM, 2017, p. 103).

As operações cibernéticas[42], em particular, e enquanto consequência do uso do espaço cibernético, levam a um impasse sobre a qualificação dessas como "ataque"[43] ou como "ato de guerra" propulsor daquilo que aqui é denominado guerra cibernética, ameaça que permeia o século XXI e que traz um novo olhar sobre os riscos humanitários do uso bélico de um domínio tão abstrato e largamente utilizado por populações civis e pelas infraestruturas críticas[44] dos Estados.

1.3 Propostas para definir a guerra cibernética

A definição de guerra cibernética não é uníssona entre governos e doutrinadores. Partindo da ideia de "guerra" por Clausewitz, imagina-se um cenário de violência organizada, de conflito armado entre Estados por motivos de origem política. As acepções clausewitzianas de guerra como "duelo em grande escala", "ato de força para obrigar o nosso inimigo a fazer a nossa vontade", e "continuação da política por outros meios" (CLAUSEWITZ, 2010, p. 7, 27) têm sido utilizadas por alguns pesquisadores – às vezes inadvertidamente – para tentar desmistificar e conceituar o cenário de violência no espaço cibernético.

---

[41] A exemplo, levando a destruição, alteração ou interrupção de indústrias, infraestruturas, sistemas de telecomunicação ou sistemas financeiros (ISLAM, 2017, p. 103).

[42] Operações cibernéticas até aqui devem ser vistas de forma correlatas a ataques cibernéticos em amplo aspecto (como ações por meio cibernético com caráter ofensivo). Posteriormente, e ao longo desta pesquisa, o emprego do termo será restringido à conotação militar, ou em contexto de conflito armado para o DIH.

[43] Seja como uso da força, ou "ataque armado" no bojo do *jus ad bellum*, previsto na Carta da ONU, ou como "ataque" – atos de guerra – para os conflitos armados em vigência, sob o *jus in bello*, vide art. 49 (1) do Protocolo Adicional I às Convenções de Genebra, de 1977 (CICV, 2017, p.38); tema discutido ao longo da pesquisa.

[44] Sistemas físicos, ou virtuais, de ativos e serviços que são vitais para os Estados e populações; sua incapacitação ou destruição podem debilitar a segurança, economia, saúde, meio ambiente, etc., diversos recursos (SCHMITT, 2017, p. 564). O Decreto nº 10.569, de 2020, que aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas no Brasil, introduz: "As infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País. Fatores que prejudiquem o adequado fornecimento dos serviços provenientes dessas infraestruturas podem acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente." (BRASIL, 2020).

Nesse caminho é que Paulo Shakarian, Jana Shakarian e Andrew Ruef (2013, p. 2) asseveram a dificuldade de se definir guerra cibernética e de, diante da gama de sujeitos capazes de atuar no espaço cibernético exercendo influência – onde cita-se o movimento islamista Hamas, o Hezbollah, e organizações mais recentes voltadas ao domínio cibernético, como Anonymous e LulzSec[45] –, chegar a um consenso sobre a guerra cibernética como uma extensão da política por ações realizadas no espaço cibernético, supostamente desenvolvendo o raciocínio clausewitziano.

> A guerra cibernética é a extensão da política por meio de ações tomadas no espaço cibernético por atores estatais ou não estatais que constituem uma séria ameaça à segurança de uma nação ou são conduzidas em resposta a uma ameaça percebida contra a segurança de uma nação[46] (SHAKARIAN et al., 2013, p. 2, tradução nossa).

O cientista político Thomas Rid (2013, p. 1-3), por sua vez, apegando-se a uma das perspectivas clausewitzianas de guerra, nega a viabilidade do termo "guerra cibernética", alegando três critérios do general prussiano para se reconhecer um ato de guerra: o caráter violento, com reflexos físicos e/ou potencialmente letais; o caráter instrumental, de sorte que deve haver meio e fim na guerra, a violência física ou a ameaça da força são os meios, e forçar o inimigo à vontade do ofensor é o fim; e o caráter ou natureza política, que traz o propósito do meio guerra. Para Rid (2013, p. 4), nenhuma ofensa cibernética poderia atender aos três critérios, que consubstanciam o uso da força e, portanto, não se falaria em guerra cibernética, termo que corresponde a uma "metáfora cansada e perdida"[47].

Fato é que uma série de ameaças podem ser percebidas no espaço cibernético, e, não necessariamente elas repercutem em danos físicos ou possuem uma conotação instrumental e fins políticos. Assim como o próprio conceito de "guerra" é problemático e de debate atemporal, as abstrações do ciberespaço tornam a concepção de ameaças cibernéticas ao nível bélico bastante controversas, sobretudo se fixadas a uma interpretação tradicional e estrita.

Richard A. Clarke e Robert K. Knake, dois dos precursores nos estudos das vulnerabilidades do espaço cibernético e de reconhecimento desse como domínio bélico, conceituam a guerra cibernética como "ações de um Estado-Nação para penetrar nos

---

[45] Grupos ou comunidades de *hackers* considerados ativistas, conhecidos mundialmente por realizar ataques cibernéticos. É controversa a possibilidade de qualificá-los como "grupo organizado", vez que constantemente são apresentados como uma comunidade descentralizada, sem definição hierárquica, etc. Ademais, tratar da (im)possibilidade de qualificá-los requer debate aprofundado, para além dos objetivos deste trabalho.

[46] Cyber war is an extension of policy by actions taken in cyber space by state or nonstate actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security. (SHAKARIAN et al., 2013, p. 2).

[47] […] the tired and wasted metaphor of "cyber war". (RID, 2013, xvi).

computadores ou redes de outra nação com o objetivo de causar danos ou interrupções" (2010, p. 6, tradução nossa[48]), voltando-se à importância da proteção à segurança nacional por mecanismos de segurança e defesa cibernética.

A conceituação de guerra cibernética como envolvimento de Estados em operações cibernéticas, sem especificar a natureza das mesmas, é demasiado abrangente. Ao mesmo tempo, compreender o fenômeno como restrito apenas à atuação direta do ator originário, em pleno cenário de globalização e complexidade das relações interativas no ciberespaço, por vezes pode ser demasiado reducionista. O que se quer dizer é que nem toda e qualquer atividade em meio cibernético levaria à caracterização de uma guerra cibernética; e que a definição de guerra cibernética, restrita tão somente às atividades militares nomeadamente estatais com uso de computadores, redes e sistemas para alcançar seus objetivos estratégicos, dissimula problemas de abstração do mundo virtual e a evasão de responsabilidades pelos ilícitos.

Há que se reconhecer a possibilidade de interpretação ampla do fenômeno "guerra cibernética", considerando uma realidade de conflitos no ciberespaço e a vasta influência de novos atores na sociedade internacional. Afinal, na contemporaneidade, uma variedade de atores tem acesso às ferramentas e técnicas do ciberespaço – onde se incluem Estados-Nação, indivíduos, empresas, grupos de crime organizado, terroristas, etc. – e podem se inserir em situações de conflito cibernético. Da mesma forma, há uma grande variedade de motivações para realização de ataques cibernéticos[49], incluindo pessoal, financeira, militar e/ou política. (LIN, 2012, p. 515).

É compreensível o emprego do termo "guerra cibernética" de forma abrangente, tendo em vista que a própria expressão "guerra" é utilizada para descrever uma pluralidade de condições e comportamentos, desde contestações simbólicas locais até o estado de conflito armado entre nações (SINGER; FRIEDMAN, 2014, p. 120). Entretanto, caminhando para a questão da aplicabilidade do direito internacional aos conflitos no espaço cibernético, sobretudo em relação à Carta da ONU de 1945 e às Convenções de Genebra de 1949 e seus Protocolos Adicionais, o vocábulo aqui é visualizado de maneira delimitada, para que seja possível a vinculação a normas que circunscrevam condutas específicas à realidade enfrentada, e para que se permita a verificação e eficácia de instrumentos protetivos.

A noção de guerra como fenômeno a ser regulado, para o direito internacional contemporâneo, demonstra que a tradicional definição de linhagem clausewitziana, como

[48] When the term "cyber war" is used in this book, it refers to actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. (CLARKE; KNAKE, 2010, p. 6).
[49] O conceito de ataque cibernético será tratado no tópico 1.3.2.

"contenda entre dois ou mais Estados, por meio de suas forças armadas, com propósito de sobrepor um ao outro e impor as condições de paz que agradem ao vitorioso"[50] (OPPENHEIM, 2012, p. 61, tradução nossa) não é suficiente para tentar dirimir os conflitos que se transfiguraram sobretudo no pós-Segunda Guerra Mundial, com o aumento dos conflitos de descolonização, e envolvimento de sujeitos que não são Estados soberanos e que por vezes não possuem forças armadas organizadas. Somando-se à nova conotação requerida para se entender "guerra" no direito internacional, dadas as situações de beligerância que não se enquadrariam na acepção tradicional, o *status* formal do fenômeno, verificável por meio das declarações de guerra, também cedeu espaço à verificação do *animus belligerandi* e da prática de atos de hostilidade (BORGES, 2006, p. 12-13).

Por tais motivos, o termo "guerra" foi substituído após a Segunda Guerra Mundial por "conflitos armados"[51], numa composição que melhor permitiria o abarcamento de situações variadas e afastaria a alegação de sujeitos de inaplicabilidade do Direito de Guerra[52]. Disso, quando se fala em guerra cibernética para o direito internacional, há que se definir se o termo "guerra" está sendo utilizado em sentido originário e estrito – como conflito entre Estados, conflito armado internacional – ou de forma extensiva, inclusive atingindo os denominados conflitos armados não internacionais[53] ou, de maneira ainda mais ampla, referindo-se a todo e qualquer conflito (de qualquer natureza) que se dê pelo espaço cibernético ou em razão desse.

Para os fins desta pesquisa, tem-se como objeto de estudo a guerra cibernética pelo/para o Direito Internacional Humanitário. É o corpo normativo que regulamenta o *jus in bello*, o

---

[50] War is the contention between two or more States through their armed forces for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases. (OPPENHEIM, 2012, p. 61).

[51] Ingrid Detter (2013, p. 20), quando da distinção entre os termos, observa que alguns Estados têm frequentemente negado que estão em "guerra", e por isso preferem a expressão "conflito". À exemplo, a autora cita que, durante a Guerra da Coreia (1950-1953), o Reino Unido negou o envolvimento em uma guerra, posto que não reconheciam a Coreia do Norte como um Estado e, portanto, não se falaria em guerra, já que fenômeno apenas entre Estados reconhecidos.

[52] O *jus in bello*. Aqui, remete-se ao Direito Internacional Humanitário como Direito de Guerra, de maneira que o último esteja contido no primeiro, apesar da terminologia mais adequada em substituição ao "Direito Internacional Humanitário" ser o "Direito Internacional dos Conflitos Armados". Por essa mesma razão diz-se que está contido no primeiro, tendo em vista as novas situações de beligerância e também as possíveis distinções que podem ser feitas doutrinariamente dentro do quadro normativo do Direito Internacional Humanitário, especificamente entre o Direito de Haia e o Direito de Genebra.

[53] O artigo 2º comum às Convenções de Genebra de 1949, tratado em seguida, auxilia na definição do que vem a ser conflito armado internacional, expondo que o conflito armado independe do estado de guerra declarado ou reconhecido por uma das partes; o Protocolo Adicional I às Convenções, de 1977, em seu art. 1º, §4º, também amplia o rol de conflitos armados internacionais para aqueles onde povos lutam contra dominação colonial, contra ocupação estrangeira e/ou contra regimes racistas no exercício do direito dos povos à autodeterminação. Já os conflitos armados não internacionais têm como principais fontes jurídicas o art. 3º comum às Convenções de Genebra e o art. 1º do Protocolo Adicional II às Convenções, e refere-se àqueles que ocorram em território de uma parte contratante, entre as suas forças armadas e forças armadas dissidentes ou grupos armados organizados, os quais tenham como chefia um comando responsável e exerçam controle sobre parte do território de maneira a permitir levar a cabo operações militares contínuas e organizadas. (CICV, 2008).

direito em situação de conflito armado; remete-se à existência de um contexto fático de hostilidades que se seguiram por motivos diversos, por vezes em razão do *jus contra bellum* não ter logrado êxito, ou dentro das possibilidades admitidas pelo *jus ad bellum* no sistema internacional hodierno constituído pelas Nações Unidas. Ou seja, sob o prisma das normas do *jus in bello*, já não se discute os meios que levaram ou as alegações de uma "guerra justa"[54], mas o que pode ser observado para balizar as condutas para que as hostilidades causem o mínimo de sofrimento possível, limitando meios e métodos de combate e, principalmente, protegendo as vítimas dos conflitos.

Por essa razão, o que aqui se aduz como "guerra cibernética" tem ligação estreita com o uso bélico do espaço cibernético. Não obstante se reconhecer que, na Era da Informação e na "sociedade em rede"[55], uma gama de ações e ataques cibernéticos, pelos mais diversos sujeitos, podem ser correntemente designadas como guerra (*lato sensu*), para os fins jurídicos aqui dispostos, o termo deve estar atrelado precipuamente ao uso da força por Estados soberanos e à visualização destes como atos de guerra[56] entre Estados, logo, como conflito armado internacional.

Não é qualquer ato de hostilidade no cenário internacional ou interno de um Estado[57] – a primeira dicotomia a ser estabelecida na aplicabilidade de regramentos de DIH –, praticado por quaisquer sujeitos, seja por meios tradicionais ou cibernéticos, que se consubstanciará numa guerra para a aplicabilidade e invocação de um conjunto de normas de direito internacional. Por isso, para delimitações jurídicas internas e em prol de cooperação entre Estados do que venha

---

[54] Há que se dizer que a doutrina da guerra justa, anteriormente pautada na guerra santa, foi bastante desenvolvida por Santo Agostinho, São Tomás de Aquino, Hugo Grotius e Francisco de Vitória para justificar hipóteses em que o recurso à força seria aceito nas relações internacionais, e, logo, legítimo (GUERRA, 2021, p. 205-206). O termo é aqui colocado em alusão à percepção de que, com o *jus ad bellum* e a possibilidade de uso da força entre os Estados, continua a existir, dentro de suas limitações e novas acepções, uma "guerra justa" (SASSÒLI, 2019, p. 494).

[55] Referindo-se à obra de Manuel Castells (2011), em que o sociólogo aborda o efeito das transformações tecnológicas nas últimas décadas, em especial na área da comunicação, o impacto da informatização sobre as culturas de todo o mundo, e a globalização das atividades econômicas decisivas no panorama estratégico dos mais diversos setores. O espanhol refere-se à Segunda Guerra Mundial como "mãe de todas as tecnologias", período no qual se concebeu o computador e que levou ao surgimento de outros dos principais instrumentos de tecnologia cibernética e à criação e desenvolvimento da *internet* ao final do século XX (CASTELLS, 2011, p. 78-82)

[56] Ver item 2.2.

[57] Aqui, refere-se aos conflitos armados internacionais e aos conflitos armados não internacionais que englobados pelas Convenções de Genebra de 1949 e pelos seus Protocolos Adicionais I e II de 1977, que oferecem a distinção entre conflitos. Mesmo assim, tendo em vista a máxima da proteção da pessoa humana, e, particularmente se observando quão delicado é se delimitar os contornos do que vem a ser uma conflito armado não internacional sem caracterizar afronta à soberania do Estado pela aplicação das regras do direito internacional, tem se notado o "direito de iniciativa humanitária" – como atinente ao Comitê Internacional da Cruz Vermelha – para se estender a aplicação do Direito Internacional Humanitário, especialmente as normas de proteção das vítimas, a diversas situações em que os atos hostis praticados não sejam considerados suficientes para caracterizar um conflito armado (BORGES, 2006, p. 44-45).

a ser a guerra cibernética, é pertinente haver que se restringir ao caráter internacional e ao uso ou permissibilidades do ator estatal[58], para que seja respeitada a soberania e para que se promova o diálogo internacional em prol da prevenção e mitigação de danos.

Todavia, não se olvida que, para o propósito de prevalência da proteção das vítimas de conflitos armados, "o desaparecimento do significado dessa primeira dicotomia no direito de guerra é, logo, bem-vindo"[59] (THÜRER, 2011, p.54, tradução nossa), sobretudo partindo-se da expectativa de que o tratamento de operações cibernéticas como matéria de conflitos armados internacionais posteriormente poderá suscitar o olhar também para uma regulamentação do assunto nos conflitos armados de caráter não internacional.

De todo o exposto, parece mais congruente utilizar-se do termo "guerra cibernética" associado a "operações cibernéticas durante conflitos armados", como tem sido usado pelo Comitê Internacional da Cruz Vermelha (2013; 2019) para melhor visualizar a aplicabilidade das normas humanitárias ao ciberespaço, enquanto os ataques cibernéticos em tempos de paz – como parte de uma guerra híbrida ou não –, possivelmente inaugurando uma guerra cibernética, são debatidos e compõem um problema ainda sem resposta para a sociedade internacional[60].

---

[58] Referindo-se às responsabilidades dos Estados pelas condutas atribuíveis a ele, incluindo possíveis violações a normas de Direito Internacional Humanitário, onde incluem-se condutas que, por mais que não tenham sido encabeçadas pelas forças armadas estatais, tenham sido instruídas, capacitadas, reconhecidas, etc., pelo Estado (CICV, 2019, p. 9).

[59] The vanishing significance of this first dichotomy in the law of war is therefore to be welcomed. (THÜRER, 2011, p. 54). Ainda, percebe-se que a divisão entre conflito armado internacional e conflito armado não internacional na contemporaneidade é bastante tênue: "As these rules are generally the same for both types of armed conflict, the line dividing them is becoming more and more blurred. […] Human beings deserve the same protection, regardless of whether they are affected by a battle taking place within one country or across borders. That is why the Security Council and other international bodies, when demanding respect for international humanitarian law, pay no heed to the legal classification of a conflict. And that is also why the International Criminal Tribunal for the former Yugoslavia refused to apply different standards to different types of conflict." (THÜRER, 2011, p. 52-53).

[60] Como será melhor analisado a *posteriori*, atualmente parece haver um consenso de que o direito internacional se aplica ao ciberespaço, conforme relatórios do *Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security* (anteriormente, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*) e resoluções relacionadas da Assembleia Geral da ONU. Porém diversas questões permanecem em aberto, sobre como operacionalmente o direito será aplicado, dentre elas sobre como será aplicado a ataques cibernéticos em tempos de paz, e sob os auspícios do *jus ad bellum* e Carta da ONU (DIPLO, 2022b). Esta pesquisa tenta se ater às consequências para o *jus in bello* e proteção de vítimas, portanto, não se prende os ataques cibernéticos inaugurando o uso da força e uma guerra no cenário internacional, discussão própria e que faz *jus* a uma investigação particular e ainda mais minuciosa; dessarte, se circunscreverá às normas de proteção de vítimas do DIH e aplicabilidade das mesmas à guerra cibernética.

1.3.1 Problemas de delimitação: entre o *Jus ad bellum* e o *Jus in bello*

Tratar dos motivos que conduziram ao conflito cibernético, nomeadamente à guerra cibernética, requer discussões aprofundadas e voltadas especificamente à mudança das relações políticas internacionais, às novas acepções de poder no cenário mundial e, por consequência, à assimilação de um ataque cibernético como uso da força. Saber quando ou compreender as situações nas quais uma guerra cibernética começa ou termina tende a ser mais desafiador que propriamente defini-la (SINGER; FRIEDMAN, 2014, p. 121) e, por isso, incorporá-la à realidade de conflitos armados já existentes, por ora, é mais factível, não obstante a viabilidade de um ataque cibernético como primeiro ato de uso da força no cenário internacional aproximar-se da iminência.

Entretanto, para assimilar os impasses que o uso do ciberespaço com fins bélicos oferece às Leis da Guerra, cumpre realizar algumas distinções, ainda que exista uma permeabilidade entre os escopos de tratamento que foram acentuados pelas abstrações da cibernética. O Direito Internacional contemporâneo oferece dois tipos de resposta aos desafios da guerra: o conjunto normativo do *jus ad bellum*, e um outro que compõe o *jus in bello*. O *jus ad bellum*, ou direito de se recorrer à guerra, tem como propósito limitar o recurso à força militar, e, referindo-se às normas clássicas de direito internacional que emergiram com a Paz de Vestfália (1648), permitia aos Estados valer-se da guerra em prol da soberania. Após a Segunda Guerra Mundial, o *jus ad bellum* passou por mudanças revolucionárias com a Carta das Nações Unidas proibindo a ameaça ou o uso da força nas relações internacionais, concedendo ao Conselho de Segurança das Nações Unidas (CSNU) o monopólio sobre o uso adequado da força à nível internacional, conforme Capítulo VII da Carta, e restringindo a licitude das ações militares de um Estado contra outro, à parte do uso da força exercido ou sancionado pelo órgão, aos casos de legítima defesa. (THÜRER, 2011, p. 41-42).

O *jus in bello*, por sua vez, limita a escolha de meios e métodos de conflito armado, e volta-se à proteção das pessoas afetadas pelas hostilidades. Na atualidade, seu desenvolvimento está consubstanciado em correntes jurídicas que se relacionam para regular conflitos armados: o Direito da Haia, o Direito de Genebra e o Direito de Nova York, divisão embasada na localidade onde as principais normas foram adotadas. Embora siga a linha do uso da força nas relações internacionais, o *jus in bello* desvincula-se da lógica do *jus ad bellum* por não depender da licitude ou ilicitude do conflito em questão; toma corpo próprio e, hoje caracterizado como

Direito Internacional Humanitário, não julga início do conflito, mas prefere a realidade factual[61] e a igualdade de direitos e obrigações entre as partes envolvidas[62] em nome da proteção humana (BORGES, 2006, p. 23, 48-49; THÜRER, 2011, p. 42-43).

A permeabilidade entre as duas áreas é ressaltada quando doutrinadores, a partir da tentativa de um conceito para a citada guerra, começam a tratar ou perceber problemas, que então se destrincham em diversos outros, como: "quando as operações cibernéticas constituem um "ataque armado" motivando a legítima defesa pelo *jus ad bellum* ou ao menos o uso da força normalmente proibido pela Carta da ONU"?; "quando uma operação cibernética desencadeia a aplicabilidade do DIH"?; "quando uma operação cibernética constitui um ataque para DIH"?. Teoricamente, essas três questões deveriam ser dispostas isoladamente, tendo em vista que as matérias do *jus ad bellum* e do *jus in bello* devem ser mantidas separadamente. Contudo, o que tem se visto é que, "tanto na prática como nas discussões acadêmicas, os mesmos critérios e questões são discutidos em relação a esses três problemas, ainda que sem o reconhecimento expresso de que são realmente os mesmos"[63]. (SASSÒLI, 2019, p. 556-557, tradução nossa).

Isso pois o surgimento de novas tecnologias de guerra, tal qual a utilização bélica do ciberespaço, são problemas importantes tanto ao *jus ad bellum* como ao DIH, e, enquanto não são encontradas respostas satisfatórias para ambos, talvez seja pertinente trabalhar as definições cabíveis de forma conjunta[64], para que posteriormente os resultados se mostrem confluentes.

---

[61] "[…] a caracterização jurídica da guerra exigia, via de regra, um reconhecimento dos Estados que atestasse formalmente esse *status* – uma declaração de guerra. Contudo, devido aos diversos problemas que poderiam surgir pela negação dos Estados beligerantes de uma real situação de conflito, como a não-aplicação do DIH nestes casos, "a abertura e cessação das hostilidades não estão submetidas hoje em dia a regras precisas. O conflito armado é um fato mais do que uma intenção"" (DAILLIER, P.; PELLET, A., 2003, p. 982, *apud* BORGES, L. E., 2006, p. 48).

[62] "While under the outdated "just war" doctrine, the rights and duties of the belligerants depended on the question of whether their cause was "just" or "unjust", the *jus in bello* is not linked to, or dependent on, the rules concerning the initiation of hostilities. It is not affected by a breach of the *jus ad bellum*. It regulates warfare, regardless of whether a particular war is "just". Under the *jus in bello*, all the parties to a conflict have the same rights and are obliged to respect the same obligations. Rules of war call for restraint even when an adversary has committed atrocities, or when a State has been the subject of an unjust attack and therefore is reluctant to restrain itself." (THÜRER, 2011, p. 43).

[63] […] in both practice and scholarly discussions, the same criteria and questions are discussed in relation to these three issues without an express acknowledgement that they are actually the same. (SASSÒLI, 2019, p. 557). Marco Sassòli faz tal observação ao comparar o desenvolvimento do tema por Marco Roscini, Michael N. Schmitt e Heather Harrison Dinniss. Ademais, embora corpos normativos distintos, Carta da ONU e DIH são complementares no que refere a proteção humana diante da guerra e seus efeitos (GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 332).

[64] É o caminho que parece estar sendo seguido, por exemplo, nas discussões do *Group of Governmental Experts* (GGE) e do *Open-Ended Working Group* (OEWG) no escopo das Nações Unidas sobre a matéria de informação e telecomunicação no contexto de segurança internacional e responsabilidades no ciberespaço. Tais serão melhor abordados no terceiro capítulo desta pesquisa, em tópico voltado aos avanços na matéria de políticas públicas internacionais para os assuntos que permeiam as guerras cibernéticas.

Afinal, supondo que as questões relacionadas ao DIH sejam solucionadas de forma satisfatória, os impasses sobre até que ponto as novas tecnologias de armas aumentam a possibilidade de guerras serem desencadeadas ou escaladas e sobre até que ponto elas aprofundam a natureza assimétrica dos conflitos armados, persiste (KELLENBERGER, 2021, p. 269). De toda sorte, voltando-se aos riscos aferidos pela utilização descomedida do novo domínio bélico e à prevalência da proteção humana, uma definição já adstrita ao contexto de conflito armado possibilitaria conclusões mais nítidas sobre a aplicabilidade e operacionalidade das normas de proteção às vítimas das guerras cibernéticas.

1.3.2 Os ataques cibernéticos e as ameaças: o caminho até a guerra cibernética

"A guerra cibernética é sempre um ataque cibernético, mas nem todos os ataques cibernéticos são guerra cibernética"[65] (ISLAM, 2017, p. 103, tradução nossa). Essa é a lógica seguida pela pesquisadora Myriam Dunn Cavelty (2010) para conceituar a guerra cibernética a partir da diferenciação entre os tipos de ameaças ou conflitos cibernéticos. A distinção entre as ameaças oferecidas pelos ataques cibernéticos é elementar para se alcançar uma delimitação de guerra cibernética mais adequada à aplicação do DIH.

A guerra cibernética corresponde a uma pequena subseção de todos os conflitos que podem ocorrer no ciberespaço. Dentre conflitos políticos, econômicos e/ou militares que utilizam do espaço cibernético e têm conotação internacional, a noção de guerra cibernética, para que seja útil e para que permita a importante avaliação dos perigos concretos, a atribuição de responsabilidades, a implementação de contramedidas preventivas e reativas, e para que efetivamente se conduzam investigações criminais, deve ser detalhada e particularizada em relação aos demais ataques cibernéticos (CAVELTY, 2010, p. 1).

Um ataque cibernético, em conceito desvinculado das noções de "ataque" pelo *jus ad bellum*[66] ou pelo *jus in bello*[67], sugere "algo que não está autorizado a acontecer"[68] a um

[65] Cyber warfare is always cyber attack but not all cyber attacks are cyber warfare. (ISLAM, 2017, p. 103).
[66] "Ataque armado" pelo art. 51 da Carta da ONU.
[67] "Ataque" pelo art. 49 do Protocolo Adicional I às Convenções de Genebra, de 1977, como ato de violência, ofensivo ou defensivo, contra o adversário do conflito armado. Afirmar que determinadas operações cibernéticas correspondem a "ataques" pelo DIH não necessariamente significa que seriam qualificadas como "ataque armado" pela Carta da ONU. (CICV, 2019, p. 7)
[68] "Sometimes an event that occurs on a computer or network is part of a series of steps intended to result in something that is not authorized to happen. This event is then considered part of an attack. An attack has several elements. First, it is made up a series of steps taken by an attacker. Among these steps is an action directed at a target (an event), as well as the use of some tool to exploit a vulnerability. Second, an attack is intended to achieve an unauthorized result as viewed from the perspective of the owner or administrator of the system involved. Finally, an attack is a series of intentional steps initiated by the attacker. This differentiates an attack from

computador ou rede, sendo uma ação direcionada a um alvo que se utiliza de ferramenta cibernética para explorar uma vulnerabilidade (HOWARD; LONGSTAFF, 1998, p. 11-12), ou, sucintamente, "qualquer ato de um *insider* ou *outsider* que compromete as expectativas de segurança de um indivíduo, organização ou nação", que se sucede por motivações diversas, sejam políticas, de tensão social, religiosa, etc. (GANDHI *et al*., 2011, p. 29, tradução nossa[69]).

Os objetivos e consequências dos ataques cibernéticos variam bastante. Podem intentar efeitos políticos, como pela desfiguração de um site de agência governamental; podem servir para facilitar a prática de ilícitos, como pela alteração de acesso ou de identidades para possibilitar que criminosos passem por barreiras de segurança; podem objetivar danos de maior remonta e de natureza estratégica, como ações voltadas a prejudicar a capacidade de outro país de implementar decisões oficiais para se defender ou para fornecer serviços aos seus cidadãos – como de energia elétrica, assistência médica, etc.(SINGER; FRIEDMAN, 2014, p. 71).

Sob o prisma militar, a guerra cibernética faz parte de uma "guerra da informação"[70], mas a prática tem demonstrado a inviabilidade de se categorizar os ataques cibernéticos em função dos autores envolvidos. Mesmo com a dissimulação e ocultação dos autores de um ataque cibernético, em certa medida é possível qualificar a guerra cibernética de acordo com a intenção dos ataques e com o dano potencial dos mesmos. É o que se propõe com a caracterização de uma "escada cibernética"[71] dos conflitos, em que "quanto mais alto na escada estiver a natureza do ataque, maior será o dano potencial"[72] (CAVELTY, 2010, p. 1, tradução nossa).

---

something that is inadvertent." (HOWARD; LONGSTAFF, 1998, p. 11-12). Os pesquisadores John D. Howard e Thomas A. Longstaff (1998) proporcionam uma visão técnica dos incidentes cibernéticos, analisando as ferramentas possíveis para se atingir uma vulnerabilidade, a ação tomada (modificar, ler, copiar, deletar, etc.) e o alvo (dados, computador, rede, etc.), e os resultados não autorizados (corromper, roubar a informação, etc., inclusive negar o serviço, o *Denial of Service* – DoS, prática realizada no ataque cibernético que ocorreu na Estônia em 2007, caso emblemático quando da tratativa de ataques cibernéticos destinados a uma nação e que estimulou os estudos sobre o advento da guerra cibernética (SILVA; SILVA, 2019, p. 129-133).

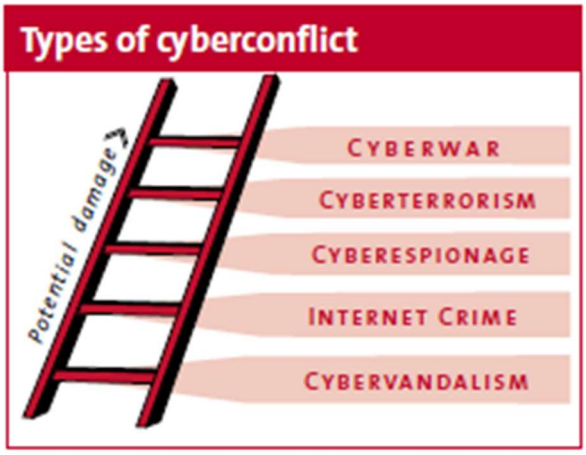
[69] We define a cyber-attack as any act by an insider or an outsider that compromises the security expectations of an individual, organization, or nation. (GANDHI *et al*., 2011, p. 29).

[70] Ou "guerra da (des)informação", onde se difundem "desinformações" com vistas a objetivos diversos. Sobre isso, os professores Marko Milanovic e Michael N. Schmitt (2020) observam a possibilidade de operações de desinformação dirigidas por Estados contra outros Estados durante a pandemia de COVID-19 serem vistas como violações a regras do direito internacional, atingindo a soberania e não-intervenção estatal; dependendo das proporções alcançadas pelas citadas operações de desinformação cibernética, os pesquisadores argumentam a possibilidade de se chegar ao nível de uso da força – sobretudo se tais operações puderem causar danos significativos, destruição, ferimentos ou mortes – e até mesmo de "ataque armado" sob o prisma do art. 51 da Carta da ONU. Um dos exemplos citados é o de se imaginar uma campanha de desinformação destinada a convencer indivíduos a profilaticamente fazer uso de substâncias que os deixem doentes ou os levem à morte, violando a soberania do Estado em que os efeitos se manifestaram; logicamente, haveria que se analisar o nexo e objetividade da conexão causal (MILANOVIC; SCHMITT, 2020, p. 269).

[71] Cyberladder (CAVELTY, 2010, p.1)

[72] The further up the ladder the nature of the attack is, the greater its potential damage. (CAVELTY, 2010, p. 1).

Figura 1 – Escada Cibernética



Fonte: CAVELTY, 2010, p. 2.

A escada cibernética auxilia, a partir de um critério negativo, e diante da inexistência de um conceito uniforme no cenário internacional e das divergências entre os próprios acadêmicos e especialistas das áreas interdisciplinares que se relacionam à cibernética, a se aproximar de uma delimitação para a guerra cibernética[73].

No primeiro degrau da escada cibernética está o vandalismo cibernético, ou "ciberhacktivismo", que se refere à modificação virtual ou destruição de conteúdo, como pelo hackeamento de *sites* ou pela desativação de servidores por sobrecarga de dados. É uma prática cada vez mais comum de conflito cibernético, e geralmente visa chamar atenção do público, possuindo efeitos limitados no tempo e relativamente inofensivos (CAVELTY, 2010, p. 1).

O vandalismo cibernético está ligado a ideia de perturbação, e tem efeitos que normalmente são facilmente revertidos, servindo somente para chamar a atenção da opinião pública. *Hackers* atacando *sites* para descaracterizá-los podem ser aqui enquadrados, à exemplo do que ocorreu com a substituição do logotipo da página do Google Paquistão pela imagem de dois pinguins e da frase em inglês "Paquistão abatido" para despertar a curiosidade do público (BALOCH, 2014, *apud* BARROS, 2015, p. 99-100).

No segundo e terceiro degraus estão os crimes na internet e a espionagem cibernética. Assim como o cibervandalismo, não dependem de conflitos preexistentes para que ocorram. Não obstante as redes governamentais também sejam afetadas, a principal vítima direta nesses casos – sobretudo quando vistos isoladamente – é o setor corporativo, como se vê em práticas

[73] Vide nota 5 desta pesquisa, compreende-se a alegação de obstáculos éticos e políticos e divergências quanto a viabilidade do termo. Todavia, a relevância do tema para a proteção de vítimas pelo DIH não deve ser engessada em razão de tais controvérsias.

de espionagem industrial, roubo de dados corporativos confidenciais, desenhos ou patentes, por exemplo. Nesse sentido, cita-se a Convenção de Budapeste de 2001 sobre Crime Cibernético[74] como instrumento para auxiliar a esclarecer a extensão da cooperação internacional e interestadual entre as jurisdições domésticas afetadas (das vítimas e daquelas donde as atividades criminosas foram perpetradas) e direcionar o combate e retificação das injustiças em caráter transnacional (WHETHAM; LUCAS JR., 2016, p. 167).

Os cibercrimes remetem àquelas práticas já tidas como criminosas que estão sendo cometidas por meios não tradicionais (usando uma rede de computadores ao invés de, à título de exemplo, uma arma), mas englobam também ilícitos emergentes[75] próprios do espaço cibernético (BRENNER, 2007, p. 383-386), e que estão sendo consideradas ilegais pelos ordenamentos. Quando o objetivo é obter informações pessoais ou não-públicas, que podem ser utilizados para diversos intuitos e vantagens, normalmente econômicas e/ou políticas, fala-se na ciberespionagem (SINGER; FRIEDMAN, 2014, p. 93). No caso das espionagens cibernéticas, e para além da espionagem industrial, tem sido notada cada vez mais a prática nas relações internacionais entre Estados, sob a justificativa de "segurança nacional"[76].

Subindo o dano potencial, alcança-se o ciberterrorismo, o terrorismo cibernético. O termo é utilizado para descrever ataques ilegais por atores não estatais contra computadores, redes e informações armazenadas que têm como objetivo intimidar o governo e causar terror na população civil. A *priori*, um ataque cibernético só consistirá em ciberterrorismo se resultar em

---

[74] A Convenção de Budapeste de 2001, tratado internacional sobre crimes cibernéticos, abrange normas penais e define estratégias conjuntas entre os Estados-membros para o enfrentamento de crimes praticados na internet; é tido como um dos mais importantes instrumentos a lidar com aspectos penais, processuais e cooperativos no combate aos crimes cibernéticos em nível transnacional, e atualmente envolve mais de 60 países. Apesar de ter sido projetada para se referir a crimes cibernéticos dentro da jurisdição dos Estados-membros do Conselho da Europa, nos anos mais recentes foi convencionado o convite a Estados que não membros, como o Brasil, convidado desde 2019. Apesar do Brasil ter caminhado para o incremento de suas políticas domésticas de combate a crimes digitais, com o Marco Civil da Internet de 2014, normas gerais de comércio eletrônico e proteção do consumidor online, e com as recentes Lei Geral de Proteção de Dados – LGPD e Estratégia de Segurança Cibernética (pelo Decreto nº 10.222/2020), ainda há que se realizar esforços para a cooperação internacional na matéria da criminalidade digital; as diretrizes da Convenção de Budapeste são salutares nesse sentido. (POLIDO, 2021).

[75] "[...] a better definition of cybercrime is the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain international order. This definition encompasses both traditional and emerging cybercrimes. It also encompasses any use of computer technology, not merely the use of networked computer technology.". Tal definição, genérica, não oferece o predicado legal necessário para responder ao crime cibernético, vez que é definição conceitual de uma categoria de crime, e não a definição de um crime ou ofensas específicas. (BRENNER, 2007, p. 386).

[76] Diversos casos podem ser citados, à exemplo da espionagem realizada pela Agência de Segurança Nacional dos Estados Unidos da América à Petrobrás e descoberta pelo governo brasileiro em 2013 (BARROS, 2015, p. 100). Na mesma época, Edward Snowden, ex-analista da Agência Nacional de Segurança dos EUA, também revelou que centenas de operações de espionagem cibernética haviam sido encaminhadas pelo governo norte-americano nos últimos anos. Outros governos que usariam da mesma tática seriam China e Rússia, apesar das imprecisões na origem dos ataques cibernéticos. (SINGER; FRIEDMAN, 2014).

violência física contra pessoas ou propriedade, ou ao menos causar danos suficientes para criar medo extremo na população (CAVELTY, 2010, p. 1-2).

Susan Brenner (2007, p. 387-389) observa que, como o terrorismo geralmente tem como objetivo desmoralizar direta ou indiretamente uma população civil, disto já se notaria uma das principais diferenças entre terrorismo e guerra[77], pois na guerra não se deve ter como alvo os civis; e o mesmo sentido seria aplicável ao ciberterrorismo e à ciberguerra. Ao menos em teoria, e tradicionalmente, a lógica é verdadeira, visto que numa visualização de guerra como confronto entre exércitos, a morte de civis, os danos materiais e a destruição são considerados eventos colaterais, já que "o foco primário da guerra seria o "triunfo" sobre o(s) Estado(s)-nação adversário(s), o que quer que isso signifique no determinado contexto" (BRENNER, 2007, p. 403, tradução nossa[78]).

Quando finalmente o potencial danoso atinge os níveis mais elevados, e os objetivos coadunam com tal, é que se alcança o degrau da guerra cibernética. A guerra cibernética corresponde a uma subseção da guerra da informação (*lato sensu*), e, no contexto jurídico e militar a que se destina, ao conflito bélico no espaço virtual que envolve principalmente meios de tecnologia da informação. A guerra da informação, conceito mais amplo, trata da influência da vontade e capacidades de tomada de decisão da liderança política e das forças armadas inimigas e/ou das atitudes da população civil no nível informacional – redes, computadores, etc. A guerra cibernética, por sua vez, reflete a natureza cada vez mais tecnológica da guerra como recurso militar, pela informatização e suas virtualidades nas áreas e aspectos das forças armadas[79]. (CAVELTY, 2010, p. 2).

Dessarte, ao tratar da guerra cibernética, refere-se àqueles ataques correlatos a atos de guerra[80], ou à situação de conflito armado[81], pela definição do artigo 2º comum às Convenções de Genebra de 1949, ou pela definição como recurso às forças armadas – como inferido no caso *Prosecutor v. Dusko Tadic*, pelo Tribunal Penal Internacional para a Ex-Iugoslávia (ISLAM, 2017, p. 103):

---

[77] Pertinente mencionar que os atos de terrorismo não abstêm o emprego do DIH. O DIH se aplica a conflitos armados – em prol da pessoa humana, quer sejam reconhecidos ou não, como desenvolvido supra –, e cobre atos de terrorismo cometidos por Estados, grupos armados (que podem ser posteriormente reconhecidos como grupos terroristas) ou indivíduos que apresentem nexo com o conflito armado. (SASSÒLI, 2019, p. 523-524).

[78] The primary focus of war in general and of particular wars is to "triumph" over the adversarial nation-state(s), whatever that means in a given context. (BRENNER, 2007, p. 403).

[79] Aspectos abordados no capítulo seguinte.

[80] Conceito tratado no item 2.2.

[81] Não se trata de uma correlação de fácil acepção, a realidade fática exibe a imprescindibilidade da análise caso a caso; diversos critérios são postos à discussão no início de um conflito armado e na verificação do vínculo de certos atos com um conflito armado já existente. Alguns aspectos dessa discussão constam no segundo capítulo desta pesquisa.

> Artigo 2º - Além das disposições que devem vigorar em tempos de paz, a presente Convenção irá aplicar-se em caso de guerra declarada ou de qualquer outro conflito armado que possa surgir entre duas ou mais Altas Partes Contratantes, ainda que o estado de guerra não seja reconhecido por uma delas.
> A Convenção será igualmente aplicada em todos os casos de ocupação total ou parcial do território de uma Alta Parte Contratante, ainda que essa ocupação não encontre qualquer resistência militar. [...]. (CICV, 2016)

> 70. [...] concluímos que existe um conflito armado sempre que há recurso à força armada entre Estados ou violência armada prolongada entre autoridades governamentais e grupos armados organizados ou entre esses grupos dentro de um Estado. O Direito Internacional Humanitário se aplica desde o início de tais conflitos armados e se estende além da cessação das hostilidades até que uma conclusão geral de paz seja alcançada; ou, no caso de conflitos internos, uma solução pacífica seja alcançada. Até aquele momento, o Direito Internacional Humanitário continua a ser aplicável em todo o território dos Estados beligerantes ou, no caso de conflitos internos, em todo o território sob o controle de uma das partes, independentemente de haver ou não combate efetivo. (ICTY, 1995, tradução nossa[82]).

À situação de conflito armado, e consoante a posição do Comitê Internacional da Cruz Vermelha de guerra cibernética como "meios e métodos de guerra que consistem em operações cibernéticas equivalentes ou conduzidas no contexto de conflito armado, na acepção do DIH" (CICV, 2013, p. 1, tradução nossa[83]) é que o termo aqui é utilizado. Não obstante a possível aplicação e visualização do *jus in bello* a conflitos em que não possuam o caráter interestatal e as dificuldades de atribuição de autoria dos ataques virtuais[84], para fins de enfrentamento do problema por meio de cooperação entre os Estados, esta pesquisa doravante considerará – para fins de delimitação – a "guerra cibernética", ou "operações cibernéticas em situação de conflito armado internacional", maiormente a partir da citada noção de Richard A. Clarke e Robert K. Knake (2010, p. 6), alterando-a para "ações *atribuíveis de responsabilização*[85] a um Estado-

[82] 70. On the basis of the foregoing, we find that an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State. International humanitarian law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, international humanitarian law continues to apply in the whole territory of the warring States or, in the case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place there. (ICTY, *Prosecutor v. Dusko Tadic*, 1995).

[83] The term is used here to refer to means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL (CICV, 2013, p. 1).

[84] A atribuição de autoria, como problema para aplicabilidade do DIH, será melhor tratada no capítulo seguinte.

[85] A lógica de atribuição de responsabilidade estatal que aqui se defende é a mesma apresentada pelo Comitê Internacional da Cruz Vermelha, vide *Position Paper* de novembro de 2019, a que não se refere tão somente a ações diretamente vinculadas às forças armadas do Estado em questão, mas também a ações conduzidas por outros ou terceiros sob os auspícios ou capacitados pelo Estado (CICV, 2019, p. 9). Afinal, das abstrações do novo domínio bélico, a dificuldade de se atribuir a autoria é um problema evidente; somado a isso, a disseminação de meios cibernéticos não é limitada às forças armadas regulares e outros órgãos do Estado (SCHMITT, 2014a, p. 190).

Nação para penetrar nos computadores ou redes de outra nação com o objetivo de causar danos ou interrupções, desde que correlatas à situação de conflito armado *internacional*".

Os termos e lógica da escada cibernética, com o dano potencial crescente até o alcance da guerra cibernética, não isolam os tipos de ataques cibernéticos, que podem coexistir conforme seja possível se verificar o objetivo do ataque[86]. Mas, por possibilitarem uma abordagem terminológica que diferencie os conflitos e ameaças do espaço cibernético, frente ao livre emprego de "guerra cibernética" para quaisquer conflitos no meio virtual, auxiliam na formação de um conceito próprio à aplicação do DIH, e, portanto, adstrito a um cenário de conflito armado.

1.4 Exemplos da praxe

É notório que apenas uma fração das possibilidades de conflito cibernético foi experienciada – ou ao menos reconhecida – no mundo, sobretudo casos de vandalismo, crimes e espionagem cibernética; e que o tema de segurança cibernética passou a ser visto como matéria de segurança nacional e internacional dos Estados mormente após os casos *Wikileaks*[87] e Snowden[88], quando a conotação de defesa cibernética ultrapassou a seara tecnológica e repercutiu nas áreas jurídica e política. Enquanto incidente cibernético internacional, todavia, os ataques cibernéticos sofridos pela República da Estônia, em 2007, ficaram conhecidos como os primeiros ataques dessa natureza direcionados a uma nação (SILVA; SILVA, 2019, p. 128-130).

Em meados de 2007 a Estônia teve servidores de instituições responsáveis pela estrutura da internet, sites governamentais e de partidos políticos (dentre eles, primeiro-ministro, presidente, parlamento e ministério se viram afetados, além do partido reformista e da polícia de fronteira), serviços de internet banking e midiáticos, etc., afetados por ataques cibernéticos. Foram realizados ataques de negação de serviço ou *Denial of Service* (DoS) e de serviço distribuído ou *Distributed Denial of Service* (DDoS), que implicam na negação de acesso a

[86] Dessa forma, em um contexto de guerra cibernética, pode haver ataques cibernéticos voltados à espionagem para se obter vantagem militar.
[87] O *Wikileaks* foi um site criado em 2006, anonimamente, pelo australiano Julian Assange. Tinha o propósito de divulgar injustiças de "regimes repressores", e, por essa razão, Assange ficou conhecido como um "ciberativista". O site ganhou maior conotação mundial quando, em 2010, divulgou documentos secretos do governo norte-americano, entre eles um vídeo que questiona a versão oficial sobre como o exército norte-americano matou 11 iraquianos em 2007, e arquivos sobre a atuação controversa dos Estados Unidos no Afeganistão. (ENTENDA, 2019).
[88] Edward Snowden, ex-analista da Agência Nacional de Segurança dos EUA, que vazou informações dos serviços de inteligência norte-americano (SINGER; FRIEDMAN, 2014, p. 50).

computadores, servidores, redes, etc.; ataques de *defacement* ou pichação de *sites*; uso de *e-mails* não solicitados ou *Sending and Posting Advertisement in Mass* (SPAM) em grande escala; etc. Tais ataques foram sentidos na economia e comunicação entre os cidadãos, governo e relações externas, mas não foi divulgado se houve efeitos mais graves. (SILVA; SILVA, 2019, p. 132-133).

Ao tentar investigar a origem dos ataques, foi identificado que os comandos teriam sido lançados de, supostamente, mais de 175 Estados, principalmente da Rússia[89] (SCHMITT, 2021a, p. 663). Não foram obtidas conclusões categóricas sobre os culpados dos ataques, mas estima-se que um primeiro momento dos ataques teria sido realizado por *patriotic hackers* e, numa fase mais avassaladora, coordenada com bastante zelo técnico e militar. Ocorre que, pouco antes do início dos ataques, o governo da Estônia teria removido um memorial soviético da Segunda Guerra Mundial do local em que estava para realocá-lo em um cemitério militar de soldados e vítimas da guerra. A remoção do "Soldado de Bronze", uma estátua de um soldado soviético que havia sido posta no centro de Tallinn, em 1947, como tributo à "libertação" pelo exército soviético frente a Alemanha nazista, não foi bem vista pelos russos residentes no país e por grupos "pró-Rússia", assim como pelo ministro das relações exteriores da Rússia, que teria condenado a atitude e sugerido, em tons de ameaça, que haveriam consequências ao governo estoniano. (STIENNON, 2016, p. 17; SILVA; SILVA, 2019, p. 131-133).

Após o incidente cibernético na Estônia, a discussão sobre a necessidade de um entendimento sobre como o direito internacional se aplicaria aos ataques no ciberespaço ganhou lugar, e passou a ter maior vigor no ano seguinte, 2008, quando ataques cibernéticos ocorreram durante o conflito armado internacional envolvendo a Geórgia e a Rússia (SCHMITT, 2021a, p. 663). Em contraste com o caso estoniano, restava clara a situação de conflito armado internacional, com ataques cinéticos recíprocos e, portanto, cenário bélico convencional, entre Geórgia e Federação Russa[90]. Nesse contexto, foram inseridos ataques cibernéticos com vistas a, por meio de técnicas de DoS e DDoS, de distribuição de programa malicioso para explorar vulnerabilidades de bancos de dados (*MS batch script* e em *Structured Query Language* – SQL), e de *defacement* e etc., prejudicar operadoras de comunicação da Geórgia, sobretudo durante as ações cinéticas do governo (SILVA; SILVA, 2019, p. 135).

---

[89] Relatos sobre a fonte dos ataques teriam reportado mais de 80.000 endereços IP, que localizam o dispositivo de onde a ação supostamente teria sido comandada (STIENNON, 2016, p. 17). Embora não tenha havido um consenso sobre a autoria dos ataques, e o governo da Rússia tenha negado a relação com o incidente, nos estudos sobre o caso constantemente é sugerida a atribuição ao governo russo (SCHMITT, 2021a, p. 663; SILVA; SILVA, 2019, p. 133; STIENNON, 2016, p. 17).

[90] Em 2008, a Geórgia estava em conflito com a Federação Russa pelo status de duas regiões do norte, Abkhazia e Ossétia do Sul; a Rússia apoiava a independência das regiões (STIENNON, 2016, p. 18).

Diante das supostas operações cibernéticas orquestradas pelo governo russo afetando a infraestrutura civil e governamental da Geórgia, e das dúvidas concernentes a ataques cibernéticos internacionais, no mesmo ano os Estados da Organização do Tratado do Atlântico Norte (OTAN) organizaram-se para o estabelecimento do *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), o Centro de Excelência em Defesa Cibernética Cooperativa da OTAN (SCHMITT, 2021a, p. 663). O Centro de Excelência está localizado em Tallinn, capital da Estônia, e assume responsabilidades de pesquisa e coordenação sobre defesa cibernética, possuindo projetos piloto para a matéria de aplicabilidade do direito internacional ao espaço cibernético[91].

Aos dois casos, considerados emblemáticos para os assuntos de segurança e defesa cibernética nacional, diversos outros puderam ser somados ao longo da última década, como o caso *Stuxnet*, em 2010, tido como o primeiro ataque cibernético voltado a atingir a infraestrutura crítica de um Estado que causou danos físicos diretos (STIENNON, 2016, p. 20). *Stuxnet* foi o nome dado ao *malware*, vírus ou software malicioso, que foi utilizado para atingir Sistemas de Supervisão e Aquisição de Dados (sistemas SCADA[92]) e interromper a capacidade do Irã de refinar urânio para armas, e que foi capaz de causar danos significativos às centrífugas de gás que auxiliavam no desenvolvimento de armas nucleares do país. Frequentemente se alega que os Estados Unidos e Israel estiveram por trás dos ataques, mas também não houve reconhecimento oficial sobre a fonte desses, bem como não foram atestados danos em altas proporções à infraestrutura no país. De todo modo, o caso *Stuxnet* possibilitou uma visão inaugural de ataques cibernéticos como "armas cibernéticas"[93], tendo em vista que foi o primeiro caso que demonstrou o potencial de destruição física dos mesmos (LIN, 2012, p. 519-520; STIENNON, 2016, p. 20-21).

Não obstante o reconhecimento da origem dos ataques cibernéticos e a inserção em contexto de conflito armado serem questões proeminentes e que precisam ser analisadas no cenário internacional, é notória a tendência de que operações cibernéticas se tornem um

---

[91] O CCDCOE será abordado no terceiro capítulo, quando da tratativa da OTAN no que refere ao avanço de políticas para coordenação do espaço cibernético.

[92] *Supervisory Control and Data Acquisition* (SCADA *system*) são sistemas de computadores que fornecem monitoramento e controle de processos industriais, de infraestrutura e de instalação. O funcionamento de equipamentos de usinas de energia, instalações de tratamento de água, sistemas de distribuição elétrica, aeroportos, fábricas, oleodutos e gasodutos, etc., na atualidade, geralmente são coordenados por tais. (SCHMITT, 2017, p. 567).

[93] O vírus *Stuxnet* e sua precisão em causar danos físicos através de meios cibernéticos, demonstrando o baixo impacto físico em comparação com outras armas tradicionais, trouxe um novo olhar sobre o desenvolvimento de armas "mais eficazes e mais limpas". Embora seja questionável o ataque cibernético, ele teve como alvo tão apenas um programa de fabricação de bombas nucleares que já havia sido objeto de esforços diplomáticos e sanções econômicas, sem ferir ou matar ninguém (SINGER; FRIEDMAN, 2014, p. 118-119; STEED, 2016, p. 82-83).

elemento fixo dos conflitos contemporâneos. É algo que tem sido visto corriqueiramente por especialistas do Direito Internacional dos Conflitos Armados[94] e que tem sido demonstrado pelo desenvolvimento de estratégias de securitização do espaço cibernético adotadas por diversos Estados[95]. Além de prática que teria sido cada vez mais empregada durante conflitos armados, como se alega aos conflitos internacionais e não internacionais no Afeganistão e Iraque, aos conflitos armados não internacionais na Líbia e na Síria, e que supostamente tem sido aplicada no conflito internacional entre Rússia e Ucrânia, desde 2014 (SCHMITT, 2014a, p. 190).

Preliminarmente, o diferencial dos ataques cibernéticos que justificam a orientação para a guerra cibernética e início da aplicação das normas de conflito armado é que "em contexto de guerra cibernética, um ataque ao sistema de tecnologia da informação ou rede de um adversário teria que ter como objetivo resultar em uma vantagem militar [...] (e não apenas política ou econômica)" (LIN, 2012, p. 525, tradução nossa[96]). Contudo, o que se nota ao detalhar e tentar definir os ataques cibernéticos que adentram à situação de conflito armado é que a afirmação de conceitos e da aplicabilidade das normas de proteção às vítimas não exime a dificuldade de se enxergar como operacionalmente isso irá ocorrer e como será possível ter consenso e cooperação internacional.

[94] O Comitê Internacional da Cruz Vermelha, enquanto organização internacional que tem como uma de suas funções desenvolver o Direito Internacional dos Conflitos Armados (ou DIH), bastante tem promovido discussões sobre o uso das novas tecnologias nos conflitos armados. Ao longo desta pesquisa são citados diversos artigos que compõem o *International Review of the Red Cross*, revista da organização que é voltada ao diálogo entre especialistas de várias nacionalidades. Uma das edições mais recentes (IRRC No. 913), inclusive, publicada em março de 2021, foi voltada exclusivamente a artigos sobre tecnologias digitais e guerra.

[95] A título de exemplificação, as políticas de defesa e segurança cibernética dos Estados Unidos da América, República Popular da China, Rússia e Israel são consideradas as mais avançadas (PINTO; PAGLIARI; GRASSI, 2021), e refletem como a exploração do espaço cibernético com finalidade militar tem sido levada à sério pelas nações que de forma mais intensa tem se envolvido em conflitos geopolíticos.

[96] In the context of cyber warfare, an attack on an adversary's IT system or network would have to be intended to result in a […] military advantage (and not merely a political or economic advantage). (LIN, 2012, p. 525).

2. AS VÍTIMAS DAS GUERRAS CIBERNÉTICAS SOB A PERSPECTIVA DO DIREITO INTERNACIONAL HUMANITÁRIO

Cada vez mais as ações no espaço cibernético têm demonstrado seu alcance prejudicial, atingindo dimensões psicológicas, sociais, políticas, etc., com implicações físicas e repercussões que vão além da virtualidade, e evidenciando a inviabilidade de se tratar o ciberespaço como um domínio paralelo e apartado da sistemática organizacional humana. A difusão de práticas de *cyberbullying* em redes sociais como Instagram, Twitter, etc., de vandalismo e/ou crimes cibernéticos interrompendo aulas virtuais[97], as alegações de interferências estrangeiras em eleições presidenciais por operações cibernéticas[98], dentre outros diversos incidentes que ocorrem em razão do e por meio cibernético e cujos efeitos transpassam o mundo virtual revelam que o pensamento do ciberespaço como ambiente apolítico, independente, irrestrito e separado do mundo real, como defendido por John Perry Barlow[99] em *A Declaration of the Independence of Cyberspace*, em 1996, não condizem com a prática.

Nessa linha de compreensão, também as operações cibernéticas que coadunam com a adesão do termo "guerra cibernética" no escopo militar, como forma híbrida para se alcançar objetivos e/ou como ataques virtuais de elevado potencial danoso, trazem preocupações acerca do custo humano que a nova arma, meio ou método de guerra, supostamente "menos sanguinário" pode acarretar. O caso *Stuxnet*, citado no capítulo anterior, tornou-se emblemático na visualização de como ataques cibernéticos podem ter consequências cinéticas, quando se verificou que um vírus poderia levar até mesmo a uma explosão termonuclear[100]. Nessa toada,

---

[97] A pandemia do COVID-19 e a necessidade de adaptação virtual dos sistemas de ensino até então maiormente presenciais trouxe à tona casos de invasão de *hackers* interrompendo aulas *online*, sob motivações diversas. No Brasil, um dos casos que chamou bastante atenção da mídia referia-se à invasão com exibição de vídeo pornográfico para alunos de nível fundamental, durante a aula virtual de escola pública no município de Taguatinga, Distrito Federal (POLÍCIA, 2021).

[98] As eleições presidenciais dos EUA de 2020 causaram bastante furor, com alegações de Joe Biden e de Donald Trump acerca de interferências externas por operações cibernéticas afetando o processo democrático do país. Por um lado, expunha-se que o presidente Vladimir Putin e o Estado russo tenham propiciado a condução de operações cibernéticas contra a eleição norte-americana ao denegrir Biden e o Partido Democrata, e ao minar a confiança do público no processo eleitoral em favor de Trump. Por outro, alegou-se, também, que o Irã e uma série de outros atores estrangeiros teriam realizado campanhas de influência secreta com vistas a dificultar as perspectivas de reeleição do ex-presidente republicano. (SCHMITT, 2021b, p. 740-741).

[99] O norte-americano John Perry Barlow (1947-2018) ficou conhecido como um dos líderes do movimento ciberlibertarianista, que prega a ausência de soberanias estatais no ciberespaço. Ele ajudou a difundir a ideia de que o ciberespaço seria livre de imposições, em um movimento de oposição ao controle estatal e de propagação do espaço virtual como sociedade de pessoas individualmente capacitadas, que se relacionam de forma democrática e consciente (DAHLBERG, 2020, p. 333); acreditava numa governança criada pelo próprio espaço cibernético e sua soberania digital, "a partir da ética, do interesse próprio esclarecido e do bem-estar comum" (BARLOW, 2019).

[100] Dmitry Rogozin, embaixador russo na OTAN, sobre o caso *Stuxnet*, chegou a comparar o alcance do vírus nas instalações da usina de Bushehr com o acidente de Chernobyl, de 1986. Apesar de, em contrapartida, ter se

observando as proporções que ações no ciberespaço podem alcançar, este capítulo destina-se a examinar como as operações de guerras cibernéticas se atrelam a terminologias comuns ao DIH, e como essas podem causar vitimizações de caráter humanitário, apesar das controvérsias sobre a severidade das ações no meio cibernético.

Para tanto, inicialmente é abordada a interlocução e complementariedade entre Direitos Humanos e DIH, a fim de contextualização do arcabouço normativo que oferece proteção a vítimas de conflitos armados e de compreensão dos desafios que a atualização na guerra impõe a um regramento tradicionalmente respaldado em conflitos cinéticos. Doravante, ciente de que "guerra cibernética" se refere a operações cibernéticas "equivalentes a" ou inseridas em situação de conflito armado, e que à delimitação de "equivalência à" sob os auspícios da Carta da ONU – com discussões sobre a utilização da nova tecnologia como inaugurando o uso da força e consubstanciando ataque armado, a possibilidade de sanções e de medidas pelo Conselho de Segurança – cumpre debate aprofundado que foge dos objetivos desta pesquisa e que merece investigação própria e detalhada, é observado sob quais aspectos operações cibernéticas são regidas pelo DIH de acordo com o potencial custo humano que implicam.

O que se quer ressaltar é que, embora desde o advento das operações cibernéticas Estados e acadêmicos estejam discutindo e se esforçando para definir a possibilidade ou o limite no qual um ataque cibernético se torna "uso da força" e "ataque armado", a ausência de uma conclusão a essas questões não afasta a convicção de que ataques cibernéticos podem ser considerados atos de guerra (SCHMITT, 2014b, p. 279-291). Em verdade, nem todo uso da força necessariamente indica a existência de um conflito armado, e, da mesma forma, nem todo ato de guerra necessariamente envolve uso da força[101] (MELZER, 2011, p. 24), mas frequentemente tais compreensões são confluentes.

A respeito disso, a classificação de um ciberataque como forma de agressão[102] e, não só por consequência, mas também, como ato de guerra, pode ser analisada sob três padrões

---

verificado tecnicamente que o vírus tinha objetivos bastante precisos e que se destinava apenas a infectar e destruir as centrífugas de enriquecimento de urânio, sem causar explosões, trata-se de um exemplo categórico onde se percebe que os ataques no ciberespaço podem afetar a infraestrutura industrial e processos baseados em instalações, inclusive com custo humano. O caso *Stuxnet*, ainda, é exemplo de que os ataques cibernéticos não dependem de conexão com a *internet*, apesar da grande maioria dos incidentes estarem ligados à essa; as instalações da usina, por segurança, não possuíam conexão, e a infecção pode ter ocorrido por dispositivo USB. (RIVIÈRE, 2011; SCHMITT, 2017, p. 567; STIENNON, 2016, p. 21-22; STEED, 2016, p. 82-83)

[101] À parte do advento de possíveis atos de guerra cibernética, os conflitos armados internacionais podiam ser desencadeados por declarações formais de guerra, sem uso de "força" entre os Estados (MELZER, 2011, p. 24).

[102] Por "agressão", a Resolução 3.314 (XXIX) da Assembleia Geral da ONU entende como o uso da força armada por um Estado contra a soberania, integridade territorial ou independência política de outro Estado, denotando o primeiro uso da força que pode recorrer à legítima defesa e gerar responsabilidade internacional. Conforme a mesma, podem ser qualificados como atos de agressão as invasões, bombardeios, bloqueios, os ataques pelas forças armadas de um Estado, etc., vide previsão não exaustiva do art. 3º da Resolução (ONU, 1974). A previsão

principais[103]: com base nos meios empregados, nos alvos desejados, e nos efeitos que se almeja alcançar (DAYEM, 2018, p. 3). Tal noção auxilia na futura fundamentação teórica sobre como ataques cibernéticos poderiam invocar o *jus ad bellum*, mas, sobretudo, também permite a reflexão sobre a aplicabilidade do *jus in bello* na medida em que um ato cibernético é vislumbrado como meio e método de guerra; de modo especial, quando um ciberataque caracteriza-se como "ato de guerra", como "arma", e converge com a percepção própria de "ataque" para o DIH.

Os efeitos da guerra cibernética às populações civis, com enfoque nas operações cibernéticas que possam resultar em morte, ferimentos ou danos físicos, ou, ainda, que afetem o acesso a serviços essenciais para a população – onde se incluem os principais serviços de *internet* – são de fundamental importância para a matéria humanitária, mas não definem a caracterização de conflitos armados para fins de aplicabilidade do DIH[104] . Por mais que as mais conhecidas operações cibernéticas da atualidade não tenham ligação aparente com um conflito armado, alguns Estados já reconheceram publicamente que utilizaram ou que foram afetados por operações cibernéticas durante conflitos armados, e um número crescente de Estados têm assumido o desenvolvimento de capacidades cibernéticas militares (GISEL; OLEJNIK, 2019, p. 10). Permeando o cenário iminente e ao mesmo tempo já existente, este capítulo aproxima-se dos preceitos e termos técnicos do DIH e sua aplicabilidade às operações cibernéticas. No mais, aborda a dificuldade de atribuição de autoria como fator de estímulo a ataques cibernéticos e como um dos principais desafios para o direito internacional.

2.1 A guerra cibernética como questão humanitária: da Carta da ONU às Convenções de Genebra

Tratar o uso de operações cibernéticas como tema de DIH implica abordá-las no contexto de conflitos armados, como recurso utilizado entre as partes beligerantes e que requer

---

do documento é voltada às guerras físicas, com dimensões territoriais e efeitos tangíveis; há ênfase na vertente instrumental da guerra, com uso de armas e da força, embora a Resolução não seja limitante e reconheça a abrangência de "ataques armados", proporcionando um espaço interpretativo onde os ataques cibernéticos podem caber. (DAYEM, 2013, p. 3).

[103] *Means-based standard*, *target-based standard* e *effects-based standard* (DAYEM, 2018, p. 3). Ou, em sentido semelhante: *instrument-based approach*, *strict liability* e *effects-based approach*, respectivamente (GRAHAM, 2010, p. 91).

[104] Não deve haver confusão entre conceituar ou caracterizar "guerras cibernéticas" em distinção a outros fenômenos – como terrorismo, guerrilha, etc. –, com base nos efeitos (BRUSTOLIN, 2019); o que se quer dizer é que, com vistas à aplicabilidade das normas protetivas do DIH, se faz pertinente observar uma abordagem a partir dos efeitos.

limitações a fim de se evitar o sofrimento humano desnecessário. Nesse prisma de aplicação *ratione materiae* (BORGES, 2006, p. 42) é que as normas humanitárias exibem suas maiores distinções em detrimento de outras disciplinas jurídicas e que, todavia, também revelam suas aproximações com outras vertentes do direito internacional.

Os três pilares da ONU, estampados na Carta, quais sejam paz e segurança, desenvolvimento e direitos humanos, mostram a convergência entre o Direito do uso da força ou Direito de prevenção à guerra (*jus ad bellum*, *jus contra bellum*), Direitos Humanos Internacionais (DHI) e o DIH. Sob a finalidade protetiva e correlata aos destinatários de sua salvaguarda é que o DIH e os DHI maiormente se complementam, exibindo a relação de continuidade e similaridade, ao passo que ambos os corpos jurídicos pretendem aumentar a proteção dos indivíduos, aliviar a dor e o sofrimento, e garantir padrões mínimos às pessoas em várias situações (DETTER, 2013, p. 179).

Enquanto guarda diferente fundamentação histórica e aplicação temporal, o DIH moderno é composto por um quadro normativo o qual, ao tempo que reafirma preceitos voltados à racionalidade nas guerras já tidos como costume, revisa seus regramentos à luz dos direitos humanos. As três correntes que consubstanciam o DIH, o Direito de Haia, Direito de Genebra e Direito de Nova York, representantes dos regramentos referentes aos métodos e meios na condução das hostilidades, à proteção de vítimas e aos esforços das Nações Unidas para desenvolvimento do DIH, respectivamente, hoje encontram-se bastante entrelaçadas, demonstrando como os DHI e as normas humanitárias constam como dois círculos jurídicos sobrepostos[105] (THÜRER, 2011, p. 127-129).

As diversas convenções restringindo ou proibindo uso de certos meios ou métodos de guerra, a exemplo de tratados sobre armas bacteriológicas, incendiárias, químicas, etc., ao lado das fontes humanitárias da contemporaneidade que categorizam as vítimas, as quatro Convenções de Genebra de 1949, atingiram o ápice de confluência entre si e de diálogo com os DHI após os Protocolos Adicionais de 1977 e constantes incentivos da ONU para tutela de direitos mesmo em tempos de intensa "obliteração de padrões de comportamento e sistemas jurídicos" (MAURICE, 1992, p. 371, tradução nossa[106]) pela violência das guerras.

---

[105] "two overlapping circles", visto que, mesmo que disciplinas autônomas, não se excluem, e seus instrumentos normativos dialogam. É o que se vê, por exemplo, nas previsões do art. 4º do Pacto Internacional de Direitos Civis e Políticos, de 1966, ao abordar a prevalência de certos direitos ainda que em tempos de emergência pública, e no art. 75 do PA I, que expõe garantias fundamentais àqueles que, por quaisquer razões, não se enquadrem nos *status* de vítimas pelo texto convencional (THÜRER, 2011, p. 128-129).

[106] Everyone who has experienced war, particularly the wars of our times, knows that unleashed violence means the obliteration of standards of behaviour and legal systems. (MAURICE, 1992, p. 371).

O PA I, de modo especial, perante as vítimas de conflitos armados internacionais, reúne as três vertentes e atualiza, ao seu tempo, a preocupação com os riscos e consequências à pessoa humana inserida em contexto ou vinculada às guerras. Naturalmente, as suas disposições protetivas dirigem-se aos cenários de hostilidades anteriores ao incremento das tecnologias da informação no meio bélico. Nessa vereda, os atos regidos pela norma seriam sobretudo aqueles que coadunassem com o uso de armas tradicionais e/ou força cinética, momento em que se inicia a discussão sobre uma zona cinzenta para a proteção humanitária.

2.2 Uso da força, ataque armado e força armada: diferentes escopos, unicidade de problema

A guerra cibernética é considerada uma das mais recentes complicações e desafios do Direito Internacional Humanitário. O novo "*hullaballoo*[107]" do DIH é notado já quando da dificuldade de se delimitar a violência cibernética e o estado de transição entre paz e guerra. Quando um ataque cibernético – por enquanto, o termo tem sido aqui utilizado em sentido amplo, indicando desde cibervandalismo até o grau mais avançado da escada cibernética – vem a consistir em ato de guerra, é assunto de constante debate. A identidade do atacante, a natureza das ações, os meios empregados e a o dano potencial são fatores que auxiliam na configuração da guerra cibernética – de forma híbrida ou mesmo "pura" – enquanto matéria de segurança global.

A delimitação de "ato de guerra" também goza de imprecisões, mas regularmente é sintetizada como aquela ação que justifica uma resposta militar; como o momento de transição de um tipo de política, e suas regras, para outro (KEATING, 2017). Ou, de maneira não menos complexa, como

> [...] todas as medidas de força que uma parte, usando instrumentos militares de poder, implementa contra outra parte em um conflito armado internacional. Estes incluem ações de combate destinadas a eliminar as forças armadas adversárias e outros objetivos militares. (GREENWOOD, 2008, p. 57, tradução nossa[108])

Designado para tratar de todas as operações militares, inclusive aquelas que envolvem apenas a ameaça de força, tais ações, desde que as partes estejam em conflito armado, são

[107] "Cyber Warfare: A New Hullaballoo under International Humanitarian Law" (AYALEW, 2015).
[108] Acts of war are all measures of force which one party, using military instruments of power, implements against another party in an international armed conflict. These comprise combat actions designed to eliminate opposing armed forces and other military objectives. (GREENWOOD, 2008, p. 57).

consideradas atos de guerra. Nessa toada, as ações que se perfaçam como ameaça, e não como uso da força, antes da inauguração de um conflito armado, não serão necessariamente atos de guerra, vez que não originam um conflito armado. Da mesma forma, utilizar-se do termo "ato de guerra" não indica a legalidade da ação, que estará sempre sujeita ao exame fático: o ato de guerra em questão pode ser visualizado como recurso à força lícito, conforme o *jus ad bellum*, ao passo que sua licitude não é relevante para análise da compatibilidade com o *jus in bello*. (GREENWOOD, 2008, p. 58).

Sob o olhar das Leis da Guerra, embora os ataques cibernéticos levem a indagações em escopos jurídicos distintos – o direito à guerra e o direito durante a guerra, já citados –, a determinação de um ataque cibernético como ato de guerra importa às duas ordens. Sem uma convenção estabelecida para, de alguma maneira, auxiliar na classificação de ataques cibernéticos como forma de agressão, filósofos e especialistas têm averiguado três padrões principais para analisar os ataques como atos de guerra[109] (DAYEM, 2018, p. 3).

O primeiro padrão observa os meios empregados num aspecto instrumental (*means-based standard*), ou seja, classifica um ataque cibernético como ato de guerra se for verificado o mesmo nível de destruição física imediata que uma arma convencional – um ataque cinético – produziria (GRAHAM, 2010, p. 91). Esse modelo compreende que os ataques cibernéticos estariam espelhando os meios militares convencionais (DAYEM, 2018, p. 3), ou seja, seriam equiparáveis às armas tradicionais de guerra, as quais se destinam a causar ferimentos ou morte de pessoas ou danos ou destruição de objetos (SCHMITT, 2017, p. 452).

Sob o segundo padrão, com base no alvo dos ataques (*target-based standard*), havendo dano à infraestrutura crítica nacional, o objeto do ciberataque corresponderia a outro fator para qualificação como ato de guerra, tendo em vista a responsabilidade objetiva pela ação (GRAHAM, 2010, p. 91). A terceira variável, que considera os efeitos do ataque (*effects-based standard*), o classifica como agressão e ato de guerra fundamentando-se nas consequências, ao passo que se mostrem potencialmente violentas ou destrutivas para suas vítimas. Esta última observa que os efeitos globais do ataque cibernético – seus danos – não necessariamente são análogos aos causados por armas convencionais ou refletem em resultados imediatos. Ao mesmo tempo, engloba aspectos das duas abordagens anteriores, na medida em que os efeitos podem implicar em danos físicos, como ressalta o primeiro padrão, mas podem também

[109] Para Lina Dayem (2018, p. 3), os três padrões auxiliam na classificação como "*act of war*" (ato de guerra). David E. Graham (2010, p. 90-91) observa que as abordagens funcionam como guia para se compreender quando o uso da força atinge o nível de ataque armado – a partir do critério tradicionalmente aceito de Jean Pictet, de escopo, duração e intensidade – nos casos de uso de força não-convencionais, como certos ataques cibernéticos.

repercutir ou gerar interferências físicas ou virtuais inaceitáveis[110] à manutenção e funcionamento da infraestrutura crítica, como pondera a segunda variável. (DAYEM, 2018, p. 3).

Esses modelos ou padrões para visualização de um ataque cibernético como ato de guerra, ou, de modo mais específico – mas não isolado –, como ataque armado, não se excluem ou limitam as possíveis abordagens sobre o tema. Contudo, permitem avaliar em que medida um ataque cibernético pode ser considerado sob o olhar das previsões da Carta da ONU. A mesma não oferece critérios para determinar quando um ato corresponde ao uso da força, e, por consequência, quando o uso da força equivale a ato de agressão que consubstancia os poderes do Conselho de Segurança, vide Capítulo VII. Ainda que os termos "agressão" e "ataque armado" sejam bastante utilizados como sinônimos, à luz da Resolução 3.314 (XXIX) da Assembleia Geral das Nações Unidas (AGNU) definindo agressão, e da previsão de legítima defesa do art. 51 da Carta, é possível se afirmar que nem sempre um ato de agressão consiste em ataque armado[111]. Por ataque armado, remete-se ao direito de uso da força em legítima defesa, em diferentes propósitos normativos dentro da Carta da ONU (SCHMITT, 2017, p. 337-339).

Categoricamente, estudiosos da guerra cibernética têm defendido que, a partir da análise da "escala e efeitos" do ciberataque, e da condução ou possível atribuição a um Estado, este ataque pode ser definido como uso da força em acepção mais gravosa[112]. Fatores qualitativos e quantitativos de escala e efeitos, postos em comparação com operações não-cibernéticas que atingem o *status* de uso da força, permitiriam a classificação (SCHMITT, 2017, p. 330-331). Ocorre que enquanto as definições de termos-chave como "uso da força" e "ataque armado"

---

[110] Definição também ambígua e permissiva de interpretações diversas – o que seria "aceitável" ou não, em respeito à soberania dos Estados? (DAYEM, 2018, p. 3). Aos olhos do DIH, discutir essa abordagem também cabe à possível visualização de operações cibernéticas no nível das proibições e restrições como "ataque", ao passo que operações que causem mera "inconveniência" ou irritação a civis não seriam "ataque". Mas também não há uma delimitação do que seria "inconveniência", termo que o próprio CICV considera problemático para a qualificação (SCHMITT, 2017, p. 418; SCHMITT, 2019, p. 339).

[111] Vide rol "exemplificativo" do art. 3º da Resolução, bem como se observando que, pela terminologia empregada na Carta, o termo "ataque armado" está necessariamente atrelado à legimitidade do uso da força pelo art. 51. Soma-se a essa posição o fato de que, ao julgar o caso Nicaragua *vs*. EUA, parágrafo 191, a Corte Internacional de Justiça (CIJ) distinguiu entre "as mais graves" formas de uso da força e aquelas menos gravosas, sendo as primeiras aquelas que correspondem ao nível de "ataque armado" para o propósito da legítima defesa (SCHMITT, 2017, p. 332).

[112] O grupo de especialistas internacionais que levou à conclusão do Manual de Tallinn 2.0 sobre o Direito Internacional aplicável a operações cibernéticas: "any cyber operation that rises to the level of an 'armed attack' in terms of scale and effects [...], and that is conducted by or otherwise attributable to a State, qualifies as a 'use of force'"(SCHMITT, 2017, p. 332). O critério de análise pela escala e efeitos é também proveniente do caso Nicarágua, onde a CIJ atribuiu necessários os parâmetros para que o uso da força correspondesse a ataque armado, conforme supracitado; parâmetros e avaliação para a "escala" e os "efeitos", contudo, não foram oferecidos no caso, e permanecem incertos (SCHMITT, 2017, p. 341).

não são assertivos nem mesmo para assessorar conflitos cinéticos tradicionais, que se valem de "definições e significados que só podem ser inferidos de precedente histórico e da praxe – como nações, a própria Nações Unidas e órgãos judiciais internacionais têm definido esses termos em casos particulares" (LIN, 2012, p. 524, tradução nossa[113]), tampouco têm sido consistentes para auxiliar no contexto de conflitos cibernéticos.

Ainda assim, dos esforços para reconhecer ataques cibernéticos como uso da força e possivelmente como ataque armado, o grupo de especialistas do Manual de Tallinn 2.0 reuniu tais fatores qualitativos e quantitativos de escala e efeitos que refletem a prática internacional em "gravidade", "iminência", "objetividade", "caráter invasor", "mensurabilidade dos efeitos", "caráter militar", "envolvimento estatal" e "legalidade presuntiva" (SCHMITT, 2017, p. 334-336, tradução nossa[114]). Esses fatores, todavia, geralmente observados em contextos cinéticos para caracterização de um ataque armado[115], com dificuldade podem ser vislumbrados de forma precisa e conjunta no que refere a ataques cibernéticos, por vezes inviabilizando que Estados acordem nesses como uso da força. De qualquer modo, podem auxiliar na classificação de ataques cibernéticos, e inclusive servir tanto para suas conotações no *jus ad bellum* como no *jus in bello*.

A exemplo, a "iminência", remetendo às consequências temporalmente imediatas e à menor oportunidade de se buscar soluções pacíficas para a controvérsia ou se evitar a conclusão dos efeitos prejudiciais, a "objetividade" como o caráter direto ou nexo de causalidade entre o ato e o efeito, e a "mensurabilidade dos efeitos" pelas consequências aparentes (SCHMITT, 2017, p. 334-335), por vezes não são plenamente viabilizadas em ataques cibernéticos que se mostram potencialmente danosos, mas que levam semanas ou meses para alcançar os efeitos pretendidos ou mesmo para serem identificados como causadores dos danos – como ocorreu no caso *Stuxnet*[116], descoberto em 2010.

---

[113] Definitions and meanings can only be inferred from historical precedent and practice – how individual nations, the United Nations itself, and international judicial bodies have defined these terms in particular instances. (LIN, 2012, p. 524).

[114] Severity; immediacy; directness; invasiveness; measurability of effects; military character; State involvement; presumptive legality (SCHMITT, 2017, p. 334-336).

[115] Os fatores citados no Manual são aqueles que os especialistas classificaram que maiormente influenciam os Estados na caracterização do uso da força, conforme escala e efeitos: "[...] when determining whether particular actions amount to an 'armed attack' [...]. The Experts found the focus on scale and effects to be an equally useful approach when distinguishing acts that qualify as uses of force from those that do not." (SCHMITT, 2017, p. 330-331).

[116] Há relatos de que o *Stuxnet* já atuava bem antes de sua descoberta, em meados de 2010 – meses ou até mesmo anos antes o vírus teria sido implantado e operava danificando as instalações de Natanz, Irã (FINK, 2013). Sobre isso, os especialistas do Manual de Tallinn 2.0 reconhecem: "In some cases, the fact that a cyber armed attack has occurred or is occurring may not be apparent for some time. This could be so because the cause of the damage or injury has not been identified. Similarly, the initiator of the attack may not be identified until well after the attack.

Somando-se como provavelmente o maior problema das operações cibernéticas às Leis da Guerra, há a atribuição de autoria, mais fortemente vinculada ao "caráter militar" e ao "envolvimento estatal" como fatores que atestam o interesse em afetar a infraestrutura crítica e intuito militar, e a associação com as atividades conduzidas por um Estado tradicionalmente por suas forças armadas e agências de inteligência (SCHMITT, 2017, p. 336). Ocorre que o nexo militar e estatal a um ataque cibernético mostra-se bastante complexo, e tal característica talvez seja a grande propulsora do aumento de operações cibernéticas com possível (suposto) vínculo estatal, sobretudo na Era da Informação e da "militarização cibernética" de atores não-estatais.

Para além das discussões sobre a qualificação como uso da força e direito à legítima defesa pertinentes ao *jus ad bellum*, os mesmos critérios também auxiliam a minimamente compreender como uma operação cibernética desencadeia a aplicabilidade, como ato de guerra, e quando constitui um ataque[117] para o DIH (SASSÒLI, 2019, p. 557). Ainda que tenha se reiterado a distinção entre os campos da Carta da ONU e do DIH, há que ser notada a complementariedade de objetivos entre os ramos, que se voltam à proteção de seres humanos da guerra e seus efeitos; é o que se aduz quando se assevera que a aplicabilidade do DIH não substitui ou isola regras essenciais da Carta (GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 306), e, ao mesmo tempo, quando se percebe que

> [...] um ato pode constituir um recurso à **força armada** para o propósito de qualificar um conflito armado internacional, sem prejuízo da questão de saber se constitui também **uso da força** na acepção do Artigo 2(4) da Carta da ONU (**embora seja provável**), muito menos um **ataque armado** pelo Artigo 51. (DROEGE, 2012, p. 545-546, tradução[118] e grifos nossos).

Por mais que a investigação sobre a causa e (i)licitude do início de uma guerra por ações cibernéticas seja bastante relevante e atual, não pertence aos objetivos desta pesquisa aprofundar-se nas dimensões da proporcionalidade e necessidade de respostas a ataques cibernéticos possivelmente inaugurando uma guerra. Sob o prisma das normas humanitárias, não há preocupação com o fato de um conflito ser ou não lícito, há preocupação em se fazer valer a proteção humana independentemente das adversidades sobre o início de um conflito

---

The classic example of both situations is employment of a worm such as *Stuxnet*. In such cases, the criterion of immediacy is not met unless the conditions described above justify taking action." (SCHMITT, 2017, p. 354).

[117] Ver subcapítulo 2.4.

[118] [...] an act could constitute a resort to armed force for the purpose of qualifying an international armed conflict, without prejudice to the question whether it also constitutes a use of force within the meaning of Article 2(4) of the UN Charter (though it is likely), let alone an armed attack under Article 51. (DROEGE, 2012, p.545-546).

armado. A regulação ou limitação dos meios e métodos de combate com vistas à proteção das vítimas dos conflitos é a justificativa principal do DIH, o que leva à sua interlocução com a matéria de Direitos Humanos e, inclusive, à confluência como "direitos humanos em conflitos armados" desde a adoção da Resolução 2.444 (XXIII) pela AGNU em dezembro de 1968[119] (BORGES, 2006, p. 32-41).

De fato, para aplicabilidade do DIH às denominadas guerras cibernéticas, é essencial a configuração de um conflito armado. Mesmo que, à luz da "restrição" ao uso da força pela Carta da ONU, dos citados art. 2º comuns às Convenções de Genebra e da conclusão internacionalmente aceita desde o caso *Tadic* – de existência de conflito armado quando houver recurso à "força armada" entre Estados[120] – possa existir uma confusão terminológica entre "ataque armado" e "força armada" dentro dos escopos que regulam o uso da força (GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 306-307), *a priori* são imprescindíveis dois elementos para correlação com a situação de conflito armado internacional à definição de guerra cibernética ora adotada[121]: a atribuição de autoria a um Estado com seu *animus belligerandi* e a equivalência de um ataque cibernético a "força armada" (DROEGE, 2012, p. 543), que difere da conotação atribuída à legítima defesa.

A atribuição de autoria, ou o "envolvimento estatal", supracitado como fator qualitativo para caracterização do uso da força nas relações internacionais, é questão-chave em termos de responsabilização[122], a qual cabe análise própria dentro do próximo capítulo. Por enquanto, à problemática de autoria estatal para que se conceba o conflito armado entre Estados, cabe notar que, diante do anonimato como regra nos ataques cibernéticos, tratar da autoria e, portanto, de aplicabilidade do DIH a operações cibernéticas ao lado e em apoio a operações cinéticas durante conflitos armados internacionais é mais factível e, inclusive, esses são os únicos tipos de operações que os Estados têm amplamente reconhecido e considerado regidos pelo DIH (GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 303).

Operações cibernéticas sozinhas, sem vínculo pré-existente ou ao lado de conflitos cinéticos, podem alcançar o *status* de conflito armado internacional; essa é a posição que tem

---

[119] Referente à "resolution XXIII on human rights in armed conflicts", adotada em 12 de maio de 1968 na Conferência Internacional sobre Direitos Humanos ocorrida no Teerã, e intitulada "Respeito aos Direitos Humanos nos Conflitos Armados" (BORGES, 2006, p. 31; ONU, 1968).

[120] Para além da fórmula aceita desde a decisão do caso Tadic em 1995, Jean S. Pictet (1975, p. 50) similarmente definiu um conflito armado internacional como a desavença com intervenção das forças armadas estatais: "any opposition between two states involving the intervention of their armed forces and the existence of victims".

[121] Vide definido no primeiro capítulo, 1.3.2, por guerra cibernética: "ações atribuíveis de responsabilização a um Estado-Nação para penetrar nos computadores ou redes de outra nação com o objetivo de causar danos ou interrupções, desde que correlatas à situação de conflito armado".

[122] O problema da atribuição e *due diligence* estatal será melhor analisado no 3º capítulo, após introdução dos impasses na aplicabilidade de alguns princípios do DIH.

sido desenvolvida por especialistas do DIH e compartilhada pelo CICV (SCHMITT, 2017, p.384; GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 304). Contudo, poucos Estados[123] compartilham de tal compreensão, logo, quando em conexão com um contexto de hostilidades cinéticas já existente, torna-se mais viável[124] tratar da atribuição de autoria a um Estado e da aplicabilidade de normas humanitárias às citadas operações.

Mesmo tendo se tornado uma constante que Estados indiquem a autoria de operações cibernéticas ofensivas uns aos outros, a definição e medida em que tais operações ultrapassam o viés da espionagem ou outras "operações de informação" – em possível violação da não-intervenção nos assuntos internos dos outros Estados – e alcançam o *status* de conflito armado internacional não é clara. O fato de determinadas operações levarem à desabilitação de sistemas ou interferirem no funcionamento da infraestrutura crítica de um Estado, e a proporção em que baixas humanas ou destruição física são geradas não são fatores decisivos; aliás, reitera-se, ainda não houve nenhum episódio em que um Estado tenha qualificado publicamente uma operação cibernética hostil fora de um conflito armado como desencadeadora de aplicabilidade do DIH (GISEL; OLEJNIK, 2019, p. 70-71). No mais, mesmo que uma operação cibernética seja realizada reconhecidamente por uma das partes – situação pouco provável, uma vez que uma das vantagens das ações no ciberespaço é a dissimulação da autoria – durante um conflito armado, não necessariamente essa será regida pelo DIH[125].

Para que operações cibernéticas configurem conflito armado internacional, devem igualmente equivaler ao recurso às forças armadas. Trata-se de termo que denota a violência necessária, em conjunto com a intenção militar, para qualificação como hostilidade à nível internacional, que sugere o comando estatal, seja este efetuado diretamente pelas forças

---

[123] L. Gisel, T. Rodenhäuser e K. Dörmann (2020, p. 304) citam a França como exemplo, que, ao excepcionalmente tratar do direito internacional aplicável a operações no ciberespaço em documento emitido pelo seu Ministério das Forças Armadas em 2019, teria reconhecido a possibilidade de conflito armado internacional ou não-internacional ser caracterizado a partir de operações cibernéticas.

[124] A dificuldade de atribuição de autoria de ataques cibernéticos existe tanto quando já há hostilidades cinéticas entre Estados ou outras situações previstas no art. 2º das Convenções de Genebra – sem hostilidades, como pela ocupação sem resistência armada, mera declaração de guerra, etc. (SCHMITT, 2017, p. 384-385) – já configuradas (durante conflito armado), quanto diante de ações cibernéticas que por si atingem o caráter violento como "força armada" (desencadeando conflito armado). Há que se falar que seria possível, por termos factuais e não jurídicos, mitigar as incertezas de autoria pela presunção legal de origem das ações, assim como pelo contexto de adversidades já existente entre as partes. Todavia, o direito internacional existente não possui base legal para tais presunções, e, ainda assim, a dinamicidade e disfarces assumidos no ciberespaço demonstram que presunções podem ser extremamente artificiais (DIAMOND, 2014, p. 72; DROEGE, 2012, p. 543).

[125] Remete-se ao nexo militar, o *animus belligerandi*; operações ou ataques cibernéticos que não tenham conotação militar, a exemplo de atos outros que se enquadrem como cibervandalismo sem vantagem militar, etc., ou mesmo ações que esbocem intuito apenas econômico. Este juízo expõe uma questão bastante controversa, sobretudo para os atos no ciberespaço.

armadas regulares ou mesmo sob auxílio ou instrução de órgãos estatais[126]. Assim como para o termo "ataque armado", não há uma definição precisa para "força armada" enquanto violência mínima ou uso de força que justifique a aplicabilidade material do *jus in bello*, mas, habitualmente, e de forma correlata ao tempo em que a Carta da ONU e Convenções de Genebra foram elaboradas, os termos se entrelaçam na conotação "armada" como uso de armas de força cinética:

> Tradicionalmente, o objetivo da guerra é prevalecer sobre o inimigo, e, na guerra tradicional, o conflito envolve o emprego de meios militares, levando ao confronto militar. Assim, quando meios ou métodos tradicionais de guerra são usados – como bombardeios ou envios de tropas – não há controvérsias de que esses se tratam de **força armada**. (DROEGE, 2012, p. 546, tradução[127] e grifo nosso).

Nesse sentido, para que uma operação cibernética implique em força armada, ou em conflito por "arma cibernética", sob a perspectiva estrita de equiparação necessária entre essas e as armas ou meios de guerra já reconhecidos internacionalmente[128], o padrão com base nos meios utilizados (*means-based standard* ou *instrumental-based approach*) seria sobrelevado. Para esse, haveria que se falar em resultados tais quais os obtidos por meios cinéticos, como destruição ou danos físicos às vítimas. Ocorre que os ataques cibernéticos possuem uma lógica distinta das armas de força cinética, posto que não necessariamente os danos causados são imediatamente visíveis ou mensuráveis; por essa razão, o critério instrumental, por si só, parece insuficiente.

É sob essa ótica, numa análise interdisciplinar com os preceitos de Clausewitz para definir guerra, que se pode expressar – da lógica material onde todo ato de guerra é instrumental para seus fins – que a "guerra cibernética" não seria guerra, mas apenas lutas de poder através do ciberespaço[129]. Tal apreciação é corroborada pela alegação de haver rasas evidências

---

[126] Vide art. 43 (1) do PA I, "as forças armadas de uma Parte em conflito se compõem de todas as forças, as unidades e os grupos armados e organizados, colocados sob um comando responsável pela conduta de seus subordinados diante dessa Parte" (CICV, 2017, p. 34). De forma correlata, em parecer do CICV (2019, p. 8-9), sobre responsabilidade internacional aos Estados diante de operações cibernéticas, nota-se que estando dentro da cadeia de comando de um Estado, a atuação de diversos atores pode ensejar a situação de violação do DIH, com atribuição de autoria estatal.

[127] Traditionally, the objective of war is to prevail over the enemy, and in traditional warfare, conflict entails the deployment of military means, leading to military confrontation. Thus, when traditional means or methods of warfare are used – such as bombing, shelling, or the deployment of troops – it is uncontroversial that these amount to armed force. (DROEGE, 2012, p. 546).

[128] Seja por meio de tratados próprios, ou pela jurisprudência, a exemplo das armas nucleares.

[129] Por isso que, a partir de uma interpretação clausewitziana de guerra, é difícil haver pleno consenso dessa com a abordagem de "conflito armado internacional" para o DIH. Afinal, a instrumentalidade e o uso potencial ou real da força – violência física – necessários para haver guerra (CEPIK; CANABARRO; FERREIRA, 2015, p. 26), onde, segundo Clausewitz (2010, p. 13), "a guerra nunca é um ato isolado" e "a guerra não consiste num único golpe", podem importar, mas não direcionam o sentido de "ato de guerra" para a aplicabilidade do DIH. Aliás,

públicas empíricas de que ataques cibernéticos produzem danos físicos e funcionais às pessoas, infraestrutura e organizações; as consequências dificilmente seriam comparáveis às provocadas pela violência cinética, logo, não haveria "armas cibernéticas" e "guerras" cibernéticas (CEPIK; CANABARRO; FERREIRA, 2015, p. 26). Em paralelo com os preceitos do DIH para delimitar um conflito armado internacional e justificar sua essência protetiva, contudo, a interpretação no sentido de exclusão de determinadas operações cibernéticas – com fulcro bélico – do escopo do DIH, como atos de guerra, parece perigosa.

Os especialistas do Manual de Tallinn 2.0 seguem uma abordagem mais próxima[130] – mas não limitada, nem expressa – das consequências ou efeitos globais das operações cibernéticas (*effects-based approach*), ao passo que notabilizaram escala e efeitos dos danos caso a caso como fator determinante para se avaliar a "força armada" em um conflito. Há a primazia da existência de hostilidades, que podem ocorrer tanto de forma híbrida com operações cinéticas, como podem envolver tão somente operações cibernéticas. O termo "armado", da mesma forma que não restringe o DIH às forças armadas regulares[131], não limita ao sentido de armas convencionais cujas extensão, duração ou intensidade das hostilidades são imediatamente passíveis de mensurabilidade. (SCHMITT, 2017, p. 383-384).

A existência de hostilidades pressupõe a aplicação de "meios" e "métodos" de guerra, termos largamente utilizados no DIH e que, ligados ao contexto de operações cibernéticas, correspondem a "armas cibernéticas e seus sistemas cibernéticos associados" e a "táticas, técnicas e procedimentos cibernéticos pelos quais as hostilidades são conduzidas", respectivamente (SCHMITT, 2017, p. 452, tradução nossa[132]). Da noção quanto ao objeto do DIH, os meios e métodos de guerra são limitados em situação de conflito armado em função da dignidade da pessoa humana e para mitigação dos efeitos causados pelas hostilidades, sejam esses meios ou métodos convencionalmente postos ou não.

---

para configurar um conflito armado internacional, não se verificam como critérios a intensidade da violência, se ocorre de forma prolongada, etc. – como ocorre para conflitos armados não internacionais. Compreende-se que determinar o que seria violência é necessário tanto para visualização enquanto conflito armado internacional como para conflito armado não internacional, mas a magnitude da violência importa muito mais ao último. Por ora, de fato, é difícil imaginar que operações cibernéticas sozinhas satisfaçam o limite de iniciar a aplicabilidade do DIH, mas cabe perceber que tal limite pode ser alcançado pela combinação entre operações cibernéticas e atos de violência cinética (SASSÒLI, 2019, p. 558; SCHMITT, 2017, p. 383).

[130] São considerados os efeitos globais, mas com delimitações para que não se obtenha uma conotação demasiadamente abrangente para as operações cibernéticas, sobretudo no que refere às normas de proibição ou restrição na condução das hostilidades, o DIH (SCHMITT, 2017, p. 415-419).

[131] Maiormente, exércitos, mas também órgãos ou agências nomeadamente estatais. Ademais, aqueles que atuam em vínculo ou sob comando estatal; ver nota explicativa 125.

[132] […] 'means of cyber warfare' are cyber weapons and their associated cyber systems; and […] 'methods of cyber warfare' are the cyber tactics, techniques, and procedures by which hostilities are conducted. (SCHMITT, 2017, p. 452).

É o que os arts. 35 (1)[133] e 36[134] do Protocolo Adicional I de 1977 pressupõem, ao impor limitações e a discussão internacional inclusive para o advento de novas armas, meios ou métodos de guerra que surjam posteriormente ao seu texto. Nessa linha, também a CIJ já asseverou pela aplicabilidade das normas humanitárias a todos os tipos de armas e formas de guerra, até mesmo "àquelas do futuro", ao abordar o uso de armas nucleares em 1996[135]; uma conclusão que, em vista ao potencial custo humano de certos ataques no ciberespaço, se aplica às operações cibernéticas em contexto de conflito armado (CICV, 2019, p. 4).

Ao se abster "força armada" ao "uso da força" como resultando ou diretamente causando mortes, ferimentos ou destruição, ou à violência cinética equivalente aos efeitos de guerras tradicionais, impasses surgem. A "ocorrência de hostilidades com nexo beligerante"[136], em vez do rigor de se atribuir como uso de "força" seus efeitos físicos entre exércitos estatais, mas vislumbrando aquelas que afetem diretamente ou adversamente operações militares ou a capacidade militar de Estados a partir de ações cibernéticas patrocinadas por outro(s) Estado(s) talvez seja a mais pertinente para a acepção do DIH ao ciberespaço (MELZER, 2011, p. 24), apesar de não se afastar de imprecisões.

Que os princípios e normas do DIH se aplicam às operações cibernéticas em situação de conflito armado, ainda que o início da aplicação seja controverso e sujeito à situação fática, é algo que tem sido crescentemente acatado por Estados e organizações internacionais (CICV, 2019, p. 4). Resta esclarecer como operacionalmente esta aplicação é possível, uma questão complexa e multidisciplinar que dificilmente se esgota em definição de conceitos – apesar de ser de extrema importância para balizar a abrangência normativa e permitir a classificação de

---

[133] Art. 35 – Regras fundamentais. 1. Em qualquer conflito armado, o direito de as Partes em conflito escolherem os métodos ou os meios de guerra não é ilimitado. [...] (CICV, 2017, p.31).

[134] Art. 36 – Armas novas. Durante o estudo, preparação ou aquisição de uma nova arma, de novos meios ou de um novo método de guerra, uma Alta Parte contratante tem a obrigação de determinar se sua utilização seria proibida, em algumas ou em todas as circunstâncias, pelas disposições do presente Protocolo ou por qualquer outra regra de direito internacional aplicável a essa Alta Parte contratante. (CICV, 2017, p. 31).

[135] Opinião Consultiva sobre a legalidade da ameaça ou uso de armas nucleares, emitida em 8 de julho de 1996, em que a Corte reconhece que o fato de que as armas nucleares terem sido inventadas após a maioria dos princípios e regras do DIH não exime a aplicabilidade das normas: "[...] it cannot be concluded [...] that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrisically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future" (CIJ, 1996, p. 37).

[136] Nessa toada, observa Nils Melzer (2011, p. 24): "Strictly speaking, therefore, the existence of an international armed conflict does not necessarily depend on the use of "force" between states but, at least in the absence of a formal declaration of war, on the occurrence of belligerent "hostilities" within the meaning of IHL. Accordingly, state-sponsored cyber operations would give rise to an international armed conflict if they are designed to harm another state not only by directly causing death, injury or destruction, but also by directly adversely affecting its military operations or military capacity". As "hostilidades", no sentido do DIH: "[…] the concept of "hostilities" refers to the (collective) resort by the parties to the conflict to means and methods of injuring the enemy" (MELZER, 2011, p. 27).

ataques cibernéticos – e em comparações com conflitos cinéticos, mas que deve ser realizada à luz das consequências as quais o DIH deseja evitar ou mitigar em nome da proteção humana.

2.3 As vítimas e o potencial lesivo de operações cibernéticas

Por mais que sejam claros os benefícios e oportunidades trazidos pelo desenvolvimento das TIC's – onde se incluem todos os avanços do campo eletromagnético e, de modo particular para a realidade deste início do século XXI, a *internet* como um dos principais recursos cibernéticos – aos Estados, sociedade e indivíduos, a dependência e o funcionamento ininterrupto dessas tecnologias evidenciou a possibilidade de utilização do ciberespaço como ambiente bastante propício para ataques com danos potenciais e elevado custo humano.

A exploração de vulnerabilidades de sistemas críticos como forma de obtenção de vantagem militar passou a ser considerada por alguns Estados como preferível em detrimento do uso de armas cinéticas, vez que, sob dados aspectos, possibilita a mitigação de riscos a civis e a outros grupos de pessoas ou bens que gozam de proteção durante as hostilidades. O Reino Unido, por exemplo, em comentários ao Grupo de Trabalho Aberto das Nações Unidas referente a desenvolvimentos no campo da informação e telecomunicações no contexto de segurança internacional (*Open-Ended Working Group* – OEWG[137]) em meados de 2020, observou que o uso de TIC's no contexto militar pode ser uma opção para diminuir uso de armas cinéticas[138] (ONU, 2020, p. 2).

Por meio de documento do seu Ministério da Defesa, também afirmou que armas cibernéticas podem ser utilizadas como novos recursos de alta precisão os quais podem entregar efeitos não-convencionais, ou seja, podem atuar sem causar danos cinéticos a um alvo, por vezes sendo a resposta mais apropriada a algumas ameaças e cenários modernos. O desenvolvimento da capacidade cibernética militar com vistas ao incremento de supostas munições "inteligentes" capazes de distinguir alvos e fornecer "letalidade direcional" representaria uma opção bastante útil em termos de otimização de denominadas "armas não

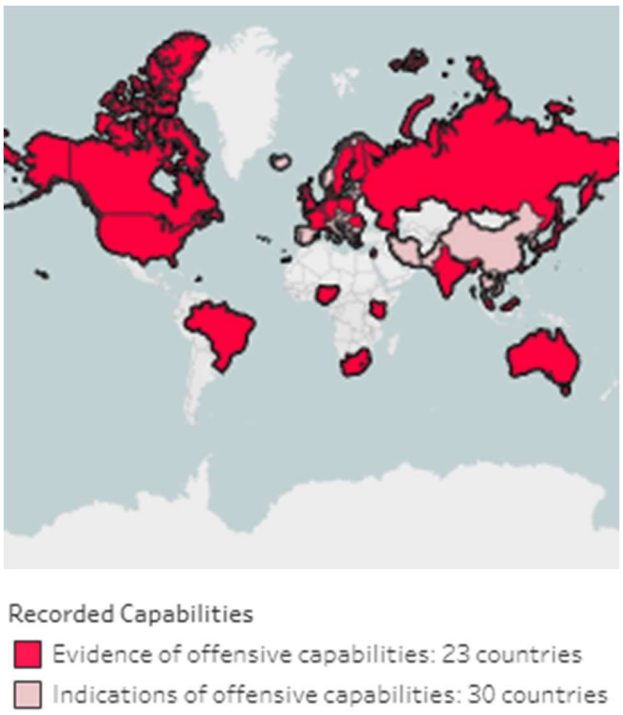
[137] OEWG on developments in the field of information and telecommunications in the context of international security.

[138] Tratou-se de resposta do Reino Unido ao "pré-rascunho" inicial do presidente do relatório do OEWG, com comentários em virtude de solicitação feita em 16 de março de 2020 pelo presidente. No texto dos comentários: "Whilst we recognise that some States held concerns about the 'militarisation of cyberspace', others – including the UK – also clearly recognised that ICT capabilities can be developed and used, in a manner consistent with international law and called on States to be transparent about the existence of their own capabilities. Indeed, as the UK noted […] the use of ICTs in military contexts may be preferable to use of kinetic weapons and can be de-escalatory" (ONU, 2020, p. 2).

letais" e de operações militares onde a presença de civis ou infraestrutura civil impede o uso de armas convencionais como bombas e mísseis[139] (REINO UNIDO, 2019, p. 42).

Fato é que os Estados têm desenvolvido cada vez mais suas capacidades cibernéticas, ofensivas ou defensivas, o que possui aspectos positivos, partindo-se de uma aplicabilidade militar embasada na possibilidade de ações com objetivos estratégicos, táticos e operacionais bem delimitados, onde o meio cibernético pode ser visto como aliado do ponto de vista humanitário (CORN, 2019). No entanto, as imprecisões do ambiente cibernético revelam questões bastante problemáticas em termos de particularidades técnicas de cada ataque efetuado, da efetiva mitigação de danos colaterais associados à infraestrutura cibernética atacada e da possibilidade de responsabilização estatal.

Figura 2 – Mapa de capacidades cibernéticas ofensivas[140]



Fonte: DIPLO, 2021.

[139] Tratou-se de documento de orientação sobre a estrutura de tecnologia de defesa do Reino Unido, sobre impulsionamento da modernização das capacidades das suas forças armadas; no mesmo, se expõe que sistemas de armas de última geração, como por mecanismos cibernéticos ofensivos ou por armas hipersônicas, podem ser aliados de uma ação militar onde a "força letal" não é desejável (REINO UNIDO, 2019).

[140] Mapa baseado em evidências de documentos oficiais e disponíveis publicamente, emitidos por instituições dos Estados, bem como a partir de indicações de meios de comunicação ou fontes técnicas; trata-se de lista não exaustiva, onde capacidades ofensivas são entendidas como capacidades das instituições estatais de realizar ataques cibernéticos contra a segurança da informação de outros Estados – onde se incluem ataques os quais permitam o acesso ou impactem seus sistemas digitais, suas informações e recursos, ou que tornem seus sistemas indisponíveis. (DIPLO, 2021).

A possibilidade de exploração das vulnerabilidades cibernéticas em operações militares que com efeito possam atingir seus objetivos dentro das proposições humanitárias, ou seja, com atenção às pessoas e aos bens afetados ou que possam ser afetados pelo conflito, encontra alguns impasses que evidenciam os riscos atrelados ao desenvolvimento dessas capacidades cibernéticas. Por um lado, há que se falar em interpretação ou adaptação de dispositivos do DIH à luz de um novo modelo de hostilidades não-cinéticas e que não necessariamente produzirá danos ou destruição material, sobretudo de forma imediata ou mensurável; é quando se nota que a "doutrina dos efeitos" (*effects-based approach*) em sua vertente mais restritiva pode ser falha para afirmar a aplicabilidade da proteção humanitária.

Além das hipóteses em que se consiga, de algum modo, restar claro o nexo entre um ataque cibernético e mortes ou ferimentos em conjuntura militar, há a questão sobre a exclusão ou alteração de dados e a visualização destes como bens protegidos ou como objetos – como objetivos militares que podem ser alvos de operações[141] – e sobre como isso perpassa as condições e proporções em que a extensão dos efeitos pode avaliar os atos de guerra ou de "violência" em contexto de conflito armado (SASSÒLI, 2019, p. 558, 560) e caracterizar o potencial custo às vítimas de guerras cibernéticas.

O DIH categoriza as vítimas de conflitos armados em grupos que recebem proteção normativa conforme o papel que desempenham ou na forma como estão inseridos nas hostilidades. As diferenciações primordiais que consubstanciam o Princípio da Distinção[142] entre combatentes e civis e entre objetivos militares e objetos civis para licitude de ataques durante as hostilidades justificam o corpo jurídico do DIH como pautado na dignidade humana e na abstenção do sofrimento desnecessário.

Dentre as categorias protegidas pelo DIH à luz das suas fontes consuetudinárias, que tradicionalmente correspondem às vítimas, constam: os feridos e enfermos que deixaram de combater, náufragos que igualmente não estão mais em combate, os prisioneiros de guerra, o pessoal sanitário e religioso, o pessoal dos organismos de defesa civil, etc., e aqueles que seriam os principais destinatários de resguardo humanitário, as pessoas civis.

---

[141] Considerando que os "objetivos militares", no escopo do DIH, estão limitados a objetos, vide art. 52 (2) do PA I; a discussão acerca do reconhecimento dos dados como objetos é outro problema que permeia a aplicabilidade do DIH às operações cibernéticas, tendo em vista questionamentos sobre a infraestrutura física ser considerada um objeto alvo de ataque, ou se também os dados constantes no sistema atacado podem ser considerados objetos (SASSÒLI, 2019, p. 559-560).

[142] Vide item 3.1.2 desta pesquisa.

A partir de um critério negativo para definição dos "civis", o art. 50 (1) do PA I aduz que todos aqueles que não sejam combatentes, são considerados pessoas civis[143]. Os combatentes em conflito armado internacional, vide art. 43 (2) do mesmo Protocolo, por sua vez, e *a priori*, são todos aqueles que têm o direito de participar diretamente das hostilidades enquanto membros das forças armadas[144]. Nessa perspectiva, o estado de guerra cibernética exibe a dificuldade de se afirmar e de distinguir alvos lícitos para as partes beligerantes quando a autoria e efetiva vinculação de uma operação cibernética a uma situação de conflito armado se mostram de difícil assunção.

É o que foi verificado no caso do conflito armado entre Geórgia e Rússia, em 2008, e a suposta autoria pelo governo russo de ataques cibernéticos antes e durante o conflito a *sites* oficiais da Geórgia, com o intuito de obstar a comunicação do governo georgiano na fase inicial e em coordenação com as hostilidades cinéticas, que acabaram afetando para além de *sites* e informações de natureza militar[145]; apesar da nítida ligação com o cenário bélico, não houve qualquer confirmação de autoria à título da Federação Russa, e as ações cibernéticas efetuadas não raramente são citadas como pequenos incidentes, de conotação e incidência leves. (ASHRAF, 2021, p. 279, 282; ROSCINI, 2014, p. 123).

Outro exemplo são as hostilidades entre Rússia e Ucrânia, iniciadas em 2014, também marcadas por ataques cibernéticos. Desde[146] a anexação da Crimeia pela Rússia, a Ucrânia tem sofrido diversos ciberataques, comprometendo persistentemente a capacidade do governo e das forças armadas ucranianas de se comunicar e de operar – via *spear phising*, *malware*, ataques DoS e DDoS e outras formas de interrupção e espionagem cibernética. Em 2015, particularmente, sofreu um ataque organizado que comprometeu temporariamente três centros de fornecimento de energia elétrica ucranianos e que, mediante acesso remoto para controlar e operar disjuntores, causaram quedas de energia e afetaram mais de 220.000 pessoas.

---

[143] Art. 50 – Definição de civis e de populações civis. 1. É considerada civil toda pessoa que não pertence a uma das categorias mencionadas no artigo 4A, alíneas (1), (2), (3) e (6) da III Convenção e pelo artigo 43 do presente Protocolo. Em caso de dúvida, a pessoa citada será considerada civil. [...]. (CICV, 2017, p. 39). Os artigos mencionados referem-se àqueles que serão reconhecidos enquanto combatentes.

[144] Ver nota 125, referente ao conceito de "forças armadas" pelo PA I. Art. 43. [...] 2. Os membros das forças armadas de uma Parte em conflito (exceto o pessoal sanitário e religioso citado no artigo 33 da III Convenção) são combatentes, isto é, têm o direito de participar diretamente das hostilidades. [...] (CICV, 2017, p. 34).

[145] Além de afetar dados do Ministério da Defesa e da presidência da Geórgia, os ataques cibernéticos teriam afetado serviços bancários, de companhias de transporte, e de provedores de internet (CONNELL; VOGLER, 2017, p. 17-18; ROSCINI, 2014, p. 7-8, 240, 264; SILVA; SILVA, 2019, p.135-138).

[146] São constantes os relatos, pela mídia, de ataques cibernéticos em meio ao conflito que se estende. A exemplo, em janeiro de 2022, cerca de 70 *sites* do governo ucraniano teriam ficado temporariamente fora do ar, após mensagens nas páginas alertando os ucranianos para que "se preparassem para o pior". O governo ucraniano alega que a Rússia estaria por trás do ataque que não gerou graves consequências, e que esse supostamente foi uma resposta ao fracasso russo diante de recentes negociações com a OTAN sobre a Ucrânia; a Rússia não se manifestou sobre o caso (UKRAINE, 2022)

Especialistas em segurança cibernética, ao analisar o evento, estimaram que o ciberataque tinha o potencial de causar danos maiores, físicos e permanentes, e que houve comedimento na ação pois a mesma seria apenas a sinalização, aviso ou ameaça, da capacidade de atacar a infraestrutura física da Ucrânia. Não obstante as alegações de que o ataque teria sido orquestrado sob um alto nível de sofisticação e preparo – com "impacto generalizado", mas "efeito geral limitado"[147] –, indicando sua direção e controle por um Estado ou entidade militar – dificilmente por um indivíduo ou organização não-estatal –, também não houve efetiva comprovação do nexo bélico ou de autoria pela Rússia. (CONNELL; VOGLER, 2017, p. 19-22).

Enquanto possuindo o "direito de participar diretamente das hostilidades", os combatentes gozam de imunidade para que não sejam processados pela participação nos conflitos armados internacionais, desde que não violem as normas humanitárias neste contexto[148]. Assim, há uma problemática que permeia a atuação no ciberespaço, posto que há certa dubiedade tanto sobre a violação do DIH via operações cibernéticas, como sobre a figura dos combatentes. A *priori*, em situação de conflito armado internacional, diante das alegações de autoria dissimulada e de atuação de *hackers* sem vínculo com uma cadeia de comando de Estado, estes poderiam ser qualificados como "civis participando diretamente das hostilidades", quando o suposto autor indivíduo ou grupo *hacker* deixaria de ser protegido como civil e poderia ser alvo da parte adversária (STINISSEN, 2015, p. 132); essa conclusão, entretanto, não é livre de complexidade e das controvérsias sobre o domínio cibernético[149].

De toda sorte, sob o ponto de vista dos civis como aquelas pessoas que não adentram à atividade combativa e que são as principais vítimas de guerras da contemporaneidade (CICV, 2010), o incremento de tecnologias nas estratégias militares, onde se incluem as operações cibernéticas como difusoras de "guerras remotas", ora podem servir como aliado num declínio

---

[147] Segundo especialistas, o autor teria passado meses planejando o ataque: após realizar o reconhecimento de todo o sistema utilizado pelas redes de energia elétrica, obteve credenciais de administrador e, então, coordenou e sincronizou toda a operação para que os centros de distribuição fossem derrubados simultaneamente. Um dos indicadores do nível de sofisticação está no aperfeiçoamento para que o impacto seja generalizado, mas com efeito geral limitado. Estima-se que teria sido a primeira operação cibernética russa voltada a expandir seus efeitos e potencial lesivo diretamente para o domínio cinético. (CONNELL; VOGLER, 2017, p. 19-22).

[148] Quando se percebem os crimes de guerra, violações de preceitos consuetudinários e costumeiros do DIH, ora dispostos no Estatuto de Roma.

[149] Três critérios precisam ser atendidos cumulativamente para que um civil perca sua proteção ao participar diretamente das hostilidades: a sua atuação deve implicar em certo nível de dano – seu ato deve ter o potencial de afetar adversamente as operações ou capacidades militares da parte oposta, ou de causar morte, ferimentos ou destruição a pessoas ou objetos protegidos contra ataques diretos; deve haver nexo causal entre a atuação e o dano infligido, de forma diretiva; deve haver um nexo com a situação beligerante, voltando-se a atingir o adversário. (MELZER, 2009, p. 46). Sob esse prisma, é possível imaginar que o ato de um indivíduo, *hacker*, poderia preencher tais critérios. Contudo, há certa complexidade em compreender o limiar de "dano" no ciberespaço, sobretudo no sentido de ultrapassar a conotação cinética, física, do mesmo (STINISSEN, 2015, p. 132).

do número de mortes de civis com apreço à vantagem militar, quando haveria substituição de armas convencionais ou de meios de guerras que levem a mortes e ferimentos de forma diretiva, ora podem instigar ataques onde cada vez mais bens e pessoas civis podem ser afetados sem uma clara percepção da origem das operações e sem perspectiva de responsabilização.

Afim de analisar o potencial custo humano de guerras cibernéticas, em novembro de 2018 o CICV organizou uma reunião com especialistas em cibersegurança de todo o mundo para analisar os riscos de operações cibernéticas em tempos de paz e de conflitos, averiguando atividades que possam resultar em morte, ferimentos ou danos físicos, ou, ainda, afetar a prestação de serviços considerados essenciais à população. O relatório elaborado a partir das discussões ressalta que uma das áreas de maior preocupação acerca da proteção da população civil se refere às vulnerabilidades de certos tipos de infraestrutura, sobretudo serviços de saúde, sistemas de controle industrial e a disponibilidade e confiabilidade de serviços de *internet*. Outros pontos de estresse são o risco de reações exageradas em razão de possível mal-entendido sobre as pretensões de operações cibernéticas hostis, a forma única como as ferramentas cibernéticas – ou armas cibernéticas – podem se proliferar, e os obstáculos que a dificuldade de atribuição de ataques cibernéticos cria na garantia de cumprimento do direito internacional (GISEL; OLEJNIK, 2019, p. 6).

O próprio documento observa que as operações cibernéticas, de forma extrínseca ao contexto de beligerância ou não, podem resultar em desde perdas econômicas substanciais até danos graves à infraestrutura, os quais podem ocorrer de duas maneiras: afetando a prestação de serviços e bens essenciais, tal como se visualiza em ataques às redes elétricas e ao setor de saúde, ou potencialmente acarretando em danos físicos, onde citam-se os casos *Stuxnet*, em 2010, com prejuízos graves a uma instalação de enriquecimento nuclear no Irã, e um ataque a uma siderúrgica alemã em 2014[150] (GISEL; OLEJNIK, 2019, p. 6).

O relatório detalha aquelas operações que, sejam revestidas como instrumentos e/ou métodos para se alcançar objetivos, se dirijam contra ou afetem hospitais e provedores de cuidados médicos, o setor de energia, instalações de água, transportes e logística, além daquelas que afetem o setor manufatureiro e ameaçam o setor financeiro dos Estados. Em particular, o setor de saúde é bastante afetado em seus sistemas de armazenamento e processamento de dados

[150] O nome da usina siderúrgica alemã não foi identificado, mas as fontes das informações revelam que ataques cibernéticos impactaram severamente componentes críticos do processo industrial. O relatório cita, ainda, outro ataque cibernético que teria sido destinado a sistemas industriais: um ataque contra planta petroquímica na Arábia Saudita, em 2017, que pretendia sabotar a produção por meio de explosão, em ato que implicaria em riscos à vida humana (GISEL; OLEJNIK, 2019, p. 64-65).

de funcionários e pacientes[151], e no gerenciamento de programações e de dispositivos de diagnóstico – como para realização de cirurgias e maquinários imprescindíveis, como raios-X, ultrassom, ressonância magnética, etc. –, mormente em razão da fraca estrutura de segurança cibernética constante ao setor (GISEL; OLEJNIK, 2019, p. 61).

Os ataques cibernéticos contra Brno, República Tcheca, em fase aguda da pandemia de coronavírus (MAČÁK; RODENHÄUSER; GISEL, 2020), exemplificam o risco lesivo das ações no ciberespaço[152]. O alcance dos ataques *WannaCry*[153] e *NotPetya*[154], em 2017, também puderam expor como as capacidades cibernéticas podem afetar indiscriminadamente populações civis. Ao passo que o primeiro, *ransomware*[155] intitulado *WannaCry* – que afetou mais de 150 países, incluindo o Brasil –, só no Reino Unido interrompeu serviços de mais de um terço dos hospitais da região; o segundo, em 2017, chegou a interromper produção de vacinas e a impossibilitar prestação de serviços médicos e realização de cirurgias ao redor do mundo (GISEL; OLEJNIK, 2019, p. 61; MAHADEVAN, 2020, p. 4).

Para além de exemplificar como ataques cibernéticos podem afetar serviços médicos, o relatório expõe que as armas cibernéticas – sobretudo *softwares* maliciosos, os *malwares* – podem adulterar dispositivos médicos, resultando em administração de doses medicamentosas

---

[151] Acerca da proteção à confidencialidade de dados, o relatório assevera que a discussão, embora necessária, foge dos escopos da reunião (GISEL; OLEJNIK, 2019, p.61); de modo semelhante, tal debate aprofundado não cabe aos objetivos desta pesquisa.

[152] Citado na introdução desta pesquisa. Os ataques cibernéticos em questão não possuíram vínculo com conflito armado existente, mas exemplificam as proporções e consequências de ações no ciberespaço afetando a infraestrutura crítica e serviços essenciais.

[153] O *WannaCry* é exemplo de *ransomware* de larga escala e proliferação indiscriminada, capaz de se propagar automaticamente entre os sistemas operacionais *Windows*. Espalhando-se em 2017, o *WannaCry* tornou sistemas ao redor do mundo inutilizáveis. (GISEL; OLEJNIK, 2019, p. 54). Dentre os efeitos sentidos pelo ataque, além de danos econômicos a diversas empresas, com efeitos mais severos cita-se a interrupção na prestação de serviços de saúde no Reino Unido. O Centro Nacional de Segurança Cibernética do Reino Unido teria especulado que um grupo de *hackers*, intitulado 'Lazarus', seria o autor da operação. Alegou-se que o grupo teria laços com o governo da Coreia do Norte, e autoridades norte-americanas, em conjunto com a própria empresa Microsoft, teriam reforçado publicamente a atribuição à Coreia do Norte. Todavia, o governo norte-coreano negou qualquer vínculo com a operação, e não houve consistência na atribuição. O caso gerou certas discussões sobre a possível qualificação da operação cibernética como "ataque armado", porém, não teria sido alcançado o limiar de uso da força sob o escopo da Carta da ONU. (SCHMITT; FAHEY, 2017).

[154] O *NotPetya* também foi projetado para se propagar automaticamente e, ao infectar um computador, possuía a capacidade de tornar o sistema inutilizável. Os danos causados afetaram diversos setores, como manufatura, energia, logística global, etc. Financeiramente, estima-se que o malware tenha causado prejuízos entre 1 e 10 bilhões de dólares americanos, tanto a governos de todo o mundo como a empresas privadas (GISEL; OLEJNIK, 2019, p. 59-66). O *NotPetya*, assim como o *WannaCry*, estaria abaixo do limite do uso da força convencionalmente posto, já que não houve relato de que tenha causado danos físicos diretos ou significativos que fossem além de perdas econômicas e de dados. Mesmo tendo sido lançado inicialmente no contexto de conflito armado entre Rússia e Ucrânia, o *NotPetya* se espalhou globalmente e repercutiu seus danos sobretudo fora da Ucrânia. Especialistas da OTAN opinaram que o *malware* provavelmente foi lançado por um ator estatal ou não estatal com suporte estatal. O governo russo seria o suspeito mais provável. (KAMINSKA; BROEDERS; CRISTIANO, 2021, p. 59-60; SCHMITT; BILLER, 2017).

[155] Tipo de *malware* voltado ao impedimento de acesso a sistemas ou arquivos pessoais, e que exige pagamento de resgate para que o acesso seja recuperado (MAHADEVAN, 2020, p. 1).

erradas e até em emissão de choques não padronizados, letais. Sob esse ponto de vista, resta visível como, embora desafios de estabelecimento de causalidade e de atribuição de autoria possam tornar obscura a análise, operações cibernéticas podem ser utilizadas em violação às proibições do DIH em situações de conflitos armados.

O setor de energia também seria constantemente alvo de ataques, os quais podem interromper redes elétricas e afetar civis de diversas formas. A Ucrânia sofreu significativamente com ataques ao setor entre 2015 e 2017, de modo especial quando o *NotPetya* atingiu a usina nuclear de Chernobyl e afetou sistemas responsáveis pelo monitoramento de radiação. Mais do que acarretar apagões que não se prolongam no tempo, especialistas em cibersegurança dos EUA concluíram que ataques cibernéticos podem até mesmo levar a incêndios e destruição total ou parcial de geradores de energia elétrica (GISEL; OLEJNIK, 2019, p. 63).

Sistemas de abastecimento de água, e de transporte e logística, também reverberam os riscos de ataques cibernéticos. O relatório apontou que, apesar de existirem poucos exemplos conhecidos de ataques cibernéticos a instalações de tratamento de águas, esses podem levar a escassez de água potável e a crises de saúde pública por contaminação (GISEL; OLEJNIK, 2019, p. 63). Em fevereiro de 2021, possivelmente aproveitando-se da metodologia de trabalho remoto necessário em razão de tempos pandêmicos e da utilização de *softwares* para tanto, um *hacker* lançou ataques, em ato de origem não conhecida ou publicizada, ao sistema de tratamento de água de uma cidade na Flórida, EUA, com objetivo de causar envenenamento pelo aumento excessivo da liberação de hidróxido de sódio[156] nas águas (LEVENSON, 2021). O ato foi percebido por um operador humano que estava na estação de tratamento a tempo; não foram divulgados casos de envenenamento e não há interpretações que vinculem a ação com atores internacionais ou situações de conflito armado, mas o acontecimento exibe como operações cibernéticas podem levar a consequências para além do virtual também nos serviços mais vitais.

Os sistemas de transporte e logística também podem ser afetados pelos ataques. O *NotPetya* afetou a logística global de suprimentos ao afetar empresas de tráfego de contêineres, acarretando não só em perdas financeiras de milhões de dólares americanos, mas no congestionamento de fornecimento de mercadorias; efeitos em cascata afetando a saúde humana poderiam ser visualizados em hipóteses semelhantes, sobretudo referindo-se à

[156] O hidróxido de sódio (soda cáustica) é liberado em pequenas quantidades e utilizado para controlar a acidez da água; no caso do ataque ao sistema de tratamento de Oldsmar, Flórida, o hacker teria aumentado a liberação do produto, bastante corrosivo, em mais de cem vezes (HACKER, 2021).

disponibilidade de alimentos e suprimentos médicos (GISEL; OLEJNIK, 2019, p. 64). Entre outras áreas de risco no setor de transportes estão a segurança cibernética de sistemas de controle de tráfego aéreo, de metrôs automatizados, etc., aos quais os ataques cibernéticos poderiam causar destruição à propriedade ou mesmo morte a civis ou militares (ISLAM, 2017, p.106-108).

Evidentemente as ações no espaço cibernético podem ter conotações diversas, assim como diferentes potenciais lesivos e escala alcançada. A avaliação dos riscos de operações cibernéticas em curso ou possivelmente inaugurando um conflito armado mostra-se bastante complexa. Se, nos conflitos "tradicionais", o DIH lida com a análise dos riscos em função da probabilidade e gravidade dos eventos esperados e essa averiguação já se faz enigmática, nos conflitos cibernéticos, apesar de ainda mais abstrata, a avaliação dos efeitos é imprescindível. Esses efeitos (aproximando-se do *effects-based standard*), segundo estipulado pelos especialistas do relatório para o CICV, podem ser observados conforme uma estrutura de avaliação objetiva, que englobe noções de "risco", "probabilidade" e "gravidade"[157], e que note os efeitos diretos ou indiretos, incidentais ou acidentais, de operações cibernéticas:

> [...] A própria gravidade dependerá dos tipos de efeitos (por exemplo, causar mortes versus corte de eletricidade), a escala desses efeitos em termos do número de pessoas ou objetos afetados (inclusive por meio de efeitos em cascata ou por reverberação) e sua duração (para efeitos temporários e reversíveis).
> Para os fins da reunião de especialistas, esta avaliação deve focar nos efeitos de preocupação principal. Estes são morte, ferimentos ou outros danos aos seres humanos, destruição física e privação de serviços essenciais.
> [...] uma avaliação inicial de impacto e risco deve se preocupar com a gravidade real dos cenários plausíveis primeiro e, em seguida, com sua probabilidade (uma vez que a probabilidade não pode ser avaliada em abstrato, pois depende do tipo de ataque e dos efeitos em questão). (GISEL; OLEJNIK, 2019, p. 67, tradução nossa[158]).

A elaboração de diretrizes auxilia, mas não retira a dificuldade prática de se orientar como essa avaliação será feita. No que tange ao potencial custo humano de operações cibernéticas, mesmo os exemplos sem – supostamente – qualquer vínculo militar demonstram a lesividade das ações, e as evidências de Estados desenvolvendo capacidades cibernéticas

---

[157] An objective assessment framework should therefore define notions such as "risk", "likelihood" and "severity" (GISEL; OLEJNIK, 2019, p. 67).

[158] The severity itself will depend on the types of effects (e.g. causing death versus cutting off electricity), the scale of these effects in terms of the number of people or objects affected (including through cascading or reverberating effects), and their duration (for temporary and reversible effects).
For the purposes of the expert meeting, this assessment should focus on effects of primary concern. These are death, injury or other harm to human beings, physical destruction, and deprivation of essential services.
[…] an initial impact and risk assessment should focus on the actual severity of plausible scenarios first, then on their likelihood (since likelihood cannot be assessed in the abstract, as it depends on the type of attack and the effects in question). (GISEL; OLEJNIK, 2019, p. 67).

ofensivas não afastam as proporções que o novo domínio bélico é capaz de tomar. De toda sorte, é notório que operações cibernéticas, em tempos de paz ou de guerra, podem ser utilizadas de modo a causar perdas por vezes imensuráveis e sofrimento, sobretudo a civis. O DIH, como pautado na proteção humana e na limitação da condução das hostilidades em conflitos armados, não se abstém de aplicabilidade às novas tecnologias, por mais que seus efeitos surjam de forma distinta e descompassada das previsões normativas então consideradas *ius cogens* no direito internacional.

Para a delimitação de quem são as vítimas de ciberguerras, ainda que tradicionalmente exista a tendência de categorização de vítimas, o desenvolvimento de capacidades cibernéticas pelos países e a ausência de orientações sobre o uso de operações cibernéticas em conflitos armados exibem o imbróglio a ser discutido entre os Estados. Os civis certamente são os mais vulneráveis em meio aos ataques orquestrados no ciberespaço e que passam por falsas suposições da falta de balizamento pelo DIH. Mas, em uma área onde a própria diferenciação entre combatentes e não-combatentes não é simples, quando ataques cibernéticos podem ser lançados com dissimulação de autoria e sob alegações de atuação de *hackers* independentes, que não gozam dos parâmetros desejados para a classificação como combatentes[159], o cenário se torna demasiadamente complexo e distante de uma simples remediação pelas fontes do DIH já existentes.

Dessarte, as vítimas de operações cibernéticas em situação de conflito armado internacional englobam tanto os combatentes como os não-combatentes, sob a fundamentação do DIH como todo o corpo normativo que almeja evitar o sofrimento desnecessário a todos[160] os sujeitos ali inseridos, combatentes ou população civil. À medida que o potencial lesivo de ciberataques acomete bens protegidos, em particular, a infraestrutura crítica civil – comunicações, energia, transportes, águas, etc.–, quais sejam objetos que podem ser considerados de uso duplo (*dual-use objects*) – utilizados tanto por militares como por civis –, os impasses de aplicabilidade de regras já existentes é agravado, requerendo a ponderação entre os anseios dos Estados, ao desenvolver suas capacidades cibernéticas, e as considerações

[159] Conforme já estipulava a Declaração de Bruxelas de 1874 sobre as leis e costumes de guerra, art. 9º, um combatente é aquele que: está sob comando de uma pessoa responsável por seus subordinados; possua emblema distintivo fixo reconhecível à distância; porta armas abertamente; conduz operações de acordo com as leis e costumes de guerra. Esses critérios foram reproduzidos em dispositivos das Convenções de Genebra de 1949, como no art. 13 (2) da I e II Convenções, art. 4 (2) da III Convenção, etc., bem como no texto do art. 44 (3) do PA I de 1977 (DETTER, 2013, p. 148-149). Evidentemente, para os especialistas em cibernética que lançam os ataques, todos esses critérios não prevalecem.

[160] Afinal, o denominado Direito de Haia demonstra como nem todos os meios e métodos de guerra são permitidos entre combatentes; a categorização oferecida pelo Direito de Genebra trata das pessoas protegidas enquanto em grupos de vulnerabilidade. O Princípio da Necessidade Militar, abordado no próximo capítulo, auxilia nesta percepção.

humanitárias. Essa análise, lastreada em estudos interdisciplinares, deve ocorrer ciente das contradições entre o incentivo ao uso de ataques cibernéticos como armas de guerra que substituem meios tradicionalmente mais destrutivos – como bombas ou mísseis –, e a possibilidade de ações que se mostrem indiscriminadas. Paralelamente a tal reflexão, existem exemplos[161] de ataques indiscriminados – como o *WannaCry* e o *NotPetya* – e ataques que demonstraram alta precisão[162] – como o *Stuxnet*.

2.4 Os "ataques" para o DIH

Ao longo desta pesquisa, os termos "operações cibernéticas" e "ataques cibernéticos" foram utilizados de forma análoga, referindo-se às ações no espaço cibernético com caracterizações e intuitos diversos, e que podem estar inseridas em conflitos armados ou mesmo implicar em ato de guerra, a partir de critérios debatidos pela doutrina e ainda em discussão internacional. No escopo das normas do DIH, entretanto, o termo "ataque" possui conotação própria e polêmica em relação às ações cibernéticas nos conflitos armados.

O Protocolo Adicional I às Convenções de Genebra, em seu art. 49 (1), define "ataque", em acepção vinculativa a todas as normas humanitárias de condução das hostilidades e de proteção das vítimas contra os seus efeitos, como "os atos de violência contra o adversário, quer sejam atos ofensivos ou defensivos" (CICV, 2017, p. 38). Posto que o termo consta em diversas regras que regem conflitos armados, sobretudo aquelas que textualizam princípios de proteção humana, indaga-se se as normas de condução das hostilidades funcionam tão somente para aquelas operações cibernéticas que se enquadrem como "ataque" na definição original do artigo, que se volta às violências como uso de forças cinéticas e suas consequências físicas.

Sob a ótica do grau de proteção que o DIH oferecerá às vítimas, em particular às populações civis, diante de operações cibernéticas, é que o debate requer maior atenção. O Título IV do PA I, dedicado à proteção da população civil, traz disposições que limitam "ataques" durante conflitos armados internacionais. É o caso da proibição de ataques voltados diretamente a civis e populações civis e a objetos civis, que se verifica no art. 51(2)[163] e no art.

[161] Monica Kaminska, Dennis Broeders e Fabio Cristiano (2021) observam que uma análise forense pós-incidente de uma operação cibernética pode auxiliar na verificação da intenção do autor e na avaliação de conformidade com os preceitos do direito internacional: a "natureza" do *malware* pode ser determinada em investigação técnica; eles realizam essa análise, inclusive, considerando os casos *NotPetya* e *Stuxnet*.

[162] Apesar de relatos onde se afirma que o *Stuxnet* afetou infraestruturas civis, a exemplo de serviços bancários, mesmo fora do Irã (CHANG, 2017, p. 45).

[163] Art. 51 – Proteção da população civil [...] 2. Nem a população civil em conjunto, nem as pessoas civis, devem ser objeto de ataques. [...] (CICV, 2017, p. 39).

52 (1)[164]; da vedação a ataques indiscriminados e desproporcionais no art. 51(4 e 5)[165]; àqueles bens indispensáveis à sobrevivência da população civil, constante no art. 54(2)[166]; àqueles que afetem o meio ambiente natural, art. 55(2)[167]; a ataques que atinjam obras e instalações contendo forças perigosas que possam causar graves perdas na população civil, como a represas, diques e usinas nucleares, vide art. 56(1)[168]; àqueles que se voltem a localidades não defendidas, art. 59 (1)[169]; etc., além do emprego do termo em diversos outros dispositivos que regulam os meios e métodos de guerra e restringem os atos contra não-combatentes (SCHMITT, 2019, p. 337).

De modo especial, bastante se defende que a delimitação de uma operação como "ataque" pelo DIH é fundamental para a aplicação de regras de salvaguarda de civis e objetos civis, que derivam sobretudo dos princípios da distinção, proporcionalidade e precaução em conflitos armados (GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 312, 323; ROSCINI, 2014, p. 178, 238-241; DIAMOND, 2014, p. 75). Nessa compreensão, apenas aquelas operações qualificáveis como "ataque" seriam reguladas por certas normas do DIH que proíbem os atos afetando populações e objetos civis, o que revela o potencial problema de não se balizar

---

[164] Art. 52 – Proteção geral dos bens de caráter civil. 1. Os bens de caráter civil não devem ser objeto de ataques ou de represálias. São bens de caráter civil todos os bens que não sejam objetivos militares [...] (CICV, 2017, p. 40).

[165] Art. 51 [...] 4. Os ataques indiscriminados são proibidos. A expressão "ataques indiscriminados" designa: a) os ataques não dirigidos contra um objetivo militar determinado; b) os ataques em que forem utilizados métodos ou meios de combate que não possam ser dirigidos contra um objetivo militar determinado; ou c) os ataques em que forem utilizados métodos ou meios de combate cujos efeitos não possam ser limitados [...], próprios para atingir indistintamente objetivos militares e civis, ou bens de caráter civil. 5. Serão considerados como efetuados sem discriminação, entre outros, os seguintes tipos de ataque: a) os ataques por bombardeio [...] que tratem como objetivo militar único um certo número de objetivos militares nitidamente separados e distintos, situados em uma cidade, uma aldeia ou em qualquer zona que contenha concentração análoga de civis, ou de bens de caráter civil; b) os ataques de que se possa esperar que venham a causar acidentalmente perdas de vidas humanas na população civil, ferimentos nos civis, danos nos bens de caráter civil ou uma combinação dessas perdas e danos, que seriam excessivos em relação à vantagem militar concreta e direta esperada. (CICV, 2017, p.39-40).

[166] Art. 54 – Proteção dos bens indispensáveis à sobrevivência da população civil [...] 2. É proibido atacar, destruir, retirar ou pôr fora de uso bens indispensáveis à sobrevivência da população civil, tais como gêneros alimentícios e as zonas agrícolas que os produzem, colheitas, gado, instalações e reservas de água potável e obras de irrigação, com o objetivo específico de privar a população civil ou a Parte adversa de seu valor de subsistência, qualquer que seja o motivo que inspire aqueles atos, seja para provocar nos civis a fome, seu deslocamento ou outros motivos. [...] (CICV, 2017, p. 41).

[167] Art. 55 – Proteção do ambiente natural [...] 2. São proibidos os ataques contra o meio ambiente natural a título de represália. (CICV, 2017, p. 42).

[168] Art. 56 – Proteção de obras e instalações contendo forças perigosas [...] 1. As obras ou instalações que contenham forças perigosas, tais como barragens, diques e centrais nucleares de produção de energia elétrica, não serão objeto de ataques, mesmo que constituam objetivos militares, se esses ataques puderem provocar a libertação dessas forças e em consequência causar graves perdas na população civil. Os outros objetivos militares situados sobre essas obras ou instalações, ou em suas vizinhanças, não devem ser objeto de ataques, quando estes puderem provocar a libertação de forças perigosas e causar em consequência perdas graves na população civil. [...] (CICV, 2017, p. 42).

[169] Art. 59 – Localidades não defendidas. 1. É proibido às Partes em conflito atacar, por qualquer meio, as localidades não defendidas. [....] (CICV, 2017, p. 45).

operações que não envolvem combates cinéticos e que, por isso, tradicionalmente não seriam consideradas "violentas" – onde se incluem as operações cibernéticas como exemplo categórico de que não é o autor, o alvo ou a intenção, isoladamente, que definem uma conduta como "ato de violência"[170] (ROSCINI, 2014, p. 179).

Por outro lado, observa-se que o fato de uma operação cibernética em situação de conflito armado não ser compreendida literalmente como um "ataque" vide art. 49 (1), *a priori*, não significaria que essa não será proibida ou restringida; as fontes do DIH poderiam fazê-lo, ao passo que o ataque cibernético (sentido não adstrito) seja considerado uma operação militar (DINNISS, 2012, p. 199-202). Afinal, em diversos momentos, as regras de condução de hostilidades do Protocolo Adicional I utilizam-se do termo "operações militares" para encabeçar limitações que indicam princípios humanitários, e reduzir operações cibernéticas potencialmente danosas à adaptação de preceitos elaborados para conflitos precipuamente cinéticos retiraria "a razão de ser" do DIH.

É o que se vê, inclusive, no dispositivo do PA I que preceitua a distinção como princípio elementar para a proteção de civis:

> Artigo 48 – Regra fundamental
> Com vista a assegurar o respeito e a proteção da população civil e dos bens de caráter civil, as Partes em conflito devem sempre fazer a distinção entre população civil e combatentes, assim como entre bens de caráter civil e objetivos militares, devendo, portanto, dirigir suas **operações** unicamente contra objetivos militares (CICV, 2017, p. 38, grifo nosso).

A definição de "operações militares" é oferecida em comentário ao PA I, parágrafo 1875, como "todos os movimentos e atos relacionados às hostilidades empreendidos pelas forças armadas", vinculada à noção de que remete a situações nas quais "a violência é usada, e não para campanhas ideológicas, políticas ou religiosas" (SANDOZ; SWINARSKI; ZIMMERMAN, 1987, p. 597, tradução nossa[171]). Tal conceito, frente às percepções estritas de "ataque", ao mesmo tempo que permite conclusões mais abrangentes das restrições e proibições trazidas pelo DIH, expõe que as operações no escopo das normas humanitárias são apenas

[170] Marco Roscini (2014, p. 178-179) argumenta que, de forma semelhante aos critérios de análise do uso da força armada, o que define um "ato de violência" como norteador também para se definir um "ataque" para o art. 49(1) do PA I é o emprego de meios ou métodos de guerra que tenham ou apresentem probabilidade razoável de resultar em efeitos violentos. O autor nota, porém, que parece haver um consenso geral de que se uma operação cibernética causar ou puder causar morte ou ferimentos a pessoas, ou mais do que danos materiais mínimos à propriedade, essa será considerada "ataque" e então se justificará a aplicabilidade total de princípios humanitários, como o princípio da distinção.

[171] […] it refers to military operations during which violence is used, and not to ideological, political or religious campaigns. [...] all movements and acts related to hostilities that are undertaken by armed forces. (SANDOZ; SWINARSKI; ZIMMERMAN, 1987, p. 597).

aquelas que impliquem em vantagem especificamente militar e se mostrem mais gravosas, onde a "violência" não se atém ao uso de força cinética, mas às consequências violentas – o que não soluciona integralmente a questão no que tange às operações cibernéticas, em que mesmo o nexo militar e mensurabilidades podem ser de difícil afirmação imediata.

O alcance de "ataque" das normas do DIH passou a ser, contudo, uma das principais questões terminológicas que pesquisadores tentam desenvolver nas últimas duas décadas, com posições permissivas ou restritivas[172] no que tange à hermenêutica e adaptabilidade às operações cibernéticas. O Manual de Tallinn 2.0 proporciona uma direção aos Estados, ainda com imprecisões[173], mas mais palpável ao observar as consequências e potenciais danos. Com base no que aduz o art. 49 (1) do Protocolo Adicional I, e atentando à noção de "violência" como referindo-se aos meios de guerra ou aos seus efeitos – considerando que as operações que causem efeitos violentos podem ser um "ataque", ainda que os meios usados para causar tais efeitos não sejam considerados instrumentos violentos (GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 312) –, os especialistas convergiram em uma definição a qual, ao mesmo tempo que inicialmente consegue diferir operações militares e ataques por meios cibernéticos, não é demasiadamente complacente ao uso descomedido do espaço cibernético.

Por "ataque cibernético" no âmbito de aplicação dos Princípios do DIH, o Manual estabelece: "Regra 92 – Definição de ciberataque. Um ataque cibernético é uma operação cibernética, seja ofensiva ou defensiva, na qual é razoavelmente esperado que se cause ferimento ou morte a pessoas ou danos ou destruição a objetos" (SCHMITT, 2017, p. 415, tradução nossa[174]). Nos parágrafos que sucedem a definição, os especialistas esclarecem que os "atos de violência" a que se refere o art. 49 (1) é que diferenciam operações militares de ataques, de modo que as normas de condução de hostilidades trazem maiores proibições ou restrições aos últimos.

---

[172] Refere-se à "*permissive approach*" e à "*restrictive approach*", inicialmente defendidas por Michael Schmitt e Knut Dörmann, respectivamente. A primeira, permitindo uma gama de operações cibernéticas contra populações civis, ao limitar "ataque" às operações que fatidicamente resultassem em lesões a pessoas ou danos físicos a objetos; a segunda, restringindo a utilização de operações cibernéticas em respeito à lei humanitária, mesmo que essas não necessariamente resultem em ferimentos ou danos, mas desde que causem efeitos prejudiciais. (SCHMITT, 2014a, p. 191).

[173] Há que se reconhecer as limitações de uma abordagem casuística baseada na antecipação de efeitos de operações cibernéticas. Ademais, há aspectos do debate em que os especialistas não entraram em consenso, como sobre o significado de "perda de funcionalidade" como um requisito para análise da escala e efeitos de um ataque cibernético (SCHMITT, 2019, p. 338).

[174] Rule 92 – Definition of cyber attack. A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. (SCHMITT, 2017, p. 415).

Os “atos de violência” não se limitam a hostilidades com uso da força cinética, posição já posta internacionalmente quando do reconhecimento de ataques químicos, biológicos e radiológicos, ainda que não impliquem em efeitos cinéticos sobre seus alvos, como “ataques” para o DIH; esses demonstram que o ponto de avaliação como “ataque” não reside tão somente na natureza ou instrumentalidade da operação militar, mas nos seus potenciais efeitos – as possíveis consequências que devem ser violentas[175]. Nessa linha, a violência militar ora tratada não se confunde com a possivelmente alegada a ataques cibernéticos (em amplo aspecto) que de algum modo se enquadrem como operações cibernéticas de cunho apenas psicológico[176], econômico, ou como espionagem cibernética, etc. (SCHMITT, 2017, p. 415)

O grau de potencial de dano ou violência empregada que citado por Myriam Dunn Cavelty (2010), em sua escada cibernética, pode servir similarmente dentro do contexto de conflito armado para diferenciação entre operações militares cibernéticas e ataques cibernéticos no texto da lei humanitária. As operações cibernéticas que de algum modo possam implicar em efeitos no mundo não-virtual, como causando ferimentos ou mortes, ou destruição ou danos – que não se restringem àqueles físicos e imediatamente visíveis – a objetos civis ou militares, certamente atingem alguma equivalência e devem ser tratados como “ataques” tradicionalmente conduzidos por outros meios e métodos de guerra.

Dentro dessa lógica, operações cibernéticas que tragam como efeitos indiretos ou reverberantes as citadas consequências violentas, serão “ataques” para o DIH, gozando de restrições para a proteção de civis. É o que se vislumbraria no exemplo de operação cibernética contra rede de eletricidade que atende a hospitais com pacientes em terapia intensiva, e que, devido ao corte de energia causado pela ação cibernética, resulte na morte desses; no caso de operação cibernética que altere sistemas de controle de rede elétrica e que resulte em incêndio; na hipótese de operação que libere águas de uma barragem ou que leve a explosão de um gasoduto ao alterar sistemas SCADA, e possa causar extensa destruição ao redor, etc. (GISEL; RODËNHAUSER; DÖRMANN, 2020, p.313; SCHMITT, 2017, p. 416).

---

[175] Afinal, a possível eventualidade do dolo deve também ser considerada pelas partes, como se vê pela projeção dos efeitos que o DIH exige; é o que se ilustra na necessidade de medidas de precaução aos efeitos do ataque, por ambos os lados, e na exigência de proporcionalidade dos ataques a serem orquestrados.

[176] A respeito da conotação psicológica que operações cibernéticas podem ter, mesmo dentro do resultado das discussões que se consubstancia no Manual de Tallinn 2.0, é perceptível a presença de controvérsias acerca dos efeitos de perturbações psicológicas que reflitam em doenças mentais como sofrimento desnecessário. Afinal, o art. 51 (2) do PA I estabelece que “[...] são proibidos atos ou ameaças de violência com o objetivo principal de espalhar o terror no meio da população civil” (CICV, 2017, p. 39), e, no Manual, há a brecha para reconhecimento do terror como condição psicológica que resulta em sofrimento humano e, logo, que pode ser visto como “ataque” (SCHMITT, 2017, p. 417) à luz do PA I. Nota-se o estabelecimento de uma ponte entre ciberterrorismo e ciberguerra, havendo que se falar em aplicabilidade do DIH quando o terrorismo cibernético for utilizado como estratégia de guerra.

O grau de violência esperado não resulta necessariamente em dano físico a objetos, mas deve ser suficiente para que se verifiquem potenciais efeitos secundários ou terciários pretendidos que visem causar mais do que danos mínimos. Por isso, os especialistas do Manual não excluíram integralmente a percepção de que uma operação cibernética contra dados – entidades não físicas – também pode se qualificar como "ataque", à proporção que essa "afete a funcionalidade da infraestrutura cibernética ou resulte em outras consequências que qualificariam a operação cibernética em questão como um ataque" (SCHMITT, 2017, p.437, tradução nossa[177]). Todavia, não houve consenso sobre o que de fato consistiria na perda da funcionalidade de objetos, e em que medida tal implicaria no reconhecimento do ato como "ataque".

Parte majoritária dos especialistas entendeu que a perda de funcionalidade constitui dano ou destruição de objetos – e, por consequência, "ataque" – se houver necessidade, para restauração das funções, de reposição de componentes físicos do objeto atacado; outros adotaram uma posição mais abrangente onde a reinstalação do sistema operacional ou de dados específicos se mostra necessária para retorno à funcionalidade originária; um terceiro grupo asseverou pela irrelevância de se compreender como um objeto é desabilitado, pois a perda da usabilidade da infraestrutura cibernética por si já leva a danos que podem qualificar a operação cibernética como "ataque"[178]. (SCHMITT, 2017, p. 417-418).

Marco Sassòli (2019, p. 555-557), sobre a tentativa de balizamento oferecida pelo Manual de Tallinn 2.0, assevera que os especialistas independentes que levaram à conclusão do texto não cederam recomendações sobre como o direito deveria ser maiormente esclarecido e desenvolvido, e, ao formular a regra delimitando o que seria "ataque" cibernético para a lei dos conflitos armados, insistiram nos efeitos violentos como "uma tentativa desesperada de voltar

---

[177] [...] a cyber operation targeting data may sometimes qualify as an attack when the operation affects the functionality of cyber infrastructure or results in other consequences that would qualify the cyber operation in question as an attack. (SCHMITT, 2017, p. 437).

[178] Os diferentes critérios para se delimitar como a perda da funcionalidade de um objeto pode ser "ataque" discutidos no Manual de Tallinn 2.0 ilustram a tentativa de classificar operações cibernéticas com base em certas hipóteses, como em caso de operação cibernética que afete sistema de controle de computadores de rede de distribuição elétrica e faz com que a rede deixe de operar – para a maioria, a necessidade de substituição dos componentes vitais do sistema indicaria a operação como "ataque". Foi debatido, também, se a interrupção de comunicação por e-mail em todo um país – atingindo indistintamente e-mails com vínculo militar ou de civis – não seria qualificável como "ataque", vez que consequências adversas em grande escala poderiam ser causadas. Contudo, parte majoritária dos especialistas reconheceu que os danos a que remete a aplicabilidade das normas dos "ataques" pertencem a um escopo distinto, de maior grau ofensivo, e que outros dispositivos do DIH podem oferecer proteção a civis independentemente da valoração do ato como "ataque" ou mesmo como mera incoveniência, a exemplo do que se vê pela proibição de punição coletiva, baseada nas disposições dos art. 87 da Convenção de Genebra III, art. 33 da Convenção de Genebra IV e art. 75(2)(d) do PA I (SCHMITT, 2017, p. 418, 539). Cordula Droege (2012, p. 559), em colocação pertinente a semelhante hipótese, observa que na sociedade atual, onde há intensa dependência entre vida civil e comunicação, tem se tornado cada vez mais difícil distinguir o que seria "mera" comunicação e o que vai além.

às categorias do mundo cinético para o qual o DIH foi realmente desenvolvido" (SASSÒLI, 2019, p. 557, tradução nossa[179]), em parte evitando a hipótese de operações que não necessariamente resultem em impacto físico, e se afastando de definições problemáticas e demasiadamente inclusivas de "ataque" – possivelmente porque os governos a que estão vinculados sabem que, quanto menos o DIH for aplicável, menos regras irão reger os ataques cibernéticos, e eles não desejam limitar suas capacidades cibernéticas.

O CICV (2019, p. 7), atento à problemática sobre os riscos de ataques cibernéticos que resultam em perda de funcionalidade sem causar danos físicos, entende que as operações em conflitos armados que sejam designadas a desativar computadores ou redes de computadores constituem "ataque" para o DIH, independentemente de o objeto ter sido afetado por meios cinéticos ou cibernéticos:

> Se a noção de ataque for interpretada como referindo-se apenas a operações que causam morte, ferimentos ou danos físicos, uma operação cibernética que vise tornar uma rede civil (como de eletricidade, bancária, ou de comunicações) disfuncional, ou da qual se espere que se cause tal efeito incidentalmente, não poderia ser coberta pelas regras essenciais do DIH que protegem a população civil e os objetos civis. Tal compreensão excessivamente restritiva da noção de ataque seria difícil de conciliar com o objeto e propósito das regras do DIH sobre condução de hostilidades. (CICV, 2019, p. 8, tradução nossa[180]).

Gisel, Rodënhauser e Dörmann (2020, p. 313-314) observam que a posição do CICV é sustentada a partir da interpretação de "ataque" pelo seu contexto: a definição de "objetivos militares" que não deve se referir apenas à destruição ou captura[181], mas também à "neutralização" como um possível resultado de um ataque, de maneira que o termo "ataque" deve ser interpretado de forma a englobar operações militares que se destinem a prejudicar o funcionamento dos objetos – neutralizando-os – sem causar danos físicos ou destruição em seu sentido originário. Nessa linha, a incapacitação de infraestruturas, sem qualquer repercussão

---

[179] This insistence on violent effects constitutes a desperate attempt to come back to categories of the kinetic world for which IHL was indeed developed. (SASSÒLI, 2019, p. 557).

[180] If the notion of attack is interpreted as only referring to operations that cause death, injury or physical damage, a cyber operation that is directed at making a civilian network (such as electricity, banking, or communications) dysfunctional, or is expected to cause such effect incidentally, might not be covered by essential IHL rules protecting the civilian population and civilian objects. Such an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the IHL rules on the conduct of hostilities. (CICV, 2019, p. 8).

[181] Art. 52 – Proteção geral dos bens de caráter civil [...] 2. Os ataques devem se limitar estritamente aos objetivos militares. No que diz respeito aos bens, os objetivos militares são limitados aos que, por natureza, localização, destino ou utilização contribuem efetivamente para a ação militar e assim sua destruição total ou parcial, sua captura ou neutralização oferecem, nestes casos, uma vantagem militar precisa. (CICV, 2017, p. 40).

material, poderia ser considerada um "ataque", e, portanto, teria resguardo no escopo humanitário.

Não obstante as tentativas de balizamento de adaptação das normas humanitárias existentes às novidades do ciberespaço, é notório que as atividades dos especialistas são pautadas em hipóteses e em incertezas que só serão solucionadas ou enfrentadas em casos práticos. O DIH, por si, já lida com a antecipação dos efeitos de um ataque, exigindo que as partes conduzam suas operações à luz de princípios dos conflitos armados. Trabalhar com a antecipação de efeitos quando os meios e métodos são significativamente mais imprevisíveis e abstratos faz com que seja questionável a coerência e eficácia normativa, e certamente requer debate internacional, acordos e posicionamentos dos Estados sobre a visualização da matéria.

Todavia, para o embate ainda sem solução, sobre em que medida uma operação cibernética é um "ataque" para o DIH, cabe lembrar que apesar dos impasses na interpretação *lex lata* do termo para o contexto cibernético e na abrangência do "uso da força" e "violência" para meios virtuais e suas consequências por vezes não materiais, as premissas essenciais do DIH não permitem escapar as ações no meio cibernético de suas restrições. De fato, é plausível se argumentar que, na exposição literal da lei, quando não qualificada como "ataque", o DIH não proíbe que a operação seja dirigida contra civis. Mas, às operações cibernéticas, permanecem as limitações enquanto meio de obtenção de vantagem no conflito, as proibições de destruir, remover ou tornar inútil objetos indispensáveis à sobrevivência da população civil; as obrigações de respeito à passagem de ajuda humanitária (DROEGE, 2012, p. 559); as proibições de medidas ou atos de terrorismo e de punições coletivas contra civis em curso de conflitos armados internacionais ou não internacionais, vide disposição do art. 33 da IV CG[182] e do art. 4º (2) do PA II[183] (CICV, 2016, p.170; 2017, p.89); bem como outras restrições à luz de princípios humanitários que alicerçam o DIH e que não podem ser circunscritas a terminologias e suas conotações originárias.

Em que pese a tendência para declarações gerais de que à ataques em contexto de guerra cibernética se aplicam as limitações impostas por regras e princípios essenciais do DIH, operacionalmente é que os maiores impasses surgem, requerendo maiores diretrizes e consenso internacional para que o DIH possa ser interpretado no ciberespaço e para que a eficácia da lei

[182] Art. 33 – Nenhuma pessoa protegida pode ser punida por uma infração que não tenha pessoalmente cometido. São proibidas as penas coletivas, assim como todas as medidas de intimidação ou de terrorismo. [...] (CICV, 2016, p. 170).

[183] Art. 4º - Garantias fundamentais. [...] 2. Sem prejuízo do caráter geral das disposições anteriores, são e permanecerão proibidos, em qualquer momento ou lugar [...]: a) os atentados contra a vida, a saúde ou o bem-estar físico ou mental das pessoas [...]; b) as punições coletivas; [...] d) os atos de terrorismo; [...] (CICV, 2017, p. 89).

cumpra o papel de proteção das vítimas apesar de toda dinamicidade de novos meios e métodos de conflitos. A união entre aspectos jurídicos e tecnológicos, a fundamentação científica e técnica para analisar em que medida princípios podem ser empregados aos ataques no ciberespaço – sobretudo no que tange à difícil distinção entre alvos militares e objetos civis no ambiente cibernético – auxiliam na prevalência dos preceitos humanitários mesmo diante das abstrações da cibernética.

3. A PROTEÇÃO DAS VÍTIMAS DAS GUERRAS CIBERNÉTICAS: PRINCÍPIOS FUNDAMENTAIS, PROBLEMAS E POSSÍVEIS SOLUÇÕES

Neste último capítulo, após a introdução ao que viria a ser a guerra cibernética para os fins do DIH e da matéria de segurança global, e em seguida às discussões sobre as vitimizações de operações cibernéticas com fulcro militar, trata-se da proteção oferecida pelos preceitos do DIH. Ocorre que, na possível insuficiência ou ausência de alcance das normas tradicionalmente postas do *jus in bello*, os princípios humanitários podem oferecer balizamento, razoável ou mínimo até que sobrevenha acordo internacional para governar os conflitos internacionais no ciberespaço.

Cumpre, portanto, analisar o que propõem os princípios fundamentais do DIH: humanidade, necessidade militar, proporcionalidade e distinção. Os princípios, diante de alegações de lacunas nos tratados humanitários – em particular, o PA I –, e da suposta carência de normas consuetudinárias para nortear como o direito seria aplicável ao ciberespaço, devem ser sobrelevados. Todavia, declarar a aplicabilidade de princípios, sem determinar como e se operacionalmente isso seria possível, não torna o DIH em sua essência, qual seja proteger as pessoas em situação de vulnerabilidade em conflitos armados e evitar o sofrimento desnecessário, mais efetivo.

Nessa toada, observam-se problematizações da empregabilidade dos princípios aos conflitos cibernéticos, bem como a questão da difícil atribuição de autoria. Nota-se que a *due diligence* estatal, como princípio geral de direito internacional, pode oferecer certo grau de segurança jurídica para a disciplina humanitária. Por fim, é avaliado o papel de políticas públicas internacionais para a apreciação da temática de segurança cibernética, com um breve acompanhamento sobre como organismos internacionais – CICV, ONU, OEA, UE e OTAN –, têm estudado as ameaças humanitárias no ciberespaço; momento em que se pondera sobre as reuniões de Tallinn e seu documento mais recente, o Manual de Tallinn 2.0 sobre o Direito Internacional Aplicável às Operações Cibernéticas, como o instrumento de *soft law* mais avançado para a resolução de impasses provenientes das guerras cibernéticas.

3.1 O DIH aplicável às ciberguerras: os Princípios Humanitários

Diante da distinta disposição em que tratados e costumes internacionais passam a orientar as novidades tecnológicas – e seus fins bélicos –, os princípios fundamentais de uma seara jurídica tal qual a dos conflitos armados podem auxiliar na assimilação de preceitos frente

à uma realidade iminente[184]. Ao gozar de generalidades e de certa ausência de entraves, presentes nas normas positivadas, os princípios expõem a base, essência ou "razão de ser" do que há de ser posto na interpretação do direito e sua fundamentalidade, por vezes podendo exercer uma função corretiva[185] ou mesmo introdutória para determinados temas.

Como "guardiões residuais da eficácia jurídica em caso de não aplicabilidade objetiva" das regras então dispostas, os princípios evidenciam as "fibras do tecido" do DIH (CINELLI, 2016, p. 64-66). Esse tecido, composto pela conexão entre as restrições impostas às partes beligerantes quanto aos meios e métodos de combate e a proteção que as vítimas devem receber durante uma situação de conflito armado, como se vê pela hodierna perda de relevância em apartar as normas de Haia e as de Genebra, tem nos princípios a inalterabilidade – precisão e concretude – e, ao mesmo tempo, a flexibilidade – abrangência e valoração – para que se interpretem, consoante as mudanças sociais e culturais, os comportamentos futuros (THÜRER, 2011, p. 59-61).

O lugar de hierarquia que os princípios se propõem a ocupar em um ordenamento jurídico, apesar de frequentemente se argumentar que estes derivam de declarações expressas em tratados ou de fonte consuetudinária, exibem o papel substancial do próprio direito. Em contrapartida aos impasses que possam surgir quando da mutabilidade cultural, social e/ou tecnológica que se impõem aos regramentos dispostos, os princípios fundamentais direcionam o caminho a ser seguido para que o direito possa ser satisfeito operacionalmente: eles expressam a substância e o significado das demais fontes, mas também inspiram[186] novos documentos de DIH (SASSÒLI, 2019, p. 144-145; HENCKAERTS, 2020, p. 21).

Conforme se aduz pelo art. 38 do Estatuto da CIJ, as principais fontes do direito internacional compreendem as convenções, os costumes e os princípios gerais do direito, além das decisões judiciais e da doutrina. Nessa linha, também está o DIH sujeito às normas gerais do direito internacional, mas, por sua qualificação situacional – conflitos armados –, possui princípios próprios[187], que visam sintetizar um dos seus objetivos primordiais, qual seja o de estabelecer restrições à condução das hostilidades (HENCKAERTS, 2020, p. 20-21; THÜRER,

[184] Considerando-se a atual falta de precedentes sobre ataques cibernéticos por órgãos internacionais no escopo do DIH.
[185] Problemática levantada por Jeroen C. Van Den Boogaard (2013), sobre o papel dos princípios humanitários em detrimento de fontes convencionais, consuetudinárias e os princípios gerais do direito internacional.
[186] Albeit derived from existing rules, […] principles also constitute an inspiration for the rules and means of interpreting them. (HENCKAERTS, 2020, p. 21).
[187] E que naturalmente dialogam com as normas gerais, sobretudo no que tange à complementariedade com os direitos humanos, e, ao mesmo tempo, com os direitos fundamentais (THÜRER, 2011, p. 64).

2011, p. 63-64). Limitar a forma de lidar com as guerras consiste em um dos meios de proteger as vítimas de violências, sejam estas vítimas de conflitos em curso ou de potenciais hostilidades.

Da lógica onde "estabelecer restrições à condução da guerra e proteger as vítimas da violência são duas faces da mesma moeda" (THÜRER, 2011, p. 64, tradução nossa[188]), os princípios humanitários – ou, em particular, os princípios sobre os meios e métodos de guerra – emergem como anseio de operacionalização do direito, como guia para as ações dos combatentes em situações de conflito armado, e frequentemente são lecionados como regras da humanidade, da necessidade militar, da proporcionalidade e da distinção, por vezes ocorrendo a projeção em diversos outros[189] princípios.

A extensa codificação de preceitos do DIH que tem ocorrido desde as origens da disciplina e que se totaliza nos dias atuais de forma contígua aos direitos humanos, contudo, em termos práticos, dificilmente corresponde ao que é ensinado e aplicado pelos combatentes: os princípios que serão[190] passados e listados como regras de conduta para os soldados desde a fase de planejamento de uma operação até a efetiva atuação ou ataque nos cenários de hostilidade. Diante do uso de operações cibernéticas, permeia a dúvida sobre em que medida esses princípios podem auxiliar a reger a novidade bélica e o comportamento estatal.

Dentre as fontes que guiam o DIH, é sabido que o direito consuetudinário habitualmente serve como recurso para orientação quando a fonte convencional não se mostrar suficiente. Quando lidando com a violência cibernética ora estudada, notoriamente há impasses na adaptação dos tratados humanitários – especialmente, Convenções de Genebra e Protocolos Adicionais – e a realidade temporal em que foram inseridos. Os costumes, como prática reiterada estatal, similarmente não orientam para um cenário tão novo e em constante análise[191].

---

[188] "[...] setting constraints on the conduct of war and protecting victims of violence are two sides of the same coin" (*Ibidem*, p. 64).

[189] Como com o princípio da precaução, o qual, a partir da distinção, apregoa que há o dever de evitar ou minimizar na medida do possível danos incidentais a pessoas ou objetos protegidos contra ataques diretos – dever que se aplica tanto ao atacante quanto à parte atacada, para que tome as medidas necessárias para proteger a sua população dos efeitos do ataque do inimigo (MELZER, 2019, p. 18); o princípio da limitação ou da proibição do sofrimento desnecessário, que sucede o imperativo da humanidade, e segundo o qual os meios e métodos de combate não são ilimitados, como se vê com as restrições ou proibições de ataques que afetem bens culturais, o meio ambiente, etc., e que causem danos inúteis ou inaceitáveis para os objetivos da guerra, ou cujos efeitos não possam ser limitados (CINELLI, 2016, p. 80-84; MELZER, 2019, p. 19-20); o princípio da neutralidade, para que os Estados que não sejam parte no conflito – considerados neutros – não sejam atacados (CRAWFORD; PERT, 2015, p. 112-113); dentre outros. Sem desmerecer a pormenorização em outras especificações, porém, são estes os quatro princípios fundamentais que norteiam a condução das hostilidades: humanidade, necessidade militar, proporcionalidade e distinção.

[190] Ou mais comumente são lecionados, aqui referindo-se sobretudo às forças armadas regulares estatais. Os princípios aqui abordados evidenciam a própria "humanização" das leis dos conflitos armados, e, em razão do direcionamento que fornecem, integram "the laws of targeting" do DIH (BIGGIO, 2017).

[191] Sobre os costumes como fonte, Jeroen C. Van Den Boogaard (2013, p. 14-15) nota que a criação da prática estatal em termos do DIH já não é fácil em razão da dificuldade de ter acesso à esta durante as operações por motivos de segurança operacional; ademais, para formação de uma *opinio juris*, dificilmente serão observados

Por mais que outros indicadores, como o balizamento por manuais militares dos Estados, possam ser arguidos como comportamento estatal, logo, como fonte costumeira, eles não representam a conduta real do Estado durante a situação beligerante, às vezes resumindo-se a meras reafirmações escritas de tratados que o Estado aceitou, e nada mais – à mercê do valor que o Estado atribui ao documento[192] (VAN DEN BOOGAARD, 2013, p. 16). Ainda que existam declarações sobre a matéria, o nível de especificidade e sua coordenação prática podem não ser suficientes para comprovar a prática geral de um Estado ou da sua *opinio juris*.

Assim, sobretudo no que se refere ao uso de operações cibernéticas em situações de conflitos armados, o regramento humanitário internacional revela pelos seus princípios a ausência de um "vácuo jurídico", dada a função que esses exercem de preencher possíveis lacunas e de orientar quando as fontes convencionais e consuetudinárias ainda se mostrarem questionáveis e insuficientes.

As discussões do capítulo anterior sobre o que viria a compor um "ataque" cibernético ocorreram em função da conjectura de que os princípios humanitários apenas restringem aquelas operações que impliquem em "ataque" como ações militares onde há uso de meios violentos. Dada a importância das consequências violentas das ações para circunscrever quando ocorre a proteção de vítimas de guerras cibernéticas pelo DIH, doravante, após o debate doutrinário sobre o alcance da salvaguarda humanitária às operações cibernéticas quando o texto convencional é passível de controvérsias, passa-se a ponderar a elucidação[193] a partir dos princípios humanitários mesmo quando não houver consenso[194] sobre a qualificação como "ataque" nos termos originários do PA I.

---

casos em que os efeitos ainda sejam considerados efêmeros ou cujos resultados não se efetuaram integralmente. Paralelamente a tal ponderação, percebe-se que a análise sobre operações cibernéticas pelos Estados ainda é relativamente recente, apesar de crescente.

[192] Não implica dizer que declarações emitidas pelos Estados ou manuais de conduta militar sejam irrelevantes. Pelo contrário, quando tratando de novas ameaças, novos meios e métodos de guerra, assim como no tocante à opinião dos Estados sobre o uso de operações cibernéticas e expectativa de comportamento futuro, eles são extremamente necessários. Todavia, em termos gerais, especialmente em casos excepcionais de guerra, é sabido que a praxe pode não corresponder à obrigação doméstica estipulada e publicizada anteriormente por aquele Estado.

[193] Proteção das possíveis vítimas, ou mesmo resposta à "zona cinzenta" do DIH na modernidade.

[194] Sabe-se da importância do que seria "ataque" para aplicabilidade do DIH, posto o pleno entendimento de que suas disposições se aplicam desde o primeiro ataque (SASSÒLI, 2019, p. 114; VAN DEN BOOGAARD, 2013, p. 22); mas a relevância de se delimitar um ciberataque como "ataque" vide PA I interessa mais à discussão sobre a possibilidade de início de uma guerra por meios cibernéticos, deflagrando o início da aplicabilidade do DIH, do que à análise sobre a proteção oferecida às vítimas quando há uso de operações cibernéticas em curso de conflitos armados, as situações de guerras híbridas, de maior probabilidade. Notadamente, "[...] the rise of cyber warfare capabilities establishes a tension between the violence centered *rationale* of the law of targeting and the nature of cyber attacks, as their effects may have devastating consequences even without causing any form of *physical violence*" (BIGGIO, 2017, p. 41).

Ocorre que, não obstante inexistir convenção ou prática reiterada do DIH que expressamente aborde as operações cibernéticas, há previsão imperativa, revestida de regra processual específica[195], que dispõe sobre as fontes de direitos e obrigações nas circunstâncias de conflitos armados. Trata-se da Cláusula de Martens[196], que emerge como premissa humanitária de origem costumeira, a fim de afastar quaisquer conclusões no sentido de que inexistem restrições às situações de beligerância que não estejam até então previstas em tratados. Inicialmente adotada na I Conferência de Paz de Haia, ao abrigo do preâmbulo da II Convenção de Haia de 1899, a cláusula foi reproduzida[197] em diversos tratados de DIH. Em sua versão mais recente, no próprio PA I:

> Artigo 1 – Princípios gerais e âmbito de aplicação
> [...]
> 2. Nos casos não previstos pelo presente Protocolo ou por outros acordos internacionais, os civis e os combatentes ficarão sob a proteção e a autoridade dos princípios de direito internacional, tal como resulta do costume estabelecido, dos princípios humanitários e das exigências da consciência pública[198]. (CICV, 2017, p. 10)

Ou seja, revela a inconsistência de se atestar pelo "vácuo jurídico", mesmo nos casos mais imprecisos, como os de guerras cibernéticas. Os princípios referenciados na cláusula não se atêm apenas aos preceitos de ética e legitimidade nos meios e métodos de guerra, mas, naturalmente, esses estão incluídos. Evidenciada a aplicabilidade dos princípios humanitários para solucionar as mais diversas situações nas hostilidades, a questão a ser analisada passa a ser, então, de adaptabilidade ou operacionalidade desses princípios, que condensam o comportamento legítimo durante conflitos armados, às ações militares no ciberespaço.

---

[195] International humanitarian law contains a specific procedural rule that outlines the sources of rights and obligations […]. This rule is the Martens Clause […].", "[…]is not a substantive rule, but is rather of procedural nature (VAN DEN BOOGAARD, 2013, p. 16, 19).

[196] Assim intitulada por sua redação ter sido proposta por Friedrich von Martens, delegado russo na Conferência da Paz de Haia, em 1899.

[197] Além da presença nos preâmbulos das Convenções de Haia de 1899 e 1907, também consta nas quatro Convenções de Genebra de 1949; sua essência já figurava, contudo, na Declaração de São Petersburgo de 1868 – tratado internacional que antecedeu as Convenções de Haia de 1899 e 1907–, quando da previsão de prevalecimento das "exigências da humanidade" (DETTER, 2013, p. 185; CINELLI, 2016, p. 67).

[198] Pela exposição do preâmbulo da II Convenção de Haia sobre as Leis e Costumes de Guerra em Terra, de 1899: "Until a more complete code of laws of war has been issued, the High Contracting Parties deem it expedient to declare that in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the **laws of humanity**, and the dictates of public conscience" (DETTER, 2013, p. 185, grifo nosso). Observa-se, pela versão em português do PA I publicizada pelo CICV, a menção aos "princípios humanitários", todavia, provém do termo "principles of humanity", não restringindo aos princípios sobre os meios e métodos de guerra, aqui abordados, ou a uma lista delimitada de regras (THÜRER, 2011, p. 401-406).

3.1.1 Princípio da Humanidade

Os princípios do DIH buscam limitar os efeitos dos conflitos armados e manter o senso de humanidade mesmo em tempos de guerra. Por isso, o Princípio da Humanidade é considerado o cerne das regras humanitárias (THÜRER, 2011, p. 66; HENCKAERTS, 2020, p. 1; SCHMITT, 2020, p. 148). Nesse quesito, a Cláusula de Martens reflete a imprescindibilidade de reconhecimento de "humanidade" – por mais rebuscado que o seu conceito possa ser, é notória a percepção de que o "agir com humanidade" deve estar vinculado a uma noção de atitude ética, de valorização da vida humana, respeito mútuo entre todos os povos e de contenção do sofrimento desnecessário – mesmo em conflitos armados, e também representa a imperatividade desse princípio no DIH, que se relaciona diretamente com os demais.

Trata-se de preceito de conteúdo abstrato, mas análogo às "considerações elementares de humanidade[199]" como agente limitador dos atos permitidos em conflitos armados; correlato ao pensamento de que o objetivo da guerra é se sobrepor ao adversário, mas nem toda conduta é permitida para alcançar tal fim. Nas observações de Emily Crawford e Alison Pert (2015, p. 115, tradução nossa[200]), evidencia uma noção que começou a ser maiormente induzida nos meios bélicos ao final do século XIX, e que expôs a "rejeição explícita da doutrina [...] de *Kriegsraison*[201] – a ideia de que em tempos de guerra, a necessidade de alcançar o sucesso militar deve prevalecer sobre todas as outras leis e costumes que restringem a conduta de alguém".

Desenvolvendo tais "considerações elementares", a CIJ reconheceu no art. 3º comum às quatro Convenções de Genebra[202] o direcionamento às premissas de humanidade, ou a um

---

[199] Os "princípios de humanidade" foram citados como "considerações elementares de humanidade" nos casos *Corfu Channel* (1949) e *Military and Paramilitary Activities in and Against Nicaragua* (1986), pela CIJ (THÜRER, 2011, p. 67, 401).

[200] It is an explicit rejection of the nineteenth century doctrine of *Kriegsraison* – the idea that in times of war, the need to achieve military success should override all other laws and customs that restrain one's conduct (CRAWFORD; PERT, 2015, p. 115).

[201] A doutrina Kriegsraison emerge na Alemanha, no século XIX, e por vezes é abordada como "a necessidade militar de Clausewitz", onde qualquer medida militarmente conveniente, ainda que viole leis de conflito armado, pode ser adotada; Kriegsraison simbolizaria a necessidade militar como "uma exceção engolidora de regras", a necessidade militar sem limitações (HORTON, 2006, p. 578, 580).

[202] Art. 3º - 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:

"nível mínimo de civilidade[203]", que indicam o dever de cumprimento de disposições consideradas básicas em quaisquer situações de conflitos armados. Percebe-se, assim, a nítida relação das obrigações em curso de conflitos armados com a inerência dos direitos humanos, em tempos de paz ou de guerra; a expectativa de se agir sob princípios éticos e morais, a característica codificação do direito internacional natural, o *jus naturale internacionalis* (DETTER, 2013, p. 188-198; BROLLOWSKI, 2013, p. 64).

O Princípio da Humanidade, nas lições da modernidade, reveste-se da importância da proteção da segurança humana em detrimento da proteção do Estado-Nação. Apoiados na prevalência de garantias fundamentais em prol da dignidade humana mesmo em períodos excepcionais, uma série de atos passaram a ser restritos na condução das hostilidades – inclusive, como percebe Hanna Brollowski (2013, p. 65-69), modelando a ligação entre normas humanitárias, o direito penal internacional e a responsabilidade estatal. Por isso, os demais Princípios Humanitários, sob a ótica basilar da humanidade, emergem como decorrentes deste primeiro, em sua nuance de moderação do interesse militar das partes em conflito.

A questão, frente à extensão que o Princípio assume, passa a ser a medida de sua observância, pelas partes envolvidas em conflito, quando as operações militares transitam para o surgimento de novos meios e métodos de guerra e apresentam suas expressões ou consequências muitas vezes adversas[204] dos cenários mais tradicionais. Afinal, pensando no fundamento em comento como alinhado à ideia de "empatia", "sentimento" ou "expressão emocional"[205], o desenvolvimento de novas armas de guerra, cada vez mais distantes e sem contato humano, pode levar à percepção de afastamento da condição de humanidade.

---

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.
2) Os feridos e enfermos serão recolhidos e tratados. [...] (CICV, 2016).

[203] Como observa Ingrid Detter (2013, p. 196-198): "[...] the substratum of these rules is anyway rooted in the human conscience. […] In war, rules demanding a minimum humane behaviour are activated […]. The contents of the Martens Clause and of Common article 3 thus reflect what is required as civilized behaviour in any situation.".

[204] Paralelamente a tais considerações, recorda-se a preocupação em se discutir em que medida os dados civis postos no ciberespaço, em um mundo cada vez mais dependente de informações inseridas no meio virtual, seriam protegidos pelo DIH – afinal, se arquivos civis em papel gozam de proteção contra ataques, desde que não impliquem em vantagem militar precisa, vide art. 52 (2) do PA I, também os dados civis no ciberespaço gozariam da salvaguarda (CICV, 2017, p. 40; 2021). Conforme o dado que foi alvo da ação, diferentes dimensões de direitos afetados podem ser analisadas no escopo das operações militares, como direito à privacidade (SCHMITT, 2021b; GEIß; LAHMANN, 2021), mas, no que tange ao DIH, o Princípio da Humanidade notoriamente converge para o respeito à dignidade humana em sua máxima de manutenção da vida.

[205] Sobre o Princípio da Humanidade e a robotização da guerra, Hanna Brollowski (2013, p. 76) reflete: Altruism can […] be understood as a particularly broad form of empathy, much akin to the notion of humanity as sentiment,

Um dos maiores debates – dentre diversos possíveis – gerados pelo uso de ataques cibernéticos em conflitos armados, é no tocante à complexa determinação de sua autoria. Presume-se que nos conflitos de caráter internacional os combatentes estão representados sobretudo pelas forças armadas regulares das partes, e estes são os principais destinatários das normas limitantes na condução das hostilidades. Igualmente, espera-se que os Estados em conflito possuam medidas de responsabilização domésticas e ciência da possibilidade de responsabilização internacional quando seus soldados erram na tomada da decisão (BROLLOWSKI, 2013, p. 81, 86) e acabem por ferir as denominadas considerações substanciais de humanidade.

Ainda assim, um dos possíveis argumentos de inaplicabilidade ou ineficácia do Princípio da Humanidade pode se valer do pensamento onde, se na prática dos conflitos armados por meios e métodos tradicionais[206] já se exige dos soldados a ponderação de suas ações com vistas aos princípios humanitários, e no furor do ato do combatente há a dificuldade de empregabilidade, que dirá nos casos em que este não possui qualquer contato com as vítimas e age defronte a telas, a milhares de quilômetros de distância do palco de hostilidades e de sofrimento humano?. Trata-se de argumento que atrela o preceito em exame unicamente ao "espírito de empatia", que pode levar à falsa concepção de que o Princípio não possui força obrigatória, diversamente dos regramentos de distinção e proporcionalidade (CRAWFORD; PERT, 2015, p. 114).

Ocorre que, com base nos ciberataques em curso de conflitos armados verificados na praxe internacional em que houve suposto vínculo estatal, nota-se que as ações cibernéticas com maior grau de lesividade e potencial custo humano[207] dificilmente foram orquestradas sem uma prévia organização e sofisticação (CONNEL; VOGLER, 2017; GISEL; OLEJNIK, 2019), reiterando que o rito de arquitetar uma operação militar perpassa por um criterioso estudo estratégico, com o cálculo de probabilidades e fins que devem observar as diretrizes humanitárias – o que, *a priori*, não deve deixar de ocorrer na coordenação de operações cibernéticas, que, por sua natureza, requerem não só agentes bastante capacitados na área informacional e tecnológica, mas tempo, recursos e articulação com os demais setores estratégicos na atividade militar.

---

but it also refers to a set of moral principles and rules that affect and determine one's behaviour towards any human being, e.g. humanity as a whole. […] The feeling of empathy as well as the sentiment of humanity is something that robots will (even in the far future) hardly be able to develop, not least due to the fact of that the ability to be empathic is directly related to an individual's own prior experiences.

[206] Referindo-se sobretudo àqueles conflitos que ocorrem exclusivamente pelos domínios terrestre, marítimo ou aeroespacial.

[207] Em especial, aquelas que afetam a infraestrutura civil.

Ademais, a representação do Princípio da Humanidade na Cláusula de Martens e a relevância da mesma foi reforçada na Resolução XXIII da Conferência sobre Direitos Humanos de 1968 de Teerã, ao se afirmar que, na pendência da adaptação de novas regras – onde se incluem dispositivos que sejam específicos para meios e métodos cibernéticos –, todos os Estados devem assegurar que civis e combatentes sejam protegidos conforme os princípios mencionados na cláusula. O acatamento jurídico e a importância da permanente vigilância de parâmetros elementares de humanidade diante de novidades bélicas também foi comprovada na referência da CIJ, já citada, à Cláusula de Martens, em Opinião Consultiva sobre a legalidade do uso e ameaça de armas nucleares de 1996, época em que ainda não havia nenhuma convenção sobre as mesmas[208]. (VAN DEN BOOGAARD, 2013, p. 18-19; DINNISS, 2012, p. 28).

Em suma, enquanto vertente de proibição de atos que levem ao sofrimento desnecessário e a danos supérfluos, resta clara a eficácia do preceito também às operações cibernéticas durante conflitos armados, visto que tais ações também se mostram potencialmente lesivas e podem causar vitimizações, como atos de guerra. Como o Princípio da Humanidade deve ser visualizado aos casos de guerras cibernéticas, por conseguinte, importa também o Princípio da Necessidade Militar, posto que, unidos e balanceados, os dois princípios explicitam o sentido do DIH, não de legitimar ou mesmo encorajar hostilidades[209], mas de limitar o que pode ser feito e utilizado em conflitos armados.

3.1.2 Princípio da Necessidade Militar

Busca-se uma situação de equilíbrio, onde o ditame da necessidade militar permite que as partes em conflito utilizem da violência armada que seja necessária para alcançar seus objetivos militares. Sem ser um imperativo em razão do preceito da humanidade, a necessidade militar, em seu sentido mais "puro" e abrangente, entende que uma parte possa fazer aquilo que seja necessário para derrotar o inimigo ou ganhar a guerra; em outras palavras, tolera que mortes, destruição e sofrimento sejam causados em tempos de conflito, vez que venham a ser

[208] Em 1994, a AGNU solicitou parecer consultivo da Corte de Haia sobre a violação do Direito Internacional nos casos de uso ou ameaça de armas nucleares, quando ainda não havia convenção sobre a proibição de armas nucleares. A CIJ emitiu opinião no sentido de que a Cláusula de Martens por si já limitaria o uso de armas nucleares, vez que o meio de guerra, por sua natureza, violaria os ditames da consciência pública e os princípios humanitários (CIJ, 1996, p. 37). Trata-se de colocação que demonstra o propósito da cláusula: obstar quaisquer alegações de vácuo jurídico humanitário diante da rápida evolução da tecnologia militar (DINNISS, 2012, p. 28).
[209] Nesse sentido, Daniel Thürer (2011, p. 68-69) ressalta: "The expression of military necessity is an expression of international humanitarian law's indifference to the question of the permissibility or legitimacy of war in a specific situation".

militarmente cruciais, enquanto medidas de segurança mais severas daquilo que seria permitido em períodos de paz (THÜRER, 2011, p. 68; MELZER, 2019, p. 17-18).

O princípio em questão, contanto, não traz uma carta branca para atos de guerra ilimitados, mas permite o uso proporcional[210] da força em casos de conflitos armados com vistas à rendição ou degradação das forças armadas inimigas (CINELLI, 2016, p. 68). Sua interpretação mais restritiva e, de fato, análoga à essência do DIH como área jurídica codificada a partir do século XIX[211], enxerga que as medidas mais severas – potencialmente resultando em vitimizações – só devem ser adotadas quando se mostrarem imprescindíveis, absolutamente necessárias, implicando em vantagem militar precisa.

Logo, a importância militar de se obter a vitória pode justificar o ferimento e morte de civis, desde que todas as possíveis precauções[212] para os proteger tenham sido adotadas, bem como formas mais seguras de se alcançar a vantagem militar tenham sido exploradas e consideradas insatisfatórias (THÜRER, 2011, p. 70). Torna-se mister o dever de estudar todas as opções alinhadas ao objetivo militar, para que os efeitos de um ataque não atinjam ou repercutam em alvos que não sejam considerados legítimos perante as normas humanitárias.

Opondo-se à utilização dos princípios fundamentais de humanidade e de necessidade militar de forma demasiadamente vaga – dando possíveis brechas a justificativas de comportamentos contrários à essência do direito convencional ou consuetudinário –, Jeroen C. Van Den Boogaard (2013, p. 25-26) reflete que a necessidade militar deve ser tratada mais como uma política do que como um princípio jurídico abstrato, balizando o leque de opções que podem ser tomadas por uma parte beligerante para que ocorra o mínimo possível de vitimizações em seus ataques, mesmo que isso denote em práticas mal vistas internacionalmente[213].

---

[210] Disto, percebe-se a procedência do Princípio da Proporcionalidade.

[211] Diz-se o DIH moderno, com a propagação de ideias humanistas e preocupação com a dignidade humana; aliás, o Princípio da Necessidade Militar, como se vê hoje, tem origem positivada pelo Código Lieber (1863), de onde se extrai o que seria necessidade militar: "consists in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war". (CRAWFORD; PERT, 2015, p. 109). A alegação de império de necessidade militar é historicamente anterior ao DIH moderno, e vincula-se à citada doutrina *Kriegsraison*, a qual, na atualidade, após período de "humanização" do direito – em que pese as recaídas ocasionais, infelizes e contranormativas –, não têm espaço nos fundamentos humanitários (SCHMITT, 2020, p. 148).

[212] Recorda-se o Princípio da Precaução, como outro possível regramento decorrente dos preceitos de equilíbrio abordados até então. O mesmo tem ligação direta com a distinção, vez que assevera seu intuito protetivo no constante cuidado que deve ser tomado por ambas as partes beligerantes para que as pessoas e bens civis sejam poupados, inclusive de danos incidentais; vide arts. 57 (1) e 58 do PA I – precauções no ataque e precauções contra os efeitos do ataque (MELZER, 2019, p. 18-19).

[213] Mesmo sem fazer qualquer alusão às armas cibernéticas, Van Den Boogaard (2013, p. 25-26) questiona a viabilidade dos princípios do DIH, por meio da Cláusula de Martens, exercerem uma função corretiva frente ao direito consuetudinário e convencional; o especialista reflete se, em alguns casos, utilizar de armas que já sejam restritas ou proibidas por um tratado, mas se apresentam como a melhor opção – causando menos vítimas – não

Sob o prisma do uso de operações cibernéticas, a colocação de Van Den Boogaard faz ponderar sobre as discussões em que as atividades militares por meios cibernéticos podem ser priorizadas em nome do menor custo humano, quando capazes de alcançar a mesma vantagem precisa[214]. Categoricamente, o sentido dos preceitos da humanidade e da necessidade militar é exatamente este: estimular que as decisões, sejam elas políticas, estratégicas, operacionais ou táticas, tomadas por um Estado, vigorem conforme a máxima da proteção de vítimas; que o emprego da violência – e suas consequências atingindo civis – seja o menor possível. Trata-se de situação que ocasionalmente requer um juízo de determinação de armas e alvos aceitáveis ou inaceitáveis bastante complexo (CINELLI, 2016, p. 70), que não deixa de existir quando referindo-se aos meios cibernéticos e havendo acometimento da infraestrutura civil interconectada e de dados civis no ciberespaço.

Enquanto preceito complementar ao da humanidade, a necessidade militar traz a base para se compreender os demais princípios humanitários, que seguem uma lógica restritiva-permissiva às operações militares, requerendo a reflexão de situações práticas em conflitos armados. À primeira vista, diante da difícil visualização imediata sobre como ataques cibernéticos podem resultar em vitimizações (o que, tradicionalmente, ocorre de forma objetiva, causando mortes ou ferimentos físicos diretos), sob os preceitos mencionados, os meios e métodos cibernéticos tendem a ser estimulados em detrimento das armas e procedimentos convencionais. De fato, eles podem proporcionar que os conflitos se deem de forma menos "sanguinária", mas presumir que não oferecem qualquer risco humano ou que não carecem de debate multilateral, em razão do direcionamento já oferecido pelos princípios, é um erro.

Alguns desafios operacionais provenientes do uso inadvertido de operações cibernéticas em conflitos armados podem ser melhor observados à luz dos princípios da proporcionalidade e da distinção, que possuem delimitações mais concretas e tendem a ser mais diretivos – menos abstratos –, e que por isso encontram maiores dificuldades na aplicabilidade e eficácia diante dos meios e métodos cibernéticos. Imagine-se que, numa situação em que dois Estados se

---

poderiam ser preferidas em nome da humanidade e da necessidade militar. Ainda não há qualquer acordo multilateral para os casos de operações cibernéticas em conflitos armados, mas a colocação é válida para se pensar como possíveis atos – espionagem cibernética, etc., ou até mesmo ataques cibernéticos com potencial de resultar em destruição e mortes –, os quais sejam vistos como de violação aos princípios gerais de não-intervenção e de respeito à soberania estatal, tendem a ser preferíveis em nome da obtenção da mesma vantagem militar com uma menor taxa de dano colateral: havendo a prevalência dos princípios humanitários.

[214] Esse ponto de vista é observado por Gary P. Corn (2019): "[...] too frequently analysis of new military Technologies gravitates immediately toward the negative, presuming adverse humanitarian impacts while understanding not only the possible military advantages new technologies may offer, but also ignoring the real potential they may have to actually mitigate the risks to civilians and other protected persons arising from hostilities. This tendency often results in overstatements of risk and premature calls for new regulation or outright bans".

encontram em conflito armado, um deles nomeadamente[215] lança ataque cibernético contra hospital em funcionamento e devidamente sinalizado, de modo a levar à paralisação de suas atividades e pôr em risco a vida de centenas de civis e feridos de guerra; *a priori*, com base nas percepções discutidas até então, trata-se de violação das Convenções de Genebra[216], coadunando como crime de guerra. Todavia, se o sistema informacional dessa mesma unidade de saúde é utilizado como aparato para comunicações militares da parte adversa, é possível que o ataque seja legítimo, tendo em vista a caracterização da unidade como objetivo militar[217]. Ainda assim, diversos parâmetros devem ser analisados no caso a caso, desde a averiguação se o tipo de ataque cibernético em questão seria o melhor para o fim almejado, até a reflexão se os danos resultantes do tipo de ataque optado podem ser considerados excessivos frente à vantagem militar esperada. Esta avaliação relaciona-se diretamente com o Princípio da Proporcionalidade.

3.1.3 Princípio da Proporcionalidade

Pelo Princípio da Proporcionalidade, compreende-se que, numa situação excepcional de guerra, é previsível que ocorram mortes e danos a civis e objetos civis, mas as ações que levarem a essas consequências devem ser proporcionais à vantagem militar pretendida. Por mais que existam proibições a ataques contra determinados bens e pessoas, em razão da vantagem militar que determinada ação oferece, é possível que ocorram danos colaterais; caso em que esses ataques não serão considerados ilegítimos, pois, para alcançar o objetivo militar, foi necessário perpassar ou atingir incidentalmente tais pessoas e/ou bens. Entretanto, para fins de não banalizar os ataques que colateralmente aflijam os protegidos pelo DIH em nome da necessidade militar, é que vigora a norma[218] da proporcionalidade, ao proibir ataques que se mostrem indiscriminados e excessivos:

> Art. 57 – Precauções no ataque
> [...]
> 2. No que respeita aos ataques, devem ser tomadas as seguintes precauções:
> b) um ataque deverá ser cancelado ou interrompido quando parecer que seu objetivo não é militar, ou é beneficiário de uma proteção especial, ou que possa vir a causar acidentalmente perdas de vidas humanas na população civil, ferimentos nos civis,

[215] Sabe-se, contudo, que a praxe internacional tem exibido a dificuldade em atribuir a autoria de ataques cibernéticos em razão de dissimulações, sendo esta outra questão a ser enfrentada.
[216] Ao que expõe o art. 19 da I CG, o art. 18 da IV CG, e reitera o PA I, art. 12 (1).
[217] Vide art. 21 da I CG, art. 19 da IV CG; arts. 12 (4) e 13 do PA I.
[218] A partir do PA I, em diversos momentos o preceito da proporcionalidade se expõe: art. 51 (5)(b), art. 57 (2)(a)(iii) e também (b), (3), citados (MELZER, 2019, p. 19).

> danos em bens de caráter civil ou uma combinação dessas perdas e danos que seria **excessiva em relação à vantagem militar concreta e direta esperada**.
> [...]
> 3. Quando for possível a escolha entre vários objetivos militares que proporcionem vantagem militar equivalente, **a escolha deverá recair sobre o objetivo cujo ataque parece representar o menor perigo para os civis ou para os bens de caráter civil**. (CICV, 2017, p. 43-44, grifo nosso)

Zen Chang (2017, p. 41-45), ao refletir sobre a adaptabilidade da regra da proporcionalidade às operações cibernéticas, destaca a proibição aos ataques que causem danos a objetos civis de forma excessiva em relação à vantagem militar antecipada, nos termos do art. 51 (5)(b) do PA I, e o problema dos efeitos indiretos como os principais tópicos que requerem aprofundamento. Os danos a objetos civis a partir de operações cibernéticas, tema já citado ao longo desta pesquisa, não devem ser comparados aos danos resultantes de ataques cinéticos como tradicionalmente posto, e o estabelecimento de um critério com base na perda da funcionalidade pode ajudar a esclarecer o que seria um "ataque" [219]. Contudo, ao passo que uma operação militar possa afetar a infraestrutura civil, sobretudo prejudicando seu funcionamento, cabe a aplicação ética e racional da proporcionalidade – o emprego de operações cibernéticas, como qualquer outra operação militar, deve ser arquitetado de modo a analisar todos os possíveis efeitos aos civis.

O juízo de proporcionalidade entre danos colaterais e a vantagem militar "concreta e direta[220]" não recai em tarefa simples. De fato, cumpre aos responsáveis pelo planejamento, deliberação ou execução dos ataques a tomada de decisão de acordo com a análise de todas as informações e fontes disponíveis no momento relevante, para que atue ponderando qual o melhor meio e método para atingir o fim almejado causando o mínimo de perdas e danos possível[221] (HENCKAERTS; DOSWALD-BECK, 2005, p. 50). Quando lidando com ataques cibernéticos em detrimento de ataques cinéticos, cabe a averiguação sobre se determinados *malwares* possuem uma natureza voltada à finalidade militar, restringindo-se a tanto, ou se podem implicar em danos a objetos civis, com a deliberação sobre em que medida esses danos não seriam considerados excessivos.

---

[219] Como exposto no capítulo anterior, à luz das discussões de especialistas no Manual de Tallinn 2.0, e considerando que a própria equiparação de resultados pode servir como brecha para que operações cibernéticas sejam empregadas pelos Estados inadvertidamente, já que por vezes não resultam em "danos" como destruição física.

[220] A antecipação dos efeitos e a contribuição para os objetivos militares da parte (SANDOZ; SWINARSKI; ZIMMERMAN, 1987, p. 683-684).

[221] Diversos Estados apregoam nesse sentido, com manuais para suas forças armadas em conformidade com o DIH, especialmente, à luz dos arts. 51 a 58 do PA I (HENCKAERTS; DOSWALD-BECK, 2005, p. 50).

Os ataques cibernéticos resultam em efeitos indiretos – os danos causados aos bens protegidos é que poderão implicar em mortes, ferimentos, sofrimento desnecessário – e, sob a ótica da proporcionalidade, há divergências entre os Estados[222], já que não há uma mensurabilidade imediata desses efeitos, e, portanto, do que seria "excessivo" em relação a uma vantagem militar. Todavia, da interpretação convencional e costumeira que origina o princípio em comento, fica claro que deve haver uma análise sobre se os efeitos indiretos ou incidentais às infraestruturas civis eram razoavelmente previsíveis, ainda que remotos; é o que decorre da leitura dos arts. 51 a 58 do PA I e da prática estatal até então consagrada[223]. Ademais, infere-se como vantagem "concreta e direta" que legitimaria as operações militares que sucedem perdas e danos civis de forma incidental, consoante comentários ao PA I, aquela a qual o resultado se mostre substancial e relativamente próximo, onde não se incluem as vantagens dificilmente perceptíveis ou que só apareceriam a longo prazo (SANDOZ; SWINARSKI; ZIMMERMAN, 1987, p. 684).

Nils Melzer (2019, p. 101-102) considera que "excessivo" é o termo-chave a ser examinado na equação de proporcionalidade, vez que denota subjetivismo, e que não há um padrão ou limiar para o "excesso". O pesquisador observa, ainda assim, que um grau de orientação objetiva pode advir do texto convencional, onde os danos incidentais a pessoas ou objetos protegidos só podem ser justificados por vantagens que, além de não serem de natureza meramente hipotética, indireta ou especulativa – ou seja, a "vantagem concreta e direta" –, sejam necessariamente de natureza "militar", logo, que não transcorram em nome de benefícios políticos, econômicos ou outros que não sejam militares. Nessa linha, cumpre a ponderação antecipada entre os efeitos indiretos e as vantagens pretendidas pela operação – uma avaliação dos riscos, ou do escopo do dano incidental que pode ser esperado –, que, na praxe beligerante, pode legitimar ou proibir um ataque cibernético às infraestruturas civis.

Em suma, levando a aplicabilidade do princípio ao espaço cibernético, é necessária a verificação sobre se as operações realizadas contra a infraestrutura civil podem causar consequências violentas e excessivas frente ao objetivo militar. Nesse contexto, operações cibernéticas que se destinem a destruir dados da parte adversária que corroborem como objetivo

---

[222] A prática estatal aponta certa disparidade, a exemplo dos EUA afirmando em manual do Departamento de Defesa (*Law of War Manual* 242, de 2015) que os danos remotos resultantes de ataques não devem ser considerados na análise de proporcionalidade, enquanto o Reino Unido (pelo Ministério da Defesa, *The Joint Service Manual of the Law of Armed Conflict*) indica uma maior preocupação com os efeitos previsíveis dos ataques (CHANG, 2017, p. 44).

[223] O CICV enumerou em normas o direito costumeiro, com dispositivo próprio ao princípio em questão: "Rule 14. Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited" (HENCKAERTS; DOSWALD-BECK, 2005, p. 46).

militar, não serão ilícitas nos termos do DIH. Mas, se tais operações atingem dados civis, como informações sensíveis de hospitais e serviços de saúde, fornecimento de água potável e de energia elétrica, serviços bancários essenciais e redes de telecomunicações, notoriamente cumpre a antecipação dos efeitos e a ponderação em comento – sobretudo se da operação for razoável se cogitar a consequência de mortes e danos a civis e destruição de objetos civis. Logicamente, trata-se de uma avaliação difícil e de um desafio para a interpretação da proporcionalidade nas condutas por meio cibernético, mas é esta espécie de provocação que faz com que surjam novas perspectivas de uma implementação mais efetiva das normas humanitárias.

Sem dúvidas, as operações cibernéticas manifestam-se também como tópico de grande preocupação em vistas à proporcionalidade na conduta militar por afetarem precipuamente infraestruturas ou objetos de uso duplo (*dual-use infrastructures* ou *dual-use objects*), como as citadas redes elétricas ou redes de telecomunicações, vez que as redes de computadores de uso civil e militar geralmente[224] estão interconectadas. Afinal, cumpre a capacidade das partes em conflito armado de utilizar-se de *malwares* que consigam se destinar unicamente à vantagem militar concreta e direta e cujos danos não sejam excessivos – ou, a partir do art. 57 (3) do PA I, que o *malware* escolhido seja aquele o qual recaia sobre o objetivo cujo ataque pareça representar o menor perigo para os civis e para os bens de caráter civil.

Por um lado, há quem se mostre desesperançoso acerca da possibilidade de acreditar que comandantes militares se inteirem de todos os aspectos de uma operação cibernética, preocupando-se sobre como e se a operação alteraria ou modificaria um único pedaço de código digital, e, portanto, avaliando a proporcionalidade nas ações no meio cibernético (CHANG, 2017, p. 43). Por outro, há que se perceber que o desenvolvimento das capacidades cibernéticas pelos Estados está em constante ascensão, logo, espera-se que a aptidão para avaliar com precisão o alcance dos danos incidentais dos ataques cibernéticos também esteja (DIAMOND, 2014, p. 79; MELZER, 2019, p. 42-43).

Em análise sobre o desenvolvimento da capacidade cibernética ofensiva pelo governo russo nas últimas décadas, Michael Connel e Sarah Vogler (2017) afirmam que um nível de personalização bastante sofisticado de um *malware* pode ser alcançado, e que diversos[225]

[224] Marco Sassòli (2019, p. 561) observa: Although passive precautions require that the network used by the military is separated from the used by civilians, no State does this for financial reasons and to ensure the resilience of its networks.

[225] Cita-se, a exemplo, a ferramenta de vigilância cibernética avançada nomeada BlackEnergy, e o *malware* Ouroboros como instrumentos altamente sofisticados e que, por sua natureza, segundo especialistas em cibernética, teriam levado anos para serem inteiramente programados (CONNEL; VOGLER, 2017, p. 19-21).

ataques cibernéticos já têm exposto que quanto maior o dano potencial da ação – especialmente para causar efeitos cinéticos –, maior tende a ser o planejamento e a destreza técnica para que se assegure que vulnerabilidades específicas de um sistema sejam atacadas. Assim, a previsão dos resultados reais, do ponto de vista estratégico, já faz parte da lógica ofensiva a qual a operação cibernética se destina; cumpre a análise pormenorizada dos efeitos primários, secundários e terciários, considerando a crescente necessidade das sociedades modernas de manter os serviços eletrônicos essenciais em funcionamento (SASSÒLI, 2019, p. 561).

Sob a ótica da proporcionalidade, portanto, uma operação cibernética pode vir a ser utilizada como meio e método em conflitos armados, mas de modo limitado e razoável frente aos objetivos almejados e aos efeitos esperados, o que pode ocorrer, a exemplo, em desativações temporárias da infraestrutura de uso duplo que coadune como alvo do ataque (SASSÒLI, 2019, p. 561), sem implicar em efeitos paralisantes de médio e longo prazo que aflijam infraestruturas civis e afetem excessivamente a população civil em geral (MELZER, 2019, p. 102). Ademais, a partir do que se aduz pelos textos convencional e consuetudinário[226], é incontestável que cumpre a cada parte no conflito tal avaliação dos efeitos de um ataque, de onde aguarda-se a precaução necessária mesmo nos casos em que a plena distinção entre objetivos militares e pessoas e objetos civis não possa se efetuar.

3.1.4 Princípio da Distinção

O princípio a partir do qual é regida a proteção de pessoas e bens, prescreve a dicotomia crucial em tempos de guerra: distinguir o que pode ser alvo de operações militares, e o que não deve ser. A distinção, como critério basilar para a conduta das partes beligerantes, proíbe que operações se realizem de forma indiscriminada, ou seja, sem a efetiva diferenciação de quem vem a ser combatente e quem é civil, e o que é objetivo militar e o que é bem ou objeto civil.

Apesar de afirmado mais recentemente no art. 48 do PA I, já no preâmbulo da Declaração de São Petersburgo de 1868 o Princípio da Distinção foi exposto como fundamento do direito consuetudinário em cenários de guerra, quando da acepção de que o único objetivo legítimo dos Estados em guerra é o enfraquecimento das forças adversárias (MELZER, 2019,

[226] Rule 18. Each party to the conflict must do everything feasible to assess whether the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.
Rule 19. Each party to the conflict must do everything feasible to cancel or suspend an attack if it becomes apparent that the target is not a military objective or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated. (HENCKAERTS; DOSWALD-BECK, 2005, p. 58-60).

p. 18). Lembrando, ligeiramente, o axioma clausewitziano onde a guerra é descrita como ato de força destinado a forçar o inimigo à vontade da outra parte, a diretriz constante na Declaração de 1868 desenvolveu-se a par das premissas de humanidade como classificação de pessoas e bens, para que então as operações sejam conduzidas pelas partes em conflito.

Nessa vereda, a classificação em comento baliza a ação ofensiva para que esta seja legítima, desde que seja voltada unicamente contra combatentes[227] e objetivos militares. Por objetivos militares, compreende-se, pelo art. 52 (2) do PA I, aqueles que "por natureza, localização, destino ou utilização contribuem efetivamente para a ação militar e assim sua destruição total ou parcial, sua captura ou neutralização oferecem, nestes casos, uma vantagem militar precisa"; enquanto figuram como bens civis, por critério negativo, aqueles que não se enquadrem como militares (CICV, 2017, p. 40).

Ocorre que, na linguagem da Era da Informação, onde as infraestruturas cibernéticas geralmente são de uso duplo, torna-se cada vez mais difícil separar o que vem a ser bem civil e o que serve para o propósito militar. Do ponto de vista de plena adaptação dos dispositivos do PA I à sociedade em rede, corre-se o risco de uma abertura de brecha para que quase todos os elementos da infraestrutura cibernética internacional – cabos, roteadores, satélites, dados, sejam elementos de *hardware* ou *software*, etc. – possam ser suscetíveis de ataques, já que transmitem também informação militar e que, portanto, podem ser alvos legítimos pela interpretação dos arts. 48 e 52 (2) e pela praxe internacional sobre objetos de uso duplo[228] (DIAMOND, 2014, p. 77-78; MELZER, 2019, p. 92-93; SASSÒLI, 2019, p. 403).

Contudo, é nesse diapasão sobre uso de operações cibernéticas que a distinção entre objeto civil e objetivo militar mostra-se inteiramente interconectada com o Princípio da Proporcionalidade. A definição do *status* do alvo da operação cibernética nos casos de objetos de uso duplo em civil ou militar dependerá da vantagem militar definitiva em que implique no

---

[227] A definição de combatentes e civis, para o enquadramento do DIH, foi discutida no item 2.3 desta pesquisa, quando da caracterização das vítimas de guerras cibernéticas.

[228] Dual-use objects, however, do not constitute a separate category in IHL. Rather, when a certain object is (or may reasonably be expected to be) used for both military and civilian purposes, even a secondary military use turns it into a military objective under Article 52 (2) (SASSÒLI, 2019, p. 403).
Pela prática internacional dos Estados, diversos manuais militares contêm a definição do artigo 52 (2), reiterada por declarações oficiais; ademais, é o que se vê na composição das Regras 8, 9 e 10 do DIH consuetudinário pelo CICV:
Rule 8. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. […]
Rule 9. Civilian objects are all objects that are not military objectives. […]
Rule 10. Civilian objects are protected against attack, unless and for such time as they are military objectives. (HENCKAERTS; DOSWALD-BECK, 2005, p. 29-36).

caso concreto, e a legitimidade da operação estará estreitamente ligada à ponderação entre os danos colaterais e a vantagem obtida.

O caso da campanha aérea da OTAN sobre a ex-Iugoslávia, em 1999, quando do bombardeio da Radio Television Serbia (RTS) de Belgrado, ilustra a discussão acerca da complexa definição do papel que um objeto de uso duplo está assumindo. Vez que, por premissa jurídica, o *status* de objeto civil e objetivo militar não pode coexistir[229] (SCHMITT, 2017, p. 445), indagou-se se a estação de transmissão de TV e rádio, por supostamente estar servindo como instrumento de propaganda do governo, e como elo da rede de comando, controle e comunicação das forças sérvias, seria um objetivo militar. Nesse caso, o Tribunal Penal para a Ex-Iugoslávia (ICTY) adotou a posição de que a mídia não seria objetivo militar legítimo meramente por distribuir propaganda, pois tal atividade faz parte da realidade bélica e do incentivo à persistência moral na guerra para a população; quanto ao ataque de bombardeio efetuado, todavia, o Tribunal concluiu que a estação da RTS de fato estava sendo utilizada como retransmissor das forças armadas, e que por isso seria objetivo militar, sendo os danos infligidos à máquina de propaganda apenas objetivos incidentais. De todo modo, a decisão do Tribunal suscitou controvérsias sobre a vantagem militar do bombardeio, mormente por argumentos no sentido de que o ataque não teria sido proporcional. (CINELLI, 2016, p. 71-72).

Marco Sassòli (2019, p. 404-405) destaca que os ataques a objetos de uso duplo são um problema corrente, e que, independentemente da tratativa às operações cibernéticas, a compreensão precisa do art. 52 (2) e do que vem a ser um objetivo militar na praxe estatal pode sofrer novos traços[230] conforme as decisões de cada governo e o impacto que deseja causar na parte adversa, inclusive implicando em ataques a alvos políticos, financeiros e econômicos para enfraquecer ou influenciar a capacidade do inimigo de continuar a guerra – coadunando com a lógica dos conflitos assimétricos, sobretudo quando uma parte não está disposta a ocupar o Estado inimigo e deseja utilizar-se de outros meios. É o que se vê, inclusive, em documentos

[229] As a matter of law, status as a civilian object and military objective cannot coexist; an object is either one or the other (SCHMITT, 2017, p. 445).

[230] Acquiring a non-military advantage over the Enemy can more effectively accomplish that aim. […] If the enemy is seen as a system, attacks upon certain targets that politically, financially or psychologically sustain an enemy regime may have a greater impact than attacks that affect military operations. In many countries, the centre of gravity is not in the armed forces. […] The limitation to military objectives may also oblige belligerents to provide hypocritical justifications for their attacks. When they interrupt the power supply to show the civilian population that it will live in the dark as long as it does not get rid of a regime, they must claim that the power stations also produce power for the military. When they attack a radio station because it maintains the morale of the population, they must assert that the station also serves as a military communications relay station. Nevertheless, hypocrisy also demonstrates the opinion juris of States and therefore contributes to the development of IHL's rules. (SASSÒLI, 2019, p. 404-405).

do Departamento de Defesa dos EUA[231], onde se presume que a definição de "objetivo militar" engloba objetos econômicos associados, indústrias que de algum modo ofereçam sustentação à guerra, etc., em interpretação demasiadamente abrangente (SCHMITT, 2017, p. 441).

De toda sorte, é nítida a ausência de uma definição alternativa que se mostre praticável e objetivamente avaliável que não assimile "objetivo militar" pela contribuição ao esforço militar (SASSÒLI, 2019, p. 405). Na realidade técnica do espaço cibernético, o que vem a ser ou não objetivo militar torna a aplicabilidade da distinção ainda mais difícil. Pelos Comentários aos Protocolos Adicionais promovidos pelo CICV em 1987[232], a interpretação do art. 52 do PA I sugere que o termo "objeto" implica em coisa material, visível e suscetível de apropriação; o termo "objetivo" igualmente sugere ponto ou alvo tangível, de modo a tradicionalmente englobar como militares aquela categoria de objetos usados pelas forças armadas, como armas, equipamentos, meios de transporte, construções ocupadas pelas forças armadas, depósitos, centros de comunicações, etc. (SANDOZ; SWINARSKI; ZIMMERMAN, 1987, p. 633-634).

Notoriamente as sugestões de 1987 não são coerentes com o atual contexto cibernético, razão pela qual academicamente bastante se problematiza o que pode ser alvo de operações cibernéticas em situação de conflito armado – se apenas a infraestrutura física cibernética, ou *hardware*, pode ser compreendida como objetivo militar, ou se os dados inseridos nos sistemas, *software*, podem ser também assimilados como "objetos" e, portanto, como objetivos militares. Os especialistas do Manual de Tallinn 2.0, em sua maioria, concordaram que a noção de "objeto" para o DIH não deve incluir dados, ao menos por ora, considerando-se o estado atual das normas de conflitos armados. Segundo eles, vez que intangíveis, aos dados não se enquadrariam no sentido de "objeto" a que se refere o PA I, mas poderiam receber tal qualificação com base nos efeitos da operação militar – ou seja, em situações onde uma operação cibernética acometa dados de forma a afetar a funcionalidade da infraestrutura cibernética ou resultando em outras consequências que qualifiquem a ação como "ataque", os dados poderiam ser vislumbrados como objetos na conotação das regras de conflitos armados (SCHMITT, 2017, p. 436-437).

---

[231] *The US Department of Defense Law of War Manual*, onde se vê a interpretação norte-americana de "objetivo militar" abrangendo aqueles que porventura estejam associados ou deem suporte à guerra, inclusive econômico. Por essa interpretação, a indústria de exportação de petróleo de um Estado inimigo poderia ser alvo de ataques segundo o DIH, se as receitas provenientes das vendas de petróleo auxiliarem economicamente ao Estado em questão. Trata-se de abordagem que permite conexões bastante remotas e até mesmo inconclusivas sobre a contribuição efetiva do alvo para a ação militar (SCHMITT, 2017, p. 441).

[232] Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, em comitê organizado pelo CICV (SANDOZ; SWINARSKI; ZIMMERMAN, 1987).

Apenas uma minoria dos especialistas assentiu para a compreensão, conforme "*the laws of targeting*" – as quais implicam no balizamento dos princípios para a condução das hostilidades –, de que determinados dados devem ser considerados como objetos. Tal posicionamento[233] preza pela proteção geral dos bens e populações civis consagrada desde o art. 48 do PA I, tendo em vista que excluir do escopo de "objetos" para a lei dos conflitos armados determinados dados civis essenciais, como dados bancários, registros fiscais, de previdência social, etc., deixaria os civis à mercê de ciberataques sem o alcance regulatório do DIH e, portanto, desprotegidos. Dessarte, percebe-se que a conclusão majoritária dos especialistas do Manual de Tallinn vai contra o objeto e propósito do DIH; percepção essa também notada pelo CICV[234] ao ressaltar a importância dos Estados entrarem em um entendimento comum sobre em que medida dados civis são protegidos pelo DIH. (SCHMITT, 2017, p. 437; SCHMITT, 2019, p. 341-342; CICV, 2019, p. 8).

De todo modo, nota-se uma zona de insegurança jurídica sobre a (i)legalidade de operações cibernéticas que tenham como alvo dados colocados no ciberespaço. Diante das incertezas na interpretação da lei dos conflitos armados quanto à qualificação de dados, pesquisadores do projeto *Cyber Law Toolkit* e sob suporte do CICV e do CCDCOE, organização sobre defesa cibernética credenciada pela OTAN, resumem os pontos de diferença entre as possíveis abordagens interpretativas perante o DIH, a partir de acepções gerais onde os dados podem ser considerados como objetos, ou de que não podem. São postas três situações de qualificação dos dados, como militares, civis essenciais e civis que não essenciais. Os dados militares seriam aqueles que fundamentadamente cumpram as vertentes dispostas no art. 52 (2) do PA I; já os dados tidos como "essenciais" carecem de delimitação precisa, tornando-se cada

---

[233] For these Experts, the key factor, based on the underlying object and purpose of Article 52 of Additional Protocol I, is one of the severity of the operation's consequences, not the nature of harm. Thus, they were of the view that, at a minimum, civilian data that is 'essential' to the well-being of the civilian population is encompassed in the notion of civilian objects and protected as such. (SCHMITT, 2017, p. 437).

[234] Conforme o parecer do CICV sobre o DIH e operações cibernéticas durante conflitos armados, que reitera outros documentos emitidos pela entidade:

Some of the specific protection afforded by IHL extends to essential data, such as data belonging to medical units, which are encompassed in the obligation to respect and protect such units. More generally, the main IHL principles and rules governing the conduct of hostilities protect civilians and civilian objects. It would therefore be important for States to agree on an understanding that civilian data is protected by these rules. Deleting or tampering with essential civilian data can quickly bring government services and private businesses to a complete standstill. Such operations could cause more harm to civilians than the destruction of physical objects. While the question of whether and to what extent civilian data constitute civilian objects remains unresolved, **in the ICRC's view the assertion that deleting or tampering with such essential civilian data would not be prohibited by IHL in today's data-reliant world seems difficult to reconcile with the object and purpose of IHL**. The replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them. **Excluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap**. (CICV, 2019, p. 8, grifo nosso).

vez mais complexo definir quais dados não são imprescindíveis[235] para o funcionamento da vida civil nos dias atuais.

Quadro 1 – Pontos de diferença entre as duas abordagens interpretativas dominantes da qualificação de dados como objetivo militar

	Dados ≠ Objeto	**Dados = Objeto**
1ª hipótese (operações cibernéticas contra conjuntos de dados militares)	Como os dados não são um "objeto" para os fins do DIH, eles não precisam preencher os critérios de um objetivo militar para que uma operação contra eles seja legal sob o DIH. Assim, desde que outras regras aplicáveis do DIH sejam cumpridas, todas essas operações cibernéticas seriam permitidas.	Permissível desde que o conjunto de dados cumpra as vertentes da definição de objetivos militares.
2ª hipótese (operações cibernéticas contra conjuntos de dados civis essenciais)		Proibido, devido ao caráter não militar e ao uso dos conjuntos de dados em questão.
3ª hipótese (operações cibernéticas contra conjuntos de dados civis não essenciais)		Proibido, devido ao caráter não militar e ao uso dos conjuntos de dados em questão, a menos que justificado sob a exceção habitual para operações psicológicas e de propaganda.

Fonte: CYBER LAW TOOLKIT, 2021.

No campo de distinção entre civis e combatentes[236] e, sobretudo, entre objetos civis e objetivos militares no contexto do ciberespaço, até então há muito que ser debatido tanto academicamente como nas relações entre os Estados. Surgem diversas abordagens que possibilitam uma tratativa e classificação entre dados, distinguindo até mesmo aqueles que seriam de nível operacional e aqueles que seriam de conteúdo: os de nível operacional remetem aos dados os quais o funcionamento da infraestrutura cibernética é dependente, já os de conteúdo são aqueles que apenas representam informações em forma de dados (SCHMITT, 2019, p. 341-342; GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 318-319). Mas a classificação de dados, por si, para qualificar quais dialogam com o Princípio da Distinção e,

[235] É possível a analogia aos dados dos quais dependem os bens especialmente protegidos pelo DIH, como unidades de saúde, propriedade cultural, o meio ambiente natural, obras ou instalações contendo forças perigosas, etc., à luz do que dispõe o PA I. Note-se, contudo, que os "bens indispensáveis à sobrevivência da população civil", conforme traz o art. 54 do PA I, não abrigam uma lista exaustiva de objetos.

[236] O Manual de Tallinn 2.0 também faz ponderações sobre quem são as pessoas que podem, à luz do DIH, ser objeto de ataque cibernético: membros de forças armadas, membros de grupos armados organizados, civis ao tempo que participam diretamente das hostilidades, e os participantes de *levée em masse*; vide Regra 96 do Manual (SCHMITT, 2017, p. 425-428).

portanto, com as normas de condução das hostilidades e com o direcionamento sobre quais operações podem ser deflagradas legitimamente e quais se julgam como "ataque", ainda é bastante problemática[237] e controversa.

Naturalmente, interpretação que seja restritiva demais, ao ponto de não considerar como atos de guerra determinadas operações cibernéticas, de impossibilitar a visualização como "ataque" dessas, ou de obstar quaisquer dados como objetos civis, é oposta à essência do DIH. Ao apregoar pela proteção daqueles em situação de vulnerabilidade em conflitos armados, o exame das normas humanitárias diante do ciberespaço deve considerar uma necessária diferenciação entre as partes do que vem a ser alvo lícito, e, portanto, uma categorização dos dados mostra-se imprescindível. Esse talvez seja um dos principais aspectos que demonstram o papel que um acordo internacional na matéria específica do DIH aplicável ao espaço cibernético pode ter, ao fomentar discussões sobre contra quem e contra o que, de fato, os Estados em conflito podem direcionar suas operações cibernéticas.

3.2 O problema da responsabilização estatal

Pelo princípio "cardinal" e "intransponível"[238] da distinção (CIJ, 1996), não só os objetos devem ser diferenciados, mas também os combatentes e população civil. Eis, portanto, mais um dentre diversos problemas quando se trata a guerra cibernética. Como levar ao campo do ciberespaço a obrigação posta pelo DIH em conflitos internacionais da distinção entre os atores? Aos que conduzem operações cibernéticas, será que não o fazem em razão da maior vantagem de dissimulação, ou será que, categoricamente, as utilizam alegando uma tecnologia que implique em menos danos incidentais?

---

[237] Sobre a posição da minoria dos especialistas do Manual de Tallinn e do CICV sobre os dados como objeto, Michael Schmitt (2019, p. 342-343) reflete: Unfortunately, no legal justification beyond the rather general claim of compliance with object and purpose has been offered to support it. Nor has useful, granular guidance explicating its implementation been set out. Moreover, such an approach glosses over the fact that the issue at hand is a definitional one. This begs the question of the normative logic of characterizing certain data as an object based on severity of the consequences, but not doing so vis-à-vis other data when the consequences of damaging or altering it are less serious. It might make sense to draw a transactional legal line on the basis of consequences caused, as is done with the rule of proportionality, but the same reasoning does not apply when merely defining a term. The debate will not be resolved in the near future, for adopting an approach by which data either is or is not an object leads to results that are unsatisfactory and impractical. And although considering the severity of consequences for the civilian population seems to reflect the foundational purposes of IHL, the lack of a clear legal basis for the position renders it *lex ferenda*, rather than *lex lata*.

[238] Como denominado pela CIJ na Opinião Consultiva sobre a Legalidade da Ameaça ou Uso de Armas Nucleares, parágrafos 78 e 79: "The cardinal principles [...]. The first is aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants […] they constitute intransgressible principles of international customary law." (CIJ, 1996, p. 257).

O PA I reitera a importância[239] de distinguir combatentes durante operações militares; trata-se de uma diferenciação sobretudo visual, para que a população civil seja protegida dos efeitos das hostilidades. Nos termos até então tradicionais e "pré-cibernéticos", o combatente em conflitos armados internacionais é caracterizado como aquele que é subordinado a um comandante responsável, que utiliza emblema distintivo fixo e reconhecível à distância, que obedece às leis e costumes de guerra, e que porta armas abertamente (DETTER, 2013, p. 148-149); assumindo-se que, quando pela natureza da hostilidade não for possível a distinção pelo uniforme, deverá ser caracterizado por portar suas armas abertamente (SANDOZ; SWINARSKI; ZIMMERMAN, 1987, p. 527-529).

Para os conflitos exclusivamente por meios cinéticos, os critérios de separação entre combatentes e civis são extremamente úteis, quando respeitados. Nitidamente, a mesma lógica enfrenta impasses nos conflitos da contemporaneidade, de forma ainda mais complexa diante da condução de operações cibernéticas. Afinal, permeia a discussão sobre ser ou não possível a distinção daqueles que conduzem tais operações, vez que não atuarão enquanto sujeitos manifestos nos campos de batalha tradicionais, mas em qualquer localidade e estrutura que permita a programação dos dados. Conjuntamente a esse pensamento de identificação dos sujeitos envolvidos, também consta a difícil perspectiva de atribuição de uma conduta no ciberespaço para fins de responsabilização da parte transgressora dos preceitos humanitários.

Sobre essas discussões, há que se convir que traçar a distinção visual entre civis e combatentes em meio a guerras cibernéticas não consiste em um assunto imperioso. Não só pela própria natureza do novo meio e método de guerra, mas também ao se ponderar que, conforme o DIH, apenas pessoas e não objetos (onde se incluem os dados) possuem o dever de se distinguir entre si; e à matéria de operações cibernéticas mais importa reconhecer a qualidade dos dados. A caracterização dos indivíduos mais interessa à seara cibernética e aos fins humanitários quando no momento de captura dos que supostamente conduziram a operação (SASSÒLI, 2019, p. 560).

---

[239] Vez que a distinção já era preconizada desde a Declaração de Bruxelas de 1874. No PA I, observa-se:
Artigo 44 – Combatentes e prisioneiros de guerra
[...] 3. Para que a proteção da população civil contra os efeitos das hostilidades seja reforçada, os combatentes devem se distinguir da população civil quando tomarem parte em um ataque ou em uma operação militar preparatória para um ataque. No entanto, levando em conta que há situações nos conflitos armados em que, devido à natureza das hostilidades, um combatente armado não pode se distinguir da população civil, ele conservará o estatuto de combatente desde que, em tais situações, use as suas armas abertamente:
a) durante cada ação militar; e
b) enquanto estiver à vista do adversário, ao tomar parte em uma evolução militar que precede o lançamento do ataque em que deve participar.
Os atos que satisfizerem as condições previstas pelo presente parágrafo não são considerados como perfídia, nos termos do artigo 37, parágrafo 1, alínea (c). (CICV, 2017, p. 34-35).

Aliás, do ponto de vista de atribuição de autoria de ciberataques, convém refletir que, se mesmo em cenários de conflito armado já iniciado, o DIH – e, portanto, os princípios protetivos – só se aplica a operações vinculadas ao conflito, também não parece ser pertinente ao ator de um ciberataque identificar-se como parte beligerante, seja como sujeito ou pela natureza dos dados que destina (*malwares*, etc.) e que acomete. Outrossim, enquanto estivesse, com sucesso, dissimulando sua autoria, poderia mais facilmente evadir-se de responsabilizações e violar o direito internacional, onde se inclui o DIH.

Frente a isso, ciente do potencial uso descomedido de ataques cibernéticos e da possível zona cinzenta na condução das hostilidades, o CICV tem reforçado que a difícil atribuição de autoria não deve ser vista como um obstáculo para aqueles Estados que conduzem, dirigem ou controlam operações cibernéticas: aos olhos do direito internacional, um Estado é responsável por todas as condutas que lhe sejam imputáveis, como violações do DIH – ainda que essas ocorram mediante novas armas e formas de guerra (CICV, 2019, p. 8-9).

À atribuição de condutas no ciberespaço, não só o denominado "*peopleware*", ou quem são os especialistas em uso das estruturas e dos programas informacionais envolvidos, é relevante. A análise das três camadas que compõem o espaço cibernético, quais sejam o *peopleware*, o *software* e o *hardware*, merece atenção (OLIVEIRA; PORTELA, 2017, p. 77-81). Há no *peopleware* os recursos humanos empregados no espaço cibernético, ou seja, a identificação dos sujeitos que operacionalizam ciberataques, e que poderiam se assemelhar à figura dos combatentes pelo DIH; todavia, ainda é incerto como essa qualificação poderia ser feita. Já no *software*, camada que abarca sistemas e que permite as ações no espaço cibernético e o gerenciamento dos *hardwares*, há uma dimensionalidade muito grande, e possibilidade que um indivíduo atue em determinado território com um servidor ou programa de origem distinta; trata-se de camada que exerce funções tanto de nível estrutural quanto operacional. É no *hardware* onde se encontra a estrutura física – computadores, roteadores, placas, cabos, etc. – e, logo, onde se assume a camada mais tangível.

Logicamente, a camada *hardware* que muito dirá sobre o papel de um Estado em conflitos armados e a sua responsabilidade diante de ações orquestradas a partir de seu território, mas, reiterando-se que a utilização do espaço cibernético depende da integralidade das três camadas, é que o estudo aprofundado de casos concretos pode levar a uma efetiva responsabilização no plano internacional quando do tema de violações do DIH por operações

cibernéticas. Sobre isso, o CICV tem realizado interpretações à luz do direito internacional consuetudinário[240] para explicar situações onde um Estado pode ser responsabilizado.

> Conforme o direito internacional, um Estado é responsável por condutas que lhe sejam imputáveis, incluindo possíveis violações do DIH. Isso engloba:
> - Condutas dos órgãos do Estado, incluindo suas forças armadas ou serviços de inteligência;
> - Condutas por pessoas ou entidades, como empresas privadas, onde o Estado possui poderes para exercer autoridade governamental;
> - Condutas de pessoas ou grupos, como milícias ou grupo de *hackers*, agindo de fato sob instruções do Estado, ou sob sua direção ou controle; e
> - Condutas de particulares ou grupos que o Estado reconhece e adota como sua própria conduta. (CICV, 2019, p. 9, tradução nossa[241]).

Em outras palavras, vigora a responsabilização internacional do Estado pelas condutas a ele atribuíveis, nada obstante o meio por onde a violação se deu – cinético ou cibernético (CICV, 2019, p. 9; GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 309-310). A afirmação feita pelo CICV a fim de tornar clara a aplicabilidade do DIH mediante o reconhecimento de um Estado como parte no conflito sinaliza a obrigatoriedade de devida diligência que cada governo possui na salvaguarda das diretrizes humanitárias.

A obrigação de "*due diligence*", ou devida diligência dos Estados, foi reconhecida pela CIJ no caso *Corfu Channel*[242], e trata do dever dos Estados de controlar as atividades que acontecem em seus territórios, de modo a assumir a responsabilidade sobre atos contrários aos direitos de outros Estados que porventura ocorram em sua dimensão espacial e soberana. O Manual de Tallinn 2.0 acata a regra à seara das operações cibernéticas e desafios humanitários, enxergando o mecanismo também como estratégia de governança e padrão de conduta a ser seguido pelos Estados quanto ao uso do espaço cibernético:

---

[240] A partir de estudos do DIH costumeiro propagados pelo CICV, especificamente, a Regra 149 sobre Responsabilidade por Violações do Direito Internacional Humanitário (HENCKAERTS; BECK, 2005, p. 530). E também pelos Artigos (em particular, 4 a 11) sobre a Responsabilidade dos Estados por Atos Internacionalmente Ilícitos da Comissão de Direito Internacional das Nações Unidas. (CICV, 2019, p. 9). Cabe observar que o Manual de Tallinn 2.0 também propôs diretrizes para atribuição de operação cibernética a um Estado, quais sejam as Regras 15 e 16 (SCHMITT, 2017, p. 87-94).

[241] Under international law, a State is responsible for conduct attributable to it, including possible violations of IHL. This includes:
- Conduct by State organs, including its armed forces or intelligence services;
- Conduct by persons or entities, such as private companies, the State empowered to exercise elements of governmental authority;
- Conduct by persons or groups, such as militias or group of hackers, acting in fact on the State's instructions, or under its direction or control; and
- Conduct by private persons or groups which the State acknowledges and adopts as its own conduct. (CICV, 2019, p. 9).

[242] *Corfu Channel case* (*United Kingdom versus Albania*), em julgamento realizado em 9 de abril de 1949, pela CIJ; paradigmático para a responsabilidade internacional dos Estados (DROEGE, 2012, p. 543).

> Regra 6 – Devida diligência (princípio geral)
>
> O Estado deve exercer a devida diligência para não permitir que seu território, ou um território ou infraestrutura cibernética sob seu controle governamental, seja usada para operações cibernéticas que afetem os direitos de outros Estados e produzam sérias consequências adversas.
> [...]
>
> Regra 7 – Cumprimento do princípio da devida diligência
>
> O princípio da devida diligência exige que o Estado tome todas as medidas viáveis para pôr fim a operações cibernéticas que afetem o direito de outros Estados e produzam sérias consequências adversas.
> (SCHMITT, 2017, p. 30, 43, tradução nossa[243]).

Trata-se de princípio geral de direito internacional que, sob a ótica dos especialistas de Tallinn e consoante declarações de Estados como Estônia, Finlândia, França, Holanda, Brasil[244], dentre outros, não deve ter a aplicabilidade excluída no contexto cibernético (SCHMITT, 2017, p. 30-31; 2021b, p. 758-759). De toda sorte, apesar da *due diligence* estatal ser de alcance limitado[245] (DROEGE, 2012, p. 543-544; SCHMITT, 2017, p. 38-43; 2021a, p. 671-672), maiormente em razão das imprecisões que enfrenta para se enquadrar às atividades e interesses em matéria cibernética dos governos, há que se reconhecer que a ideia de uma obrigação de vigilância ou de prevenção entre Estados pode ajudar a evitar que operações cibernéticas "que produzam sérias consequências adversas" sejam estimuladas ou de alguma forma facilitadas pelos Estados.

O próprio princípio pode ser utilizado para atenuar o problema de atribuição da conduta a um Estado, as dissimulações e os questionamentos sobre uma responsabilização tão somente

---

[243] Rule 6 – Due diligence (general principle)
A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.
[…]
Rule 7 – Compliance with the due diligence principle
The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States. (SCHMITT, 2017, p. 30, 43).

[244] É o que se vê, especificamente, a partir dos comentários enviados pelo Brasil ao "*pre-draft*" inicial do relatório do OEWG sobre os desenvolvimentos no campo da informação e telecomunicações no contexto de segurança internacional, em abril de 2020.

[245] Os especialistas de Tallinn oferecem discussões sobre até que ponto a devida diligência pode ser empregada pelos Estados, vez que corresponde a uma obrigação legal que é violada por omissão e que pode defrontar uma série de empecilhos factuais (SCHMITT, 2017, p. 36-43). Ademais, Cordula Droege (2012, p. 544-545) questiona a possibilidade de atribuição estatal e, por correlação, a devida diligência, quando não for possível afirmar assertivamente que há controle governamental ou possibilidade clara de responsabilização nos termos dos Artigos sobre Responsabilidade dos Estados por Atos Internacionalmente Ilícitos da Comissão de Direito Internacional das Nações Unidas.

presuntiva[246]: no caso de um ataque cibernético cuja autoria não possa ser atribuível de modo confiável, mas que pode ser geolocalizado, o Estado de onde consta a condução da operação poderia ser obrigado a encerrá-la (SCHMITT, 2021a, p. 673). Nesse contexto, mesmo que ainda em desenvolvimento e requerendo maiores delineamentos, o princípio da *due diligence* estatal para o ciberespaço tal qual ostentado pelo Manual de Tallinn 2.0 proporciona um espírito de cautela e moderação entre os Estados – não apenas, mas também no que tange ao DIH.

3.3 As Políticas Públicas Internacionais

Há que se reconhecer, após a análise do fenômeno guerra cibernética e os estudos que vão desde o incremento das capacidades ofensivas dos Estados até os impasses ao DIH, que as mudanças na tecnologia global estão em ascensão e que não necessariamente são maléficas ou implicam em retrocesso humanitário. Pelo contrário, o aprimoramento das capacidades cibernéticas defensivas e ofensivas dos Estados, associado aos princípios existentes do *jus in bello* e à devida diligência estatal, pode proporcionar que as operações militares sejam mais assertivas e acarretem em menos danos civis[247].

Fato é que as regras e mecanismos existentes precisam ser aplicados sob uma nova perspectiva, e que os princípios humanitários devem ser repensados. O fenômeno guerra cibernética carece de melhor compreensão, e requer discussões sobre como atualizar os pormenores do DIH a uma seara ainda tão abstrata. Em artigo intitulado "*Twenty Years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*" publicado em 2020 pela *International Review of the Red Cross*, os especialistas vinculados ao CICV Laurent Gisel, Tilman Rodenhäuser e Knut Dörmann ressaltam que a temática está na agenda global há pouco mais de duas décadas[248], e ainda há muito a ser esclarecido.

Nesse período, alguns Estados e organizações internacionais dedicaram e continuam a dedicar esforços consideráveis para elaborar e implementar medidas preventivas que visem

[246] Como aborda Cordula Droege (2012, p. 543), ao problematizar a atribuição de condutas a um Estado com base em presunções sobre a origem dos atos no ciberespaço.
[247] Em posição similar, também Lesley Swanson (2010, p. 326): "Cyber warfare, if properly limited, may allow militaries to act on an expanded list of targets while also avoiding the loss of civilian lives. In other words, cyber warfare could play an important niche role, by supplementing or amplifying more traditional forms of warfare".
[248] "Legally, discussions on whether and how international humanitarian law applies to, and restricts, cyber operations during armed conflicts began over two decades ago". Referindo-se aos trabalhos iniciais sobre operações militares no campo informacional pelo Departamento de Defesa dos EUA, em 1999, e aos primeiros exames acadêmicos sobre questões do DIH e ciberespaço, no mesmo período (GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 291).

assegurar um melhor cumprimento[249] do DIH em casos de operações militares no ciberespaço; é o que se vê sobretudo pelos diversos seminários de especialistas organizados pelo CICV e pelas posições sobre como o DIH seria aplicado às operações cibernéticas publicadas por alguns Estados. Inclusive, a partir das discussões entre especialistas de diferentes nacionalidades fomentadas pelo CICV é que adveio o reconhecimento de uma obrigação positiva dos Estados, ainda que não envolvidos em um conflito armado, de tomar medidas contra os Estados violadores do DIH, usando suas influências para impedir as violações – debate reproduzido no Manual de Tallinn, pelo princípio geral de *due diligence* (SWANSON, 2010, p. 325; GISEL; RODENHÄUSER; DÖRMANN, 2020, p. 289; SCHMITT, 2017, p. 30-50).

Dentre as mais diversas discussões sobre a matéria, surgem argumentos favoráveis a criação de um novo acordo ou tratado internacional para lidar especificamente com situações de guerra cibernética, partindo desde o ideal de busca de consenso multilateral sobre a interpretação do regramento já existente ao ciberespaço, até o raciocínio de que as noções ocidentais tradicionais de guerra descritas pelo DIH estão defasadas e que novas leis internacionais são imprescindíveis para que exista uma cobertura das situações que ocorram no novo espaço. Da mesma forma, há argumentos desfavoráveis à feitura de tratado internacional[250], sob justificativas de que tais "não ofereceriam nenhuma alternativa real para desenvolver e continuar o diálogo entre as nações e provavelmente complicariam as questões em jogo[251]" e que, para lidar com situações iminentes, mais valeria o constante diálogo aberto entre organizações internacionais e Estados e o estímulo à transparência em suas políticas. (EILSTRUP-SANGIOVANNI, 2017; SWANSON, 2010, p. 325-326, tradução nossa).

De toda sorte, assim como asseverou o CICV em declaração proferida em debate aberto[252] do CSNU em junho de 2021, apesar de novos estudos e do estímulo a acordos sobre como o direito internacional limita as operações cibernéticas durante conflitos armados serem importantes, as regras balizadoras do DIH só terão efetividade mediante implementação em nível nacional (CICV, 2021c). Para tanto, foram sintetizados[253] alguns pontos importantes sobre como os Estados podem e devem garantir a proteção humanitária:

---

[249] De onde infere-se, também, o *compliance* estatal reiterado pelo Manual de Tallinn; e não só como *due diligence* em relação à soberania de outros Estados, mas também como matéria contígua de direitos humanos.

[250] Uma possível percepção é a de que os Estados devem desenvolver novas normas a partir dos costumes ou da codificação pela prática reiterada (SWANSON, 2010, p. 326).

[251] International treaties, however, would not offer any real alternative to developing and continuing the dialogue among nations, and would likely complicate the issues at stake. (SWANSON, 2010, p. 326).

[252] Debate sobre a manutenção da paz e segurança internacionais no ciberespaço: "United Nations Security Council Open Debate on Cyber Security, maintaining international peace and security in cyberspace".

[253] Em outros documentos estimulados pelo organismo, especialistas tem debatido o desenvolvimento de tais medidas (CICV, 2021c).

> Primeiro, cada Estado é responsável por todos os seus órgãos envolvidos em operações cibernéticas e por outros atores que atuam sob suas instruções, direção ou controle. Os Estados devem garantir que todos esses atores respeitem o Direito Internacional Humanitário.
> Segundo, os Estados devem desenvolver processos internos claros para garantir que, se meios ou métodos de guerra cibernéticos forem usados, eles cumpram com a estrutura legal aplicável.
> Terceiro, os Estados têm a obrigação de tomar todas as precauções possíveis para evitar ou pelo menos minimizar os danos civis acidentais ao realizar ataques, inclusive aqueles que se deem por meios e métodos de guerra cibernética. No ambiente das TIC, isso pode incluir a adoção de medidas técnicas como '*system-fencing*', '*geo-fencing*' ou '*kill switches*'[254].
> Quarto, os Estados também têm a obrigação de implementar medidas para proteger a população civil contra os perigos resultantes de operações militares cibernéticas. Algumas dessas medidas podem ser implementadas já em tempos de paz. (CICV, 2021c, tradução nossa[255])

Nota-se que, ao levantar a necessidade de diálogo entre Estados e a adoção de medidas para prevenir e mitigar danos humanos por guerras cibernéticas, em outras palavras, o CICV tem manifestado a importância de políticas públicas internacionais sobre a temática. Por "políticas públicas internacionais", acolhe-se o conceito de intersecção entre políticas públicas e as relações internacionais oferecido por Franck Petiteville e Andy Smith (2006, p. 362-363, tradução nossa[256]) como "conjunto de programas de ação reivindicados por autoridades públicas com o objetivo de produzir efeitos para além do âmbito de um território nacional-estatal", onde se incluem o que seriam as políticas externas – sob uma autoridade pública central, Estados ou organizações relativamente integradas, como a UE –, e também as políticas multilaterais – aquelas fomentadas ou produzidas no âmbito de organizações internacionais.

---

[254] O próprio CICV explica: *system-fencing* importa medida técnica para impedir que o *malware* se execute se não houver correspondência precisa com o sistema a que se destina; *geo-fencing*, por sua vez, medida para limitar o *malware*, para que ele opere apenas em IP específico; e *kill switches*, prática para desabilitar o *malware* após determinado tempo ou mesmo quando ativado de forma remota. (CICV, 2021c).

[255] First, each State is responsible for all its organs involved in cyber operations and other actors that act on that State's instructions, or under its direction or control. States must ensure that all of these actors respect international humanitarian law.
Second, States should develop clear internal processes to ensure that if cyber means or methods of warfare are used, they comply with the applicable legal framework.
Third, States have an obligation to take all feasible precautions to avoid or at least minimize incidental civilian harm when carrying out attacks, including through cyber means and methods of warfare. In the ICT environment, this may include implementing technical measures such as 'system-fencing', 'geo-fencing', or 'kill switches'.
Four, States also have an obligation to put in place measures to protect the civilian population against the dangers resulting from military cyber operations. Some of these measures may have to be implemented already in peacetime. (CICV, 2021c).

[256] Si l'on entend par « politiques publiques internationales » l'ensemble des programmes d'action revendiqués par des autorités publiques ayant pour objet de produire des effets dépassant le cadre d'un territoire stato-national, on peut distinguer deux types de politiques publiques internationales : les « politiques étrangères » d'une part, relevant d'une autorité publique centrale (les États, mais aussi, par extension, une organisation relativement intégrée comme l'Union européenne aujourd'hui), et, d'autre part, les politiques publiques multilatérales produites par (ou dans le cadre) d'organisations internationales (PETITEVILLE; SMITH, 2066, p. 362-363).

Observando o ciclo de políticas públicas[257], entre identificação do problema, formação de agenda, formulação de alternativas, tomada de decisão, implementação, monitoramento e posterior avaliação (SECCHI, 2012, p. 33-34), a temática das guerras cibernéticas e preocupação humanitária encontra-se, traçando uma adaptação ao nível internacional, entre as fases iniciais e intermediárias de identificação do problema, composição de agenda e elaboração e análise de alternativas – com vistas a uma tomada de decisão. O grau de amadurecimento e aprimoramento da matéria pelas nações, enquanto dependente de interesse, aprofundamento e aplicação no âmbito nacional de cada Estado, é variável, e frequentemente ligado ao seu nível de desenvolvimento econômico e militar.

Nessa compreensão, para além do estímulo a cooperação internacional entre Estados mediante políticas externas deles em relação a outros, enfatiza-se o papel que organizações internacionais ou instituições multilaterais têm exercido para facilitar e/ou desenvolver projetos e ações sobre a utilização do ciberespaço. Percebe-se o peso que a globalização tem exercido no desenvolvimento de políticas públicas, aumentando a interdependência entre os Estados e suscitando respostas coletivas e cooperativas deles; trata-se da "multilateralização da ação pública", que revela a busca pela governança da globalização, por uma leitura comum dos fenômenos globais, pela adoção de padrões regulatórios ou mesmo pela instauração de processos inibitórios perante os Estados (PETITEVILLE; SMITH, 2006, p. 363-364). A abordagem multicêntrica[258] – para além da deliberação unicamente por atores estatais – do que seriam as políticas públicas obedece aos caminhos que a globalização tem percorrido, e exibe o potencial que diversos atores têm de examinar os pormenores e viabilizar estratégias de implementação (SECCHI, 2012, p. 3).

Constata-se a aplicabilidade desse ensejo à governança e à adoção de políticas públicas internacionais também na área cibernética, onde se verifica o frequente impulso à busca de

---

[257] A fase inicial, de identificação do problema, consiste na "discrepância entre o *status quo* e uma situação ideal possível" e, uma vez identificado por algum ator político com interesse na resolução desse problema, este poderá lutar para que tal entre em uma lista de prioridades de atuação – a agenda. A formação da agenda traz o "conjunto de problemas ou temas entendidos como relevantes", aqueles temas reconhecidos como merecedores de intervenção pública. A fase de formulação de alternativas é alcançada quando, da introdução do problema na agenda, são realizados esforços para a construção e busca de soluções para os problemas; passa-se ao estabelecimento de objetivos e estratégias, ao estudo acerca de cada alternativa de solução e suas consequências. Em seguida, a tomada de decisão caracteriza "o momento em que os interesses dos atores são equacionados e as intenções (objetivos e métodos) de enfrentamento de um problema público são explicitadas". Então, há as fases de implementação, avaliação, e até mesmo de extinção da política pública. (SECCHI, 2012, p. 34-54).

[258] Segundo Leonardo Secchi (2012, p. 3), "[...] essa abordagem adota um enfoque mais interpretativo e, por consequência, menos positivista, do que seja uma política pública. A interpretação do que seja um problema público e do que seja a intenção de enfrentar um problema público aflora nos atores políticos envolvidos com o tema (os *policymakers*, os *policytakers*, os analistas de políticas públicas, a mídia, os cidadãos em geral)"; a abordagem multicêntrica de políticas públicas evita uma pré-análise de personalidade jurídica de uma organização antes de enquadrar as suas políticas como sendo públicas, além de considerar um espectro amplo de fenômenos.

respostas aos problemas relevantes para a coletividade por atores internacionais. Logo, de modo particular, cumpre observar o incentivo à produção de normas de conduta coletiva e à interpretação do DIH tradicional ao novo meio e método de guerra. Considera-se a missão e responsabilidade que determinadas entidades internacionais assumem de influenciar ou interferir diretamente na resolução de temas sociais internos aos Estados com vistas a enfrentar questões da agenda global, como a paz e segurança. Por isso, parte-se a um breve acompanhamento das atividades do CICV, da ONU, da OEA, da UE, e da OTAN como principais entidades que laboram o direito internacional e que mais têm se manifestado em prol de políticas públicas – o tratamento e resolução para problemas coletivamente relevantes[259] – sobre o uso de operações cibernéticas.

3.3.1 O Comitê Internacional da Cruz Vermelha

O CICV faz parte do Movimento da Cruz Vermelha e do Crescente Vermelho, tem status jurídico internacional *sui generis*, e é entidade neutra e independente que há bastante tempo assume o desenvolvimento do DIH, inclusive monitorando o cumprimento e levando à celebração de tratados internacionais de natureza humanitária. Apesar de não se qualificável como organização intergovernamental, e de não possuir um elemento de criação internacional (SASSÒLI, 2019, p. 212-213; THÜRER, 2011, p. 296-298), é notória a sua atuação na sociedade internacional, em consonância com os direitos humanos e em prol da maior aplicabilidade da salvaguarda dos vulneráveis em guerra.

Assim, há que reconhecer o CICV e o papel que tem desempenhado de modo complementar ao que expõe a definição de Franck Petiteville e Andy Smith (2006, p. 362-363) para políticas públicas internacionais como abarcando àquelas suscitadas por organizações internacionais. A entidade, mesmo com natureza jurídica distinta, é o principal palco de discussões e pesquisas sobre a compreensão e implementação do DIH, e visa o desenvolvimento do ramo para que atinja não só acadêmicos e estudantes, pessoal militar e humanitário, mas também os formuladores de políticas públicas.

[259] A partir da abordagem multicêntrica de políticas públicas, a que se filia Leonardo Secchi (2012, p. 2-3), não limitada de elaboração por atores estatais, e composta pelos dois elementos fundamentais de intencionalidade pública e resposta a um problema público.

Sobre o uso de operações cibernéticas em conflitos armados, há décadas[260] a Cruz Vermelha já tem levantado preocupações e atentado sobre o potencial de resultados inconclusivos dos Estados na aplicabilidade do DIH. Na atualidade, a entidade corriqueiramente tem oportunizado debates sobre como adaptar e quais os desafios de implementação das regras humanitárias no ciberespaço; seja por meio de seu periódico acadêmico, lido por autoridades governamentais, OI's, profissionais humanitários, acadêmicos, etc., ou por publicações diversas nos seus meios de comunicação. Ademais, o CICV tem exercido seu mandato e missão ao difundir suas conclusões sobre o uso de operações cibernéticas em pareceres ou mesmo ao prestar declarações em debates multilaterais sobre o assunto.

De modo particular, em adição às diversas publicações e documentos da CICV retromencionados nessa pesquisa, aqui cabe citar declarações mais recentes proferidas em nome da entidade, exibindo sua contribuição para formação da agenda e formulação de alternativas para a construção de políticas públicas. Durante sessão do segundo mandato do OEWG das Nações Unidas sobre os desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional, em 15 de dezembro de 2021:

> [...] Em nossa opinião, desenvolver entendimentos comuns sobre como e quando o Direito Internacional Humanitário se aplica a operações cibernéticas durante conflitos armados, e partilhar práticas sobre como operacionalizar esses limites legais, é essencial para proteger a população civil.
> Além disso, entender os limites que outros Estados respeitam em suas operações cibernéticas pode ser uma importante medida de construção de confiança.
> [...] o CICV reconhece que há outras questões que precisam ser mais estudadas. Embora as regras existentes do DIH sejam a pedra angular da proteção de civis, da infraestrutura e das sociedades contra riscos digitais, é necessário esclarecer, por exemplo, como a noção de bens civis deve ser entendida em um mundo digitalizado.
> [...] O CICV pretende contribuir para este OEWG com conhecimentos técnicos e jurídicos em questões relacionadas ao uso de operações cibernéticas durante conflitos armados, e também estamos disponíveis para discutir bilateralmente com delegações interessadas ou grupos regionais. (CICV, 2021a, tradução nossa[261]).

---

[260] Como se verifica até mesmo pela perspectiva de desenvolvimento do DIH a partir de publicações da *International Review of the Red Cross*, onde pelo menos desde os anos 2000 é possível encontrar pesquisas sobre o que à época era denominado apenas como "guerra da informação" (CHURCH, 2000).

[261] [...] In our view, developing common understandings of how and when international humanitarian law applies to cyber operations during armed conflicts, and exchanging practice of how to operationalize these legal limits, is essential to protect the civilian population.
Moreover, understanding the limits that other States respect in their cyber operations can be an important confidence-building measure.
[...] the ICRC recognizes that there are other issues that need further study. While existing rules of IHL are the cornerstone of the protection of civilians, infrastructure, and societies against digital risks, clarification is needed, for instance, on how the notion of civilian objects is to be understood in a digitalized world.
[...] The ICRC is aiming to contribute to this OEWG with both technical and legal expertise on questions relating to the use of cyber operations during armed conflict, and we are also available to discuss bilaterally with interested delegations or regional groups. (CICV, 2021a).

E em depoimento ao CSNU, em 20 de dezembro de 2021, onde foram abordados quatro[262] pontos de relevância sobre o uso de operações cibernéticas durante conflitos armados; o último deles, em especial, enfatiza a busca por implementação do DIH nas forças armadas e a responsabilidade assumida pelos Estados:

> [...] Precisamos de medidas concretas para proteger os civis em tempos de conflito armado – aproveitando os processos existentes e desenvolvendo novas medidas quando necessário.
> Os militares geralmente descrevem as capacidades cibernéticas como uma 'ferramenta' adicional à sua disposição. Eles raramente, ou nunca, questionam que as capacidades de TIC estão sujeitas às mesmas regras que qualquer outro meio ou método de guerra. Os líderes militares e civis são responsáveis por garantir o respeito ao Direito Internacional Humanitário, que se aplica apenas em situações de conflito armado.
> Nossa pesquisa e experiência mostram que a implementação do DIH e a proteção de civis requerem processos claros. Por exemplo,
> - As forças armadas precisam de instruções sobre os limites legais das operações cibernéticas em seus manuais ou regulamentos;
> - As forças armadas precisam de processos específicos de delimitação de alvos cibernéticos, que devem se basear na experiência dos Estados adquirida em operações cinéticas;
> - Os Estados precisam revisar a legalidade das capacidades cibernéticas que desenvolvem ou adquirem para garantir que possam ser usadas em conformidade com as regras existentes de direito internacional.
> Além disso, os riscos específicos apresentados pelas operações cibernéticas também exigem medidas cibernéticas específicas para evitar ou minimizar os danos civis. Isso pode incluir um reconhecimento cuidadoso para evitar danos a redes ou infraestruturas civis, comando e controle sobre recursos cibernéticos, e medidas técnicas para evitar que o *malware* se espalhe fora de controle. (CICV, 2021b, tradução nossa[263]).

---

[262] São eles: o risco de que as tecnologias cibernéticas se tornem um catalisador de conflitos, crises humanitárias e sofrimento; a ameaça real, e à nível global, que as operações cibernéticas representam para os civis; a imposição de limites do DIH ao uso de quaisquer meios e métodos de guerra, inclusive as capacidades de TIC; e, então, a necessidade de medidas concretas para a proteção de civis quando em situação de conflito armado (CICV, 2021b).

[263] […] We need concrete steps to protect civilians in times of armed conflict – by building on existing processes and developing new measures where needed.
Militaries often describe cyber capabilities as an additional 'tool' at their disposal. They rarely, if ever, question that ICT capabilities are subject to the same rules as any other means or method of warfare. Military and civilian leaders are responsible for ensuring respect for international humanitarian law, which applies only in situations of armed conflict.
Our research and experience show that implementing IHL, and protecting civilians, requires clear processes. For example,
- Armed forces need instructions on the legal limits of cyber operations in their manuals or regulations;
- Armed forces need cyber-specific targeting processes, which should build on the experience of States gained in kinetic operations;
- States need to review the legality of cyber capabilities they develop or acquire to ensure that they can be used in compliance with existing rules of international law.
Moreover, the particular risks posed by cyber operations also require cyber-specific measures to avoid or minimize civilian harm. This can include careful reconnaissance to avoid harming civilian networks or infrastructure, command and control over cyber capabilities, and technical measures to avoid malware spreading out of control (CICV, 2021b).

Em declaração posterior, de abril de 2022, o CICV reiterou a aplicabilidade de princípios e regras internacionais estabelecidas para limitar também a condução de operações cibernéticas, e endossou a relevância de fóruns internacionais para a troca e discussão entre Estados sobre "como" e "quando" o DIH se aplica diante das TIC. A partir dessas reuniões, o CICV constatou progressos sobre a tratativa do tema pelos Estados, com publicações de opiniões nacionais sobre como o direito internacional abarca o ambiente da informação. Tais publicações são de extrema importância e fornecem uma fonte única e oficial para que outros Estados as consultem e as considerem ao formar suas próprias opiniões sobre o assunto – o CICV não só apoia esse trabalho dos Estados, como é uma das entidades de amparo ao *Cyber Law Toolkit*, projeto cuja plataforma informa as visões nacionais já apresentadas, e que fornece a reunião de todas as posições existentes até então sobre um determinado assunto[264] (CICV, 2022).

É evidente o interesse do CICV para que os Estados, por meio de seus representantes, regulamentos e documentos publicados, manifestem, na medida do possível, a interpretação e a aplicação das regras humanitárias existentes à realidade cibernética. Assim, é salutar o empenho da entidade em manter o problema das operações cibernéticas durante conflitos armados em ênfase na agenda internacional, inclusive oferecendo apoio jurídico e técnico para que os Estados e grupos multilaterais interessados compreendam as principais questões atinentes ao tema, conheçam as possíveis consequências, alcancem um consenso e tracem objetivos em prol da proteção das potenciais vítimas, com estratégias ou ações tangíveis.

3.3.2 As Nações Unidas (GGE e OEWG)

Não obstante outros[265] fóruns relacionados terem sido realizados no escopo da ONU, delimitando-se à seara humanitária e às conotações mais recentes atreladas ao conteúdo e finalidade desta pesquisa, é dada especial atenção aos *Group of Governmental Experts* (GGE) e *Open-Ended Working Group* (OEWG) sobre segurança internacional e uso do ciberespaço. Isso porque as discussões multilaterais atinentes a problemas relacionados à "segurança da informação" foram introduzidas quando a Federação Russa apresentou o que seria uma primeira

[264] A exemplo das discussões sobre dados como objeto, vide Quadro 1 constante nesta pesquisa.
[265] Como a partir do Instituto das Nações Unidas para a Pesquisa sobre Desarmamento (UNIDIR), que promove pesquisas em prol da busca de soluções para problemas ou ameaças emergentes; ou pela União Internacional de Telecomunicações (UIT), agência da ONU responsável por tecnologias da informação e comunicação com vistas ao desenvolvimento de normas técnicas de promoção segura do acesso à tecnologia do ciberespaço (BARROS, 2015, p. 151-152).

tratativa[266] sobre o tema à AGNU, em 1998. Logo após, a análise sobre as ameaças e riscos do uso de tecnologias em desfavor da segurança internacional passou por breve fase de inércia dos Estados sob o ponto de vista jurídico, possivelmente pela descrença e distanciamento factual atribuído pela maioria à época. Contudo, em 2003, a AGNU encarregou o Secretário-Geral de reunir especialistas governamentais para tratar sobre ameaças cibernéticas e avaliar medidas cooperativas para combatê-las, retornando aos propósitos descritos na resolução de 1998. (SCHMITT, 2021a, p. 662).

Desde então, as discussões se intensificaram e resultaram em seis[267] reuniões consecutivas de especialistas governamentais para examinar o impacto do desenvolvimento da TIC na segurança internacional e assuntos militares, entre 2004 e 2021. *O United Nations Group of Governmental Experts* (GGE) *on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, inicialmente, *GGE on Developments in the Field of Information and Telecommunications in the Context of International Security*, é composto por 25 Estados, entre os quais constam os cinco membros permanentes do CSNU, e os demais são alocados conforme distribuição geográfica equitativa e manifestação de interesse (DIPLO, 2022a; ONU, 2022a).

Os peritos governamentais indicados pelos Estados, guiados por um presidente selecionado entre os membros a cada reunião e mediante mandato incluído em resolução da AGNU, resolvem sobre a temática comentando rascunhos e respondendo consultas informais entre as sessões, até que se apresente um relatório final com suas conclusões e recomendações à AGNU (ONU, 2022a). Nem todos GGEs realizados findaram seus trabalhos adotando um relatório de consenso ou apresentando respostas substantivas aos problemas relativos às ciberguerras, mas há que se reconhecer que o projeto das reuniões tem suscitado que os Estados reflitam sobre normas, regras e princípios para o comportamento responsável dos Estados, medidas de construção de confiança, de cooperação internacional e capacitação tecnológica, e principalmente sobre como o direito internacional se aplica ao ciberespaço (SCHMITT, 2021a, p. 662-663; DIPLO, 2022a).

O terceiro mandato do GGE (2012/2013), baseado nos trabalhos anteriores e buscando progressos, foi o primeiro a abordar o direito internacional. Em seu relatório final, reconheceu

---

[266] *Draft resolution* apresentada ao Primeiro Comitê da AGNU, responsável pela agenda sobre desarmamento e segurança internacional. A resolução foi adotada sem votação como UN General Assembly A/RES/53/70 (SCHMITT, 2021a, p. 662).

[267] Os seis GGEs convocados: em 2004/2005, vide UN General Assembly A/RES/58/32; em 2009/2010, A/RES/60/45; em 2012/2013, A/RES/66/24; em 2014/2015, A/RES/68/243; em 2016/2017, A/RES/70/237; e em 2019/2021, vide A/RES/73/266. Apenas quatro dos GGEs concluíram seus trabalhos adotando relatório de consenso – aqueles findados em 2010, 2013, 2015 e 2021. (DIPLO, 2022).

por consenso que o direito internacional – em particular, a Carta da ONU – se aplica ao ciberespaço, sobrelevou a aplicabilidade da soberania dos Estados e as normas e princípios decorrentes, bem como o respeito aos DHI, e asseverou a responsabilidade dos Estados pelos atos internacionalmente ilícitos atribuíveis a eles também no contexto cibernético – em outras palavras, a *due diligence* estatal no campo cibernético (ONU, 2013; SCHMITT, 2021a, p. 663-664).

Apesar dos significativos avanços até então, foi o GGE 2014/2015 que, em seu relatório final (Res. AGNU A/70/174), introduziu normas voluntárias para o comportamento responsável dos Estados no ciberespaço, e que considerou especificamente o DIH – sem, contudo, citá-lo – ao observar "os princípios internacionais estabelecidos, incluindo, quando aplicável, os princípios da humanidade, necessidade, proporcionalidade e distinção" (ONU, 2015, p. 13, tradução nossa[268]). Os pontos levantados no relatório anterior foram reiterados com algum aprofundamento, como pela declaração de aplicabilidade do que seriam os princípios do DIH e também pela afirmação de que os Estados têm jurisdição e dever de ingerência sobre a infraestrutura cibernética em seu território (ONU, 2015, p. 12).

Diante dos progressos, foi estimulada a continuação dos estudos em novo GGE, voltado à compreensão das ameaças existentes e potenciais do uso das TICs e à busca por possíveis medidas de cooperação para resolvê-las, como a partir de entendimento comuns sobre a aplicabilidade do direito internacional. A necessidade de maior desenvolvimento de conceitos para a paz e segurança internacionais no uso das TICs, nos níveis jurídico, técnico e político foi frisada (ONU, 2015, p. 13) como direcionamento para o próximo mandato. Todavia, o mandato 2016/2017, referente ao quinto GGE, não terminou com um consenso sobre um relatório final. Rússia e China, por exemplo, se opuseram à referência textual à "autodefesa" e ao "direito internacional humanitário[269]" no relatório, dificultando conclusões sobre como operacionalmente o direito internacional seria aplicável ao uso das TICs pelos Estados (SCHMITT, 2021a, p. 664).

Apesar do suposto fracasso do GGE 2016/2017, e, logo, de um consenso sobre a efetiva aplicabilidade das normas de conflitos armados ao ciberespaço, a AGNU aprovou a convocação

[268] [...] notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction (ONU, 2015, p. 13).

[269] Observa-se que, apesar da afirmação no GGE anterior, pela declaração de aplicabilidade dos princípios humanitários, o termo "Direito Internacional Humanitário" não havia sido disposto. Dessarte, considera-se a possibilidade de ter havido uma mudança de posição de alguns Estados, tanto de preceitos do *jus ad bellum* quanto do *jus in bello*, em função das tensões políticas inflamadas por ciberataques – a suposta interferência da Rússia nas eleições presidenciais dos EUA em 2016, o *malware Wannacry*, dentre outros ataques cibernéticos que teriam sido patrocinados por Estados contra infraestruturas na Ucrânia, por exemplo (EFRONY, 2021).

de um novo GGE, desta vez sob novo título[270], enfatizando o comportamento responsável dos Estados pelas atividades empreendidas no espaço cibernético. O GGE 2019/2021 foi concluído com relatório final reconhecendo a aplicabilidade do DIH apenas a situações de conflitos armados, e sustentando o papel dos princípios, como levantado no relatório de 2015. A necessidade de um estudo mais aprofundado sobre como e em quais circunstâncias esses princípios se aplicam ao uso das TICs pelos Estados[271], porém, foi explicitada (ONU, 2021b, p.18).

Em suma, em que pese o desenvolvimento de padrões para o comportamento tido como "responsável" dos Estados no espaço cibernético frente ao aumento de ataques cibernéticos e seus impactos na infraestrutura crítica – inclusive com avanços na recomendação de normas[272] para a redução dos riscos à paz, segurança e estabilidade internacionais –, o sexto GGE ficou aquém das expectativas na abordagem da proteção de vítimas pelo DIH e na busca por propostas concretas de operacionalização das normas humanitárias ao novo contexto. O Grupo reconheceu suas limitações e incentivou o diálogo entre Estados também por organizações regionais e por outros fóruns, bem como a atuação de outras partes interessadas, como a academia e a comunidade técnica, para o compartilhamento contínuo sobre como o direito internacional se aplica, mormente diante de situações específicas. Ademais, o relatório investiu às discussões no OEWG a capacidade de melhor desenvolver e implementar resoluções às diversas questões sobre o uso do ciberespaço (ONU, 2021b, p. 22-23).

O Grupo de Trabalho Aberto (*Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* – OEWG) iniciou a primeira reunião de seu mandato em 2019 e se estendeu até 2021, por certo período correndo de forma paralela ao sexto GGE. Mesmo com mandatos de propostas semelhantes, o OEWG trouxe a possibilidade de participação de todos os Estados-membros da ONU, bem como cedeu maior espaço[273] para opiniões advindas do setor privado, academia e sociedade civil (DIPLO, 2022b). Além de trazer no seu escopo a continuidade dos estudos e discussões dos GGEs anteriores, ao OEWG foi dada a missão de estabelecer um diálogo

[270] *GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*.
[271] "[...] The Group noted that international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognised the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict." (ONU, 2021b, p.18).
[272] Referindo-se ao incremento e aprofundamento das normas voluntárias elencadas no relatório final de 2015.
[273] Pelo mandato do OEWG, são realizadas reuniões consultivas com as partes interessadas, desde empresas, organizações não governamentais, outras entidades e academia (DIPLO, 2022b).

institucional regular com ampla participação sob os auspícios da ONU, função elementar tendo em vista a dinamicidade de atores no espaço cibernético.

O primeiro mandato do OEWG foi concluído em relatório final publicado pouco antes[274] do relatório do sexto GGE, havendo relação de continuidade entre os fóruns e com menção em ambos relatórios da análise de propostas para promoção do comportamento responsável dos Estados frente às TICs e da implementação de um Programa de Ação[275] a partir da continuidade dos trabalhos em um novo OEWG (ONU, 2021a, p. 11). Isso pois já em dezembro de 2020 a AGNU havia previsto a renovação do mandato do OEWG para 2021 até 2025. Por conseguinte, a sessão organizacional do segundo OEWG ocorreu em junho de 2021, e a primeira e segunda sessões substantivas, em dezembro de 2021 e entre março e abril de 2022, respectivamente. Com a terceira sessão de natureza substantiva agendada para o final de julho de 2022, até o momento o fórum ainda tem buscado o consenso em questões organizacionais, como a definição sobre como as partes interessadas poderão participar das sessões, e tem procedido com a discussão de questões substantivas de maneira informal (ONU, 2022b; DIPLO, 2022a; 2022c).

Dentre os trâmites e discussões parciais do OEWG em andamento, nota-se a maioria dos Estados-membros adepta ao reconhecimento dos trabalhos realizados até o momento – fruto das negociações e acordos realizados, onde se incluem os relatórios finais dos GGEs e do primeiro OEWG – e favorável ao próximo passo, de implementação das normas existentes. Para tal implementação, considerações sobre a obrigação de *due diligence*, medidas de proteção da infraestrutura crítica e de determinação de atribuição do ato ilícito têm sido aprofundadas. Há, pela maioria dos Estados, o ensejo pela assimilação sobre como exatamente o direito internacional – de modo especial, o DIH e os DHIs – se aplica às atividades estatais no espaço cibernético. Em contrapartida, alguns Estados asseveram pela carência de norma vinculante própria às especificidades, e pedem a elaboração de um instrumento original, internacional e juridicamente vinculante para regular o comportamento dos Estados no ciberespaço. (DIPLO, 2022b; 2022c; ONU, 2022b).

[274] O relatório final do OEWG 2019/2021 foi publicado em março de 2021; o relatório do GGE 2019/2021, por sua vez, foi oficialmente publicado em julho de 2021, embora uma versão preliminar tenha sido divulgada já em maio de 2021.

[275] Este Programa de Ação (Programme of Action – PoA) visaria promover o comportamento responsável do Estado no ciberespaço, e funcionaria como um fórum permanente da ONU voltado ao uso das TICs pelos Estados. Em sua estrutura organizacional, teria reuniões anuais e monitoramento frequente; o PoA intensificaria a cooperação e a capacitação dos Estados sobre as TICs, bem como realizaria consultas com outras partes interessadas. (DIPLO, 2022b).

Ainda há muito que ser debatido e esmiuçado nos fóruns da ONU, e o incentivo à continuidade desses, com a maior participação de atores, poderá render bons frutos. A questão que ecoa na busca de consenso de tais fóruns é a protelação na resposta aos impasses jurídicos que cada vez mais têm se alargado em atividades no ciberespaço. Determinar em que medida e em quais circunstâncias recaem os princípios do DIH a partir de operações cibernéticas, como deve ser aferida a atribuição de autoria, e como a *due diligence* deve ser vislumbrada[276], a exemplo, são pontos-chave para a continuidade dos trabalhos sobre a operacionalidade do direito internacional (em particular, do *jus in bello*). De todo modo, os esforços e continuidade dos fóruns pela AGNU revelam o engajamento dos Estados e demais atores internacionais em dialogar e acrescentar suas posições de forma mais transparente. Ainda que os frutos não sejam imediatos, é sabido que o diálogo é a força motriz do direito internacional, e é ele que gera "construções" – sejam elas consuetudinárias ou até mesmo convencionais – para o futuro.

3.3.3 A OEA

A Organização dos Estados Americanos tem abordado temas relativos à segurança cibernética desde 1999, ao estabelecer um grupo de trabalho sobre crimes cibernéticos. Almejando reforçar a agenda de segurança cibernética nas Américas, a OEA atualmente possui um Programa de Segurança Cibernética que promove a cooperação entre instituições públicas e privadas, e que objetiva o desenvolvimento de capacidades de segurança cibernética e de políticas públicas para um ciberespaço seguro (BARROS, 2015, p. 156; OEA, 2022b).

A maior preocupação com o uso de operações cibernéticas pelo Estado e sua acepção relativa à guerra cibernética, contudo, é relativamente recente. De modo particular, é a partir da atuação da Comissão Jurídica Interamericana (CJI), um dos órgãos principais da OEA, que o tema tem sido enfatizado. A CJI atua como órgão consultivo em assuntos jurídicos e, em sua função de desenvolver o direito internacional e de analisar os problemas jurídicos atinentes ao progresso do hemisfério, tem inserido a aplicabilidade do direito internacional ao ciberespaço como tópico da sua agenda[277] (OEA, 2022a).

---

[276] Nesse quesito, também Dan Efrony (2021): "Ultimately, if the question of how basic rules and principles of international law, such as the rules of attribution, sovereignty and due diligence, apply in cyberspace is still politically and legally unresolved, then broadly-formulated rule-based statements and other norms in the eleven-norm list remain non-enforceable. Their implementation remains in fact subject to the good will of responsible cyber powers".

[277] "Public International Law applicable to cyberspace" está entre os tópicos da agenda da CJI, a serem discutidos durante a sessão ordinária programada para o período de 1º a 10 de agosto de 2022, conforme Resolução CJI/RES.272 (C-O/22). (OEA, 2022a).

Entre os anos de 2018 e 2020, a CJI desenvolveu um projeto intitulado "Direito Internacional e Operações Cibernéticas do Estado: Melhoria da Transparência" para fornecer parâmetros claros sobre a aplicação do direito internacional ao espaço cibernético e contribuir com a transparência na forma como os Estados-membros entendem tal aplicabilidade (OEA, 2020b). O projeto, sob relatoria do Doutor Duncan B. Hollis, funcionou como um fórum regional para a temática ao distribuir um questionário sucinto, porém detalhado, para os Estados-membros.

Pautado em quatro[278] objetivos que obedecem e estão correlacionados com as orientações do CICV e os ensejos dos fóruns da ONU, o projeto almejou reverter o déficit de informações sobre como os Estados visualizam a regulação das operações cibernéticas pelo direito internacional. Observando que poucos membros da OEA puderam participar dos GGEs, e que no OEWG as discussões ainda se encontram bastante genéricas, adveio como um fórum adicional para encorajar e, em certa medida, "agilizar" a resolução de impasses (OEA, 2020b, p. 4-5). Dentre as perguntas – preparadas em conjunto com o Departamento de Direito Internacional da OEA e com contribuições do CICV – enviadas aos Estados-membros:

> 1. O seu Governo tornou público algum documento oficial, discurso ou declaração similar resumindo como entende que o direito internacional se aplica às operações cibernéticas? [...]
> 2. Os ramos do direito internacional atual (como a proibição do uso da força, o direito de legítima defesa, o direito internacional humanitário e os direitos humanos) aplicam-se ao ciberespaço? Existem áreas em que a novidade do ciberespaço exclui a aplicação de um conjunto específico de direitos ou obrigações legais internacionais?
> 3. Uma operação cibernética por si só pode constituir um uso de força? [...] Uma operação cibernética pode ser qualificada como uso da força ou ataque armado sem causar os efeitos violentos que se utilizaram para marcar tais limiares em conflitos cinéticos passados?
> 4. Fora do conflito armado, quando é que um Estado seria responsável pelas operações cibernéticas de um ator não estatal? Que grau de controle ou participação deve ter um Estado nas operações do ator não estatal para acionar a responsabilidade legal internacional desse Estado?
> [...]
> 6. De acordo com o direito humanitário internacional, uma operação cibernética pode ser qualificada como um "ataque" segundo as normas que regem a condução de hostilidades se não causar morte, lesões ou danos físicos diretos ao sistema informático em questão ou à infraestrutura que suporta? Pode uma operação cibernética que produz apenas uma perda de funcionalidade, por exemplo, ser qualificada como ataque? Em caso afirmativo, em que casos?

[278] Quais sejam: "a) identificar áreas de convergência na forma como os Estados entendem quais são as regras legais internacionais que se aplicam e como o fazem. [...] b) identificar pontos de vista divergentes sobre que normas internacionais se aplicam ou como o fazem. [...] c) limitar os riscos de escalada ou conflito não intencional, já que os Estados têm interpretações diferentes da aplicação do direito internacional e desconhecem ou não compreendem como os outros veem o problema; e d) dar à OEA e aos Estados membros uma voz apropriada nos diálogos mundiais sobre a aplicação do direito internacional." (OEA, 2020b, p. 1).

> 7. Uma operação cibernética que só ataca dados seria regida pela obrigação do direito internacional humanitário de dirigir ataques apenas contra alvos militares e não contra alvos civis?
> [...]
> 9. A devida diligência é uma norma do direito internacional que os Estados devem respeitar no exercício da sua soberania sobre as tecnologias da informação e das comunicações nos seus territórios ou sob o controle dos seus cidadãos?
> [...] (OEA, 2020b, p. 12-13).

As inquirições, bastante assertivas, foram elaboradas nos primeiros meses de 2019, e aguardavam retorno dos Estados para os meses seguintes. Como resultado geral do questionário, notou-se a baixa porcentagem de respostas, evidenciando não só o interesse imediato de poucos Estados em regular suas condutas no ciberespaço a partir do direito internacional, como também a relutância dos Estados na transparência sobre suas posições acerca da aplicação do direito internacional.

À luz do último relatório[279] do projeto da CJI, constatou-se que os Estados têm, apenas em certa medida, ciência das ameaças existentes e potenciais do uso desmedido do espaço cibernético. Boa parte dos Estados-membros já possui ou está desenvolvendo atividades nacionais de cibersegurança. Porém, essas baseiam-se sobretudo em estratégias ou políticas nacionais de regulamentação das TICs que acobertam a segurança cibernética e a cibercriminalidade à nível interno. Há um misto de impasses – técnicos, políticos e legais[280] – que contribuem para o silêncio ou reticência dos Estados em posicionar-se ou emitir declarações diretivas voltadas ao âmbito da segurança internacional (OEA, 2020b, p. 7, 16).

Vários Estados da OEA não responderam às perguntas dentro das especificações esperadas, por vezes remetendo ao OEWG em andamento na ONU como o ambiente onde suas declarações e posições estavam sendo construídas. Ocorre que, como o próprio relatório de respostas consolidado pelo Dr. Hollis expõe, até o momento os Estados comumente têm prestado depoimentos bastante generalizados no citado fórum (OEA, 2020b, p. 5); possivelmente como um reflexo da postergação pretendida. A "insistência" no tema com a abertura de novas oportunidades de diálogo e manifestação pode ser salutar nesse sentido.

---

[279] Ao longo do projeto, foram emitidos cinco relatórios sobre o tema da melhoria da transparência e a forma como os Estados-membros entendem a aplicação do direito internacional às operações cibernéticas estatais. O quinto relatório, de agosto de 2020, apresentou as conclusões do projeto, bem como anexou o questionário enviado aos Estados e as respostas substantivas recebidas. (OEA, 2020b).

[280] O desafio técnico por vezes decorrente da ausência de capacidade técnica para atribuir – ainda que não a autoria, mas a origem – de uma operação cibernética; político e legal, sobretudo pela falta de experiência governamental em questões atinentes à cibernética, e ao mesmo tempo, em demonstrada reticência sobre a manutenção da sua liberdade de participar de operações cibernéticas, ainda que futuramente. No mais, há que citar a existência de desafios políticos externos – a relutância de adotar posições contrárias a Estados que atualmente podem ser considerados grandes potências na capacidade cibernética ofensiva ou defensiva, como EUA, Rússia e China, e assim evitar o envolvimento com disputas entre os Estados, por exemplo. (OEA, 2020b, p. 7-8).

Ademais, das respostas obtidas, percebeu-se a desigualdade das capacidades legais dos Estados na área cibernética: alguns demonstraram possuir amplo conhecimento sobre o uso de operações cibernéticas e suas implicações, enquanto outros exprimiram uma baixa familiaridade com as especificidades do assunto. Diante disso, o projeto da CJI pôde reconhecer a necessidade de criação de maior capacidade jurídica internacional entre os membros da OEA, o que possivelmente refletirá no planejamento de mais iniciativas sobre a temática, como já se espera pela extensão e continuidade da matéria na agenda da CJI. (OEA, 2020a; 2020b, p. 6-7).

Uma manifestação, citada de forma inominada no último relatório, reitera o potencial da OEA como fórum governamental onde a discussão diplomática pode ocorrer de forma mais acautelada e propícia para a construção de opiniões bem fundamentadas – e, portanto, transparentes: refere-se ao desenvolvimento de uma perspectiva latino-americana sobre a governabilidade internacional e viabilidade de um marco legal para o ciberespaço (OEA, 2020b, p. 8, 35).

Nessa observação, ventilou-se a possibilidade de que os países latino-americanos elaborassem um instrumento de compreensão do direito internacional no ciberespaço, colocando-se à par dos Estados europeus e dos especialistas do norte global, onde a maioria das ideias sobre o direito internacional (inclui-se o DIH) no ciberespaço foram desenvolvidas. Uma possibilidade ousada, mas dentro dos propósitos da OEA e do engajamento que a AGNU tem asseverado como necessário.

Notoriamente, pelos esforços mais recentes da OEA, percebe-se que o diálogo sobre o uso do ciberespaço continuará na agenda da organização, que, inclusive, deverá contribuir nas discussões em andamento neste segundo mandato do OEWG. Dos resultados daquele que seria o primeiro projeto específico a tratar sobre o uso de operações cibernéticas pelos Estados nas Américas, e que foi traduzido para todos os idiomas da OEA – permitindo a ampla ciência dos desafios no hemisfério –, restou claro o papel que o fórum regional pode ter na busca por transparência e na construção da capacidade jurídica dos seus Estados-membros. Construção essa que pode ocorrer até mesmo promovendo perspectivas novas, mais abrangentes e atreladas ao desenvolvimento dos direitos humanos no ciberespaço – em tempos de conflito armado ou de paz –, sob um prisma não europeu.

3.3.4 A União Europeia

Na Europa, a segurança cibernética não é uma preocupação recente. Como marco jurídico voltado ao reconhecimento das ameaças do meio e à adoção de uma política comum

destinada à proteção da sociedade contra ilícitos no ciberespaço, vale rememorar a Convenção de Budapeste sobre o Cibercrime, de 2001. Aquele que seria o primeiro tratado internacional[281] a versar sobre segurança cibernética, delimitou-se aos crimes cometidos através da *internet* e redes informáticas, e emergiu como base para a tratativa da criminalização de condutas e para a formação de uma estrutura de cooperação internacional sobre os cibercrimes.

Contudo, referindo-se ao uso de operações cibernéticas e conflitos armados internacionais, bem como à ênfase dada aos organismos internacionais regionais – como a União Europeia (UE) – enquanto fóruns políticos, foi apenas em 2013 que o bloco de países europeus emitiu um documento expondo a aplicabilidade do DIH, bem como dos DHI, aos conflitos armados que se estenderem ao ciberespaço[282]. Tratou-se da Estratégia da União Europeia para a Cibersegurança (ECS -UE) [283], que prevê a coordenação de políticas também nas áreas jurídica, diplomática e de defesa e segurança dos Estados-membros (SCHMITT, 2021a, p. 665; UE, 2013).

A posição da organização foi ratificada posteriormente, para além dos documentos de atualização da ECS, inclusive com menções à *due diligence* e a questões conexas com os impasses da aplicabilidade do direito internacional ao ciberespaço (SCHMITT, 2021a, p. 665; ONU, 2021c, p. 44). A ECS, pautada na promoção de políticas de transparência, responsabilização e segurança no mundo digital, apresentou ações específicas para melhorar o desempenho geral e uniforme da UE. Sem descaracterizar os Estados-membros como os principais responsáveis pela sua própria segurança cibernética, foram apresentadas cinco prioridades estratégicas: a garantia da resiliência do ciberespaço; a redução drástica da cibercriminalidade; o desenvolvimento da política e das capacidades no domínio da defesa cibernética; o desenvolvimento de recursos industriais e tecnológicos para a cibersegurança; e o estabelecimento de uma política internacional em matéria de ciberespaço coerente com os valores fundamentais da organização regional (UE, 2013, p. 5).

Nessa toada, pode-se inferir que a partir da propositura da ECS houve um incremento e ramificação das atividades atinentes à melhoria das capacidades e à cooperação nos assuntos de cibersegurança, donde foram elaboradas políticas específicas para assuntos de criminalidade e investigação penal no ciberespaço, para facilitação do acesso a bens e serviços digitais, e até

---

[281] Data de 2001 e foi elaborado no escopo do Conselho da Europa, entrando em vigor em 2004. Dá especial atenção às violações de direitos autorais, fraudes, pornografia infantil e violações de segurança de redes (CONSELHO DA EUROPA, 2001).

[282] "Se os conflitos armados se estenderem ao ciberespaço, aplicar-se-á ao caso vertente o Direito Internacional Humanitário e, se for caso disso, a legislação sobre os direitos do homem." (UE, 2013, p. 18).

[283] "Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace" (SCHMITT, 2021a, p. 665).

mesmo para refutar campanhas de desinformação através de comunicação estratégica[284]. Em 2014, por exemplo, foi adotado um Quadro Estratégico para a Ciberdefesa, posteriormente atualizado, como parte da cooperação UE-OTAN. (UE, 2019, p.13-14).

A ECS passou por sucessivas atualizações ao longo dos anos. Dentre um dos pilares da estratégia lançada em 2013, constava a Diretiva SRI[285] (relativa à segurança das redes e da informação), que inaugurou o primeiro ato legislativo em matéria de cibersegurança na UE, tornando-se elemento jurídico central para o tema. A diretiva trouxe como obrigação aos Estados-membros a adoção de estratégias nacionais sobre segurança das redes e dos sistemas de informação, e também exigiu a criação de equipes de resposta a incidentes de segurança informática (*Computer Security Incident Response Team* – CSIRT) integradas em estruturas de cooperação com o propósito de intercâmbio de informações entre os Estados-membros (UE, 2019, p. 15-17).

Dessarte, dos projetos lançados e em curso, nota-se a visão abrangente da UE sobre a prevenção e a resposta a interrupções cibernéticas e a ataques cibernéticos. Destacando o papel da "ciberdiplomacia", o grupo igualmente tem apelado por um modelo reforçado de governança da *internet*, com a inclusão de partes interessadas (empresas, organizações outras, etc.) e com o ensejo a esforços para o desenvolvimento das capacidades cibernéticas de países terceiros. Conforme as declarações cedidas ao longo dos GGEs das Nações Unidas, a preocupação constante com os desafios do meio cibernético foi, inclusive, motivadora da elaboração de uma estrutura para resposta conjunta do grupo às atividades cibernéticas maliciosas dirigidas contra Estados-membros, intitulada *Cyber Diplomacy Toolbox*, estrutura que inclui a adoção de medidas diplomáticas proporcionais ao escopo, escala, duração, intensidade, complexidade, sofisticação e impacto da atividade cibernética sofrida. (ONU, 2021c, p. 42; HÄRMÄ; MINÁRIK, 2017).

A propositura da *Cyber Diplomacy Toolbox* é direcionada à prevenção de conflitos[286], à mitigação de ameaças cibernéticas e à melhor estabilidade das relações internacionais. Para isso, até mesmo considera que nem todas as medidas de resposta diplomática exigem a efetiva atribuição de autoria da operação cibernética[287] (HÄRMÄ; MINÁRIK, 2017). Em que pese os

---

[284] Respectivamente: a Agenda Europeia para a Segurança, de 2015; a Estratégia para o Mercado Único Digital, de 2015; a Estratégia Global, de 2016 (UE, 2019, p. 14).

[285] A Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, a qual trazia medidas destinadas a garantia de um elevado nível comum de segurança das redes e da informação em toda a União Europeia (UE, 2019, p. 69).

[286] Conforme observam Annegret Bendiek e Matthias Schulze (2021, p. 5), as sanções previstas a partir da *Cyber Diplomacy Toolbox* devem ser ajustadas para ficar abaixo do limiar de conflito armado.

[287] Tal questão ainda é controversa, com argumentos em que a atribuição deve ser vista como ato soberano dos Estados-membros, os quais possuem capacidades técnicas e de inteligência variadas. Como lidar com o processo

desafios de implementação de suas medidas[288], a iniciativa demonstra o interesse em promover ações que visem uma ordem internacional com parâmetros do uso responsável do ciberespaço a partir da harmonização das áreas técnica e jurídica (BENDIEK; SCHULZE, 2021, p. 6-7).

As medidas da UE na última década têm demonstrado o crescente incentivo à cooperação na matéria cibernética e os objetivos de facilitar a mitigação de ameaças imediatas e de longo prazo, e de influenciar o comportamento de atores mal-intencionados a longo prazo. Em dezembro de 2020, a UE começou a delinear uma nova estratégia de cibersegurança[289], voltada à proteção dos cidadãos e das empresas, e com maior enfoque na segurança das infraestruturas críticas. A nova ECS, ao ser norteada pelo ideal de um ciberespaço "global, aberto, livre, estável e seguro, baseado no Estado de Direito, nos direitos humanos, nas liberdades fundamentais e nos valores democráticos[290]" estimula que a UE adira a normas, regras e princípios de comportamento responsável do Estado no ciberespaço – propósito também levado às discussões na AGNU, com o convite para o estabelecimento de um programa de ação que ofereça uma plataforma permanente de cooperação e intercâmbio de boas práticas no escopo das Nações Unidas. (ONU, 2021c, p. 42-43; CONSELHO EUROPEU, 2022).

Sobre o DIH e as condutas no ciberespaço, a UE continua a promover fortemente que o direito internacional – a Carta das Nações Unidas, o DIH e os DHI – se aplica ao meio digital, e tem se sustentado como um dos principais atores na temática de fortalecimento de confiança entre Estados no espaço cibernético, com forte atuação nos fóruns da ONU (UE, 2021). Nesse âmbito, tem estimulado que os Estados emitam declarações e documentos sobre como ocorre tal aplicabilidade, e tem endossado que a organização regional e seus Estados-membros não requerem e não veem a necessidade de criação de um novo instrumento jurídico internacional para tratar da aplicabilidade do DIH, haja vista que os princípios humanitários abordados ao

---

de atribuição, seja ela técnica, jurídica e/ou política para a classificação de responsabilidade, portanto, é tema polêmico e pendente de harmonização de critérios pelos Estados-membros da UE. (BENDIEK; SCHULZE, 2021, p. 6).

[288] Em julho de 2020, por exemplo, após anos dos incidentes iniciais, o Conselho da UE impôs sanções contra cidadãos da Coréia do Norte, China e Rússia, considerados responsáveis pelos ataques *WannaCry*, *Cloud Hopper* e *NotPetya*, respectivamente. O decurso de tempo entre o ataque e a atribuição decorre dos desafios técnicos e legais, onde se requer recursos forenses e de inteligência de tecnologia da informação. Apenas alguns Estados-membros da UE iriam dispor dessa capacidade de atribuição, entre eles, Suécia, Países Baixos, Estônia, Áustria, França e Alemanha; nem sempre há a "vontade" política de partilhar as informações obtidas e, nesse sentido, as estratégias de cibersegurança e ciberdiplomacia da UE têm atuado (BENDIEK; SCHULZE, 2021, p. 8-9).

[289] A "Estratégia de Cibersegurança da UE para a Década Digital", a terceira ECS, após atualização em 2017 (ONU, 2021c, p. 42).

[290] "The European Union's cybersecurity for the digital decade aims to promote and protect a global, open, free, stable and secure cyberspace grounded in human rights, fundamental freedoms, democracy and the rule of law." (ONU, 2021c, p. 41).

longo desta pesquisa já ofereceriam proteção integral para a população civil (ONU, 2021c, p. 44-45).

Portanto, o que há de ser aprofundado e discutido, aos olhos da organização e dos seus Estados-membros, é como o arcabouço jurídico existente se aplica. A busca de um entendimento comum nesse sentido é primordial, e deve ocorrer pela transparência entre os Estados sobre seus posicionamentos e pela capacitação sobre o direito existente como meio de promoção da estabilidade internacional e de prevenção de conflitos no espaço cibernético. Por isso, tem visualizado nos fóruns da ONU a oportunidade de avançar na adoção de medidas de construção de confiança[291] sobre o uso do ciberespaço – agora, em um projeto à nível global.

3.3.5 A OTAN (os Manuais de Tallinn)

Frente à ausência de um documento vinculante e que abordasse diversos aspectos do uso do ciberespaço, e ao evidente interesse político e militar dos Estados-membros da OTAN em buscar respostas e conjecturar cenários de impasse internacional, em 2009, o Centro de Excelência em Defesa Cibernética Cooperativa da OTAN (CCDCOE) convidou especialistas para produzir um manual sobre a lei internacional aplicável à guerra cibernética.

A criação do CCDCOE, como referência de pesquisa e treinamento em defesa cibernética, foi sugerida já em 2004, pela Estônia. Porém, apenas após a repercussão daqueles que seriam os primeiros ataques cibernéticos politicamente motivados, em 2007, é que as demais nações da Aliança cederam maior atenção às ameaças do uso do domínio[292]. Desse modo, desde 2009 o CCDCOE tem realizado reuniões sobre segurança e defesa cibernética, discutindo aspectos jurídicos e tecnológicos da nova tendência. (CCDCOE, 2022).

O lançamento do projeto de elaboração do Manual de Tallinn representa o processo de pesquisa mais conhecido internacionalmente no âmbito do direito internacional e ciberespaço. Reunindo juristas e pesquisadores de renome internacional de países parceiros, o projeto seguiu os moldes de processos que resultaram em documentos como o Manual de Oxford de 1880, o Manual de San Remo de 1994, e o Manual de Harvard de 2009 sobre aplicabilidade do direito

[291] "The European Union and its member States will be guided in their use of ICT by existing international law, as well as through adherence to voluntary norms, rules and principles of responsible State behaviour and their implementation in cyberspace, as articulated in the successive reports of the Group of Governmental Experts of 2010, 2013 and 2015." (ONU, 2021c, p. 45).

[292] O CCDCOE foi estabelecido por iniciativa da Estônia, de forma conjunta com a Alemanha, Itália, Letônia, Lituânia, Eslováquia e Espanha, em maio de 2008; recebeu status de organização militar internacional no mesmo ano, pelo Conselho do Atlântico Norte (CCDCOE, 2022).

internacional[293]. Como resultado das pesquisas, em 2013 foi publicado o primeiro Manual de Tallinn, intitulado "*Tallinn Manual on the International Law Applicable to Cyber Warfare*", inteiramente voltado à análise de operações cibernéticas envolvendo uso da força e daquelas que ocorrem no contexto de conflitos armados; em 2017, sobreveio novo grupo de especialistas e o Manual de Tallinn 2.0, ampliando o escopo do primeiro estudo (CCDCOE, 2022; SCHMITT, 2017, p. 1).

O Manual de Tallinn 2.0 (*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*) proporcionou uma visão mais abrangente do uso de operações cibernéticas, promovendo discussões sobre o uso dessas em tempos de paz – ou quando estiverem abaixo do limite do uso da força –, bem como modificou e aumentou os debates do primeiro documento. Desde seu introito, é informado que a sua dissertação em regramentos comentados é fruto de discussões entre especialistas independentes e suas percepções acadêmicas e pessoais, que não vincula os Estados que patrocinam o projeto e fazem parte da OTAN, assim como não representa a posição do CCDCOE como organização militar, ou da própria OTAN. Não é, portanto, um documento oficial, nem possui qualquer natureza vinculativa; indica o resultado de discussões sobre como direito internacional – público – já existente deve ser interpretado à luz do ciberespaço, mas não é um "guia de boas práticas", nem uma declaração crítica sobre como as normas humanitárias deveriam[294] ser. (SCHMITT, 2017, p. 2-3).

Sob o aspecto geral de declaração do DIH já existente como aplicável às operações cibernéticas, o Manual de Tallinn 2.0 converge com as conclusões dos GGEs da ONU. Todavia, as discussões em sua elaboração transpõem as dificuldades geopolíticas de uma resolução sobre em que medida se aplica, aprofundando-se no exame de conceitos e nos possíveis cenários de conflito cibernético. Durante esta pesquisa, bastante foram mencionadas as posições examinadas pelos especialistas em termos de operacionalização da proteção jurídica em atividades no ciberespaço; não sem motivo, pois enquanto não há *opinio juris* ou considerável posicionamento pormenorizado dos Estados sobre a "suficiência" das normas humanitárias – seja por suposta incapacidade legal, por receio de cunho político, etc. –, no Manual há um diálogo entre possíveis visões. Essa característica é suficiente para tornar o projeto uma

[293] Respectivamente: *The Laws of War on Land Oxford Manual*, de 9 de setembro de 1880; *San Remo Manual on International Law Applicable to Armed Conflict at Sea*, elaborado *pelo International Institute of Humanitarian Law* (IIHL); e *Manual on International Law Applicable to Air and Missile Warfare*, elaborado em 2009 por programa de pesquisa sobre política humanitária e conflito da Universidade de Harvard (SCHMITT, 2017, p. 1).
[294] "[...] Tallinn Manual 2.0 is intended as an objective restatement of the *lex lata*. Therefore, the Experts involved in both projects assiduously avoided including statements reflecting *lex ferenda*" (SCHMITT, 2017, p. 3).

referência no "desenvolvimento progressivo do direito", ainda que o documento não possua tal objetivo[295].

Há controvérsias sobre o papel que o Manual pode desempenhar como texto acadêmico o qual cede orientações sobre como interpretar os desafios humanitários no ciberespaço e que pode servir como uma fonte aos consultores jurídicos dos Estados. Marco Sassòli (2019, p. 562-564), por exemplo, questiona a neutralidade das posições arguidas ao longo do documento, e discorda da aplicabilidade objetiva das normas humanitárias já existentes – convencionais ou consuetudinárias – de forma integral[296]. Até certo ponto, o estabelecimento de "*blackletter rules*[297]" para afirmar como o direito já posto acolhe a realidade cibernética (MELZER, 2019, p. 44) seria falho, mas é uma tentativa de agasalhar juridicamente situações que idealmente seriam resolvidas mediante novos tratados.

Mette Eilstrup-Sangiovanni (2017, p. 389-393) considera que o Manual, mesmo apresentando as regras ajustadas pelos especialistas, possui disparidades significativas sobre como princípios específicos do direito internacional se aplicam, e passa por cima de questões e conceitos chegando a conclusões insatisfatórias[298]. Para a pesquisadora, a negociação de um tratado internacional específico aos conflitos cibernéticos é imprescindível, posto que se alcançaria orientação e traria restrições claras ao comportamento dos Estados.

O papel que os fóruns multilaterais existentes até o momento têm exercido e a influência que o Manual de Tallinn pode reproduzir na capacitação legal sobre o ciberespaço muito enfatiza o potencial que instrumentos não vinculativos ou normas voluntárias de "comportamento responsável[299]" possuem de direcionar a prática estatal e mesmo vir a formar direito consuetudinário. Segundo aduz Eilstrup-Sangiovanni (2017, p. 402-403), essa abordagem de normas de *soft law* não seria eficaz para lidar com conflitos cibernéticos, mormente por quatro características do ciberespaço: o grande número de interessados no

---

[295] "This Manual [...] does not represent 'progressive development of the law'" (SCHMITT, 2017, p. 2-3).
[296] "While the Tallinn Manual is extremely helpful, it was unable to introduce new rules where they are needed, and it is often criticized as being produced mainly by experts linked to NATO" (SASSÒLI, 2019, p. 562).
[297] Refere-se à disposição em regras objetivas, enumeradas conforme o impasse aludido (p. ex., soberania, jurisdição, responsabilidade internacional, normas de condução das hostilidades, etc.), cujo texto indica a conclusão que os especialistas chegaram sobre como o direito internacional se aplica, reafirmando-o (MELZER, 2019, p. 44). Após cada dispositivo, é apresentada a fundamentação dos especialistas, inclusive averiguando posições distintas; o Manual de Tallinn 2.0 possui 154 regras, substituindo o documento anterior (SCHMITT, 2017).
[298] "[...] the Manual fails to define the precise preconditions to treating a cyber operation as equivalent to an "armed attack" under international law, thereby allowing victims to respond forcefully in self-defense as well as legitimizing forceful response by third parties in collective defense. […] The crucial question of when an offensive cyber-operation amounts to an armed attack thus remains unsettled. […] without a clear common understanding of when a cyberattack amounts to an act of war, simply insisting that IHL applies in cyberspace is of little use." (EILSTRUP-SANGIOVANNI, 2017, p. 393-394).
[299] Como as trazidas pelos GGEs, em seus relatórios.

domínio cibernético, ou seja, a gama de atores heterogêneos demandando uma coordenação centralizada; a dificuldade de monitoramento do comportamento dos atores, e de suas intenções benignas ou malignas; conjuntamente, a facilidade de acesso ao uso de armas cibernéticas; e a necessidade de uma efetiva implementação – de medidas de coordenação, monitoramento, etc. – à nível doméstico, que ocorreria mais facilmente quando da feitura de um tratado. Todos esses fatores seriam decisivos para a elaboração de um documento precisamente codificado e juridicamente vinculativo, com normas claras de proibição e previsão de fortes sanções.

Por outro lado, em posição a qual a maioria dos Estados nos fóruns da AGNU parece convergir até então[300], a busca por programas de ação à nível internacional, e o referenciamento a normas de *soft law* ou a guias de comportamento no espaço cibernético, no contexto atual, tem a sua função e valor. O diálogo contínuo sobre melhorias tecnológicas e sobre políticas transparentes podem ajudar os Estados a enfrentar o problema de atribuição, por exemplo, e a detalhar ambiguidades existentes quando se trata de interpretação do DIH existente ao ciberespaço, levando ao desenvolvimento futuro de normas costumeiras ou codificadas com base na experiência (SWANSON, 2010, p. 326). Ainda, não deixa de ser verdade que as ameaças cibernéticas em termos de segurança internacional ainda são uma realidade muito nova, estão submissas a tecnologias em constante evolução, e que a expressão em regras formais e rígidas nesse campo corre o risco de se tornar desatualizada antes mesmo de entrar em vigor (EILSTRUP-SANGIOVANNI, 2017, p. 402; MAČÁK, 2017; SASSÒLI, 2019, p. 563).

Por vezes, a mistura de abordagens iniciais de instrumentos de *soft law* – sejam eles elaborados por atores estatais ou não –, em conjunto com o surgimento – ainda que lento – de regras vinculantes, pode vir a fornecer uma resposta lógica e funcional a um fenômeno em ascensão; e o estímulo a que os Estados expressem publicamente suas opiniões sobre em que medida o direito internacional se aplica ao ciberespaço pode acelerar a cooperação em prol de políticas protetivas (MAČÁK, 2017, p. 898). Ademais, os projetos de capacitação técnica e legal propostos nas organizações regionais e também no escopo da ONU indicam uma iniciativa de troca de experiências e tecnologias entre Estados que podem preceder mecanismos de monitoramento eficazes.

Nessa seara, instrumentos como o Manual de Tallinn são bem-vindos enquanto propulsores do debate e desenvolvimento do direito aplicável ao ciberespaço. O próprio projeto do CCDCOE percebe a dinamicidade do ciberespaço, e tem para o instrumento de *soft law* a previsão de continuidade das suas discussões na elaboração do Manual de Tallinn 3.0.

[300] Quando do término dos trabalhos do sexto GGE, em 2021, e início do segundo OEWG, no primeiro semestre de 2022 (DIPLO, 2022b).

(CCDCOE, 2022b). De toda sorte, diante das incertezas e dos terrenos ainda desconhecidos do cenário de guerra cibernética, o caminho a passos lentos, mas progressivos, para a adoção de políticas internacionais baseadas na devida diligência e transparência dos Estados pode render frutos que não excluem uma possível futura convenção sobre o uso de operações cibernéticas e responsabilidade internacional ou, especificamente, sobre armas cibernéticas. Pelo contrário, guarnecem referências, experiências em âmbito interno, o debate de opiniões e a prática inerentes à construção de um instrumento vinculativo que seja condizente com os objetivos estratégicos e políticos dos Estados.

CONSIDERAÇÕES FINAIS

A busca pelo conceito de "guerra", qualquer que seja o intuito desta inquirição – predominantemente político, econômico, militar, e/ou jurídico – implicará, sempre, em trabalho inacabado, conexo às transformações próprias da dinâmica social. Aproximar-se de um conceito, apto aos fins que se almeja, contudo, possibilita que as práticas relacionadas ao termo sejam delimitadas e minimamente balizadas sob a ótica do direito.

Ao início desta pesquisa, afirmou-se que a guerra é um fenômeno mutável e complexo, donde a metáfora clausewitziana serve para remeter ao desenvolvimento de tecnologias como aparato de superioridade em detrimento do adversário. O uso de operações cibernéticas como nova tecnologia em cenários de conflito armado e o potencial ofensivo que inflige às vítimas desses conflitos traz à tona uma série de indagações a partir de um recorte do que viria a ser "guerra cibernética".

Apesar das disparidades na seara acadêmica e das incongruências na praxe internacional, não referindo-se a meras situações de perturbação ou tensão entre duas ou mais partes orquestradas no ciberespaço, mas assumindo que efeitos violentos podem decorrer de ações no novo domínio e implicar em problema humanitário, aproximou-se de uma delimitação. Eis que o termo foi aqui utilizado referindo-se a conflitos armados internacionais em que há uso de operações cibernéticas com fulcro militar, restrição que por si só procede controvérsias sobre a possibilidade de ações no ciberespaço assumirem a feição de uso da força estatal, e serem visualizadas como atos de guerra segundo os ditames do Direito Internacional Humanitário.

A partir de uma lógica de escalabilidade dos conflitos cibernéticos, observou-se que a distinção entre as ameaças dos ciberataques (em amplo aspecto) com base nos possíveis efeitos danosos permite que seja alcançada uma delimitação de guerra cibernética adequada e, ainda que com ressalvas a serem sanadas em diálogo internacional, mais propensa à aplicação e eficácia do DIH. Em pleno século XXI e diante de uma sociedade cada vez mais interconectada, atos de violência, uso de força, ataques "armados" podem ser vislumbrados a partir de ações no ciberespaço, mas a conotação atribuída a cada tipo de atividade, frente a termos tão complexos para o direito internacional, requer mais estudos sobre a existência de critérios de avaliação de ataques cibernéticos – de natureza técnica, correspondente aos avanços na área de tecnologia da informação, mas também jurídica.

Como e em que medida um ataque cibernético pode, isoladamente, dar início a uma situação de guerra, na acepção do *jus ad bellum*, persiste como tema enigmático para a

sociedade internacional, sobretudo quando ainda se questiona o nível de violência de uma atividade no meio cibernético. Apesar disso, defende-se que ações efetuadas no novo domínio, na proporção em que visem eliminar as forças armadas adversárias ou atingir objetivos militares, podem ser reconhecidas como atos de guerra.

Analogias com o grau de destruição que seria alcançado por armas convencionais (*means-based standard*) e até de destruição em massa, ou com a delimitação sobre quem ou o que seria o alvo o ataque (*target-based standard*), separadamente, não funcionam bem para fundamentar como um ataque cibernético pode ser visto como ato de guerra. Nessa toada, a análise das consequências que se mostrem potencialmente violentas ou destrutivas, sob a perspectiva de efeitos globais (*effects-based standard*), introduz um modelo de avaliação mais plausível – mas que ainda precisa ser melhor elaborado – ao contexto do ciberespaço.

Ao passo que determinados ataques cibernéticos possam ser classificados como atos de guerra, não há que se questionar a submissão aos preceitos do DIH. Em tempos onde a assimilação do termo inicial de um conflito armado foge de formalidades como por ato jurídico declaratório, reconhecer que as normas protetivas de vítimas de guerra se aplicam desde o primeiro ataque ou ato de guerra, e que esse também pode ocorrer por meios cibernéticos, implica em avanço humanitário.

Entende-se que a preocupação em se fazer valer a proteção humana independe das adversidades sobre o início de um conflito armado, mas que a discussão aprofundada sobre o momento em que o DIH passa a regular os conflitos cibernéticos é imprescindível. Nos dias atuais, não há exemplos claros e amplamente reconhecidos de conflitos armados iniciados por ataques cibernéticos, mas desvincular-se dessa possibilidade e deixar de questioná-la não condiz com a importância que o uso do ciberespaço tem exercido no andamento de tarefas essenciais do cotidiano de um simples cidadão e no desenvolvimento de capacidades militares de atores estatais ou não-estatais.

Para conflitos armados em curso, a compreensão de que operações cibernéticas em seu escopo, de forma híbrida, são regidas pelo DIH é crescente entre Estados e organizações internacionais. Seja por meio de documentos oficiais, declarações ou discussões em fóruns internacionais, nota-se a tendência de admissão de que o uso de operações cibernéticas não compõe zona cinzenta no arcabouço humanitário. Contudo, a mera declaração de aplicabilidade do DIH, sem avaliar como isso é possível, reforça a incapacidade de operacionalizar os limites jurídicos e de restringir quais procedimentos e mecanismos podem ser utilizados pelas partes em conflitos armados.

Nessa toada, há que se assumir a conjuntura nebulosa e imprecisa que ainda atravessa o uso de operações cibernéticas e os limites impostos pelo DIH tradicionalmente elencado nas Convenções de Genebra e seus Protocolos Adicionais. Compreende-se que os princípios humanitários têm o potencial de guiar a condução das hostilidades, ao lado da análise técnica das particularidades tecnológicas de cada atividade cibernética.

O desenvolvimento da capacidade militar dos Estados por meios cibernéticos, até certo ponto, prezando pela razoabilidade em seu emprego, pode ser visto como aliado sob o viés humanitário. Por isso, os princípios podem oferecer um direcionamento sobre as condições e proporções em que os atos de guerra cibernética são regulados, maiormente considerando os seus potenciais efeitos e as suas vitimizações.

As vulnerabilidades afloradas pelo uso descomedido do ciberespaço em situações de conflitos armados referem-se sobretudo ao acometimento de certos tipos de infraestrutura, como serviços de saúde, sistemas de controle industrial, disponibilidade e confiabilidade de serviços de *internet*, etc., ocasionando danos que por vezes não são materiais, imediatamente mensuráveis ou atribuíveis. Assim, quando tratando de guerra cibernética, a elaboração de uma estrutura de avaliação interdisciplinar, atenta aos efeitos diretos ou indiretos, incidentais ou acidentais das operações cibernéticas, e a par dos princípios humanitários, pode auxiliar na efetivação e respeito às restrições e deveres dos Estados na condução das hostilidades.

O emprego de operações que afetem a prestação de serviços e bens civis essenciais, e se revestem de meios ou métodos cibernéticos para o alcance de vantagem militar, a *priori*, não é proibido pelo DIH. Mas como, operacionalmente, as considerações humanitárias limitam essas atividades, é algo a ser constantemente debatido, à luz do surgimento de novas capacidades ofensivas – apetrechos ou "armas" cibernéticas – e da avaliação de seus efeitos.

A noção de que os princípios norteiam apenas os cenários de "ataque" como atos de violência pela força física é superada pela própria essência das regras humanitárias. Reitera-se: as consequências ou efeitos violentos que devem ser avaliados; sob esse prisma, percebe-se que até mesmo os dados, enquanto entidades não físicas, são protegidos pelo DIH, que não os resguarda apenas dos ataques cinéticos.

Notoriamente, as abstrações da cibernética trazem à tona a necessidade de diretrizes claras sobre como as limitações do *jus in bello* se aplicam ao ciberespaço; uma construção em que o consenso internacional sobre a interpretação aprofundada das normas diante das novas tecnologias é salutar, mas onde o interesse geopolítico não é uníssono e a flexibilidade com as terminologias e suas conotações originárias não é simples. Frente à presente dificuldade, reconhecer a prevalência dos princípios fundamentais da humanidade, necessidade militar,

proporcionalidade e distinção, incute o melhor caminho em prol da garantia de proteção das vítimas de guerras cibernéticas.

Entende-se que os princípios que serão passados e listados como regras de conduta para os combatentes desde a fase de planejamento de uma operação até um efetivo ataque durante as hostilidades; eles podem auxiliar a reger a novidade bélica, e o modo como eles são interpretados e empregados à luz do ciberespaço pode servir como guia de observação do comportamento estatal.

Verificou-se, confirmando a hipótese de pesquisa, que os princípios humanitários oferecem balizamento razoável ou mínimo, suficiente para demonstrar que as situações de guerra cibernética não ocorrem em um "vácuo jurídico", ainda que as fontes convencionais e consuetudinárias se mostrem questionáveis ou insatisfatórias. Naturalmente, o agir com humanidade, dentro do postulado de necessidade militar, e a tomada de decisões cujas consequências sejam proporcionais à vantagem militar, prezando pela máxima distinção mesmo quando os alvos coadunam como objetos de uso duplo, são desafios da aplicabilidade do DIH no uso de operações cibernéticas pelos Estados.

Nos posicionamentos dos Estados e nos debates acadêmicos à nível internacional, questões como a (i)legalidade de operações cibernéticas que tenham como alvo dados colocados no ciberespaço ainda estão em aberto. Nesta pesquisa, compreende-se que a avaliação dos possíveis efeitos da operação cibernética, ao lado das considerações sobre o objeto e propósito protetivo do DIH – exprimidas pelos princípios –, é capaz de esclarecer em que medida determinadas atividades cibernéticas podem ser efetuadas sem causar vitimizações contrárias à essência das normas internacionais sobre conflitos armados.

Sobre a possível responsabilização internacional ante o uso de operações cibernéticas em desconformidade jurídica, percebe-se que a difícil atribuição de autoria não constitui um impeditivo para que os Estados, por meio das suas forças armadas ou não, cumpram a obrigação de devida diligência sobre seu território, ou sobre um território ou infraestrutura cibernética sob seu controle governamental. Nessa vereda, o argumento de dissimulação de autoria e a busca contínua por assertividade no vínculo do autor do ataque cibernético com o Estado cederia espaço à *due diligence* como princípio geral de direito internacional cabível ao ciberespaço. Não se despreza a importância de desenvolvimento de mecanismos que melhor direcionem a origem de um ataque, mas entende-se que a obrigação de vigilância ou de prevenção entre Estados pode se efetivar como política em prol da proteção de potenciais vítimas.

Sem dúvidas, a *due diligence* sobrevém como obrigação de esforço, e não de resultado. Por isso, possui limitações. Entretanto, norteia a adoção de medidas preventivas e de políticas

públicas que visem assegurar o melhor cumprimento do DIH. Em meio aos debates sobre a necessidade ou desnecessidade de uma convenção internacional específica ao uso de operações cibernéticas em conflitos armados, reflete-se que a prevenção e mitigação de danos humanos por guerras cibernéticas inicia-se pelo estímulo e acolhimento a políticas públicas internacionais que percorram a matéria das ameaças no ciberespaço.

À nível de acompanhamento de políticas públicas internacionais no bojo ou fomentadas por entidades internacionais como OEA, UE e OTAN, notou-se o grau de amadurecimento e aprimoramento de capacidades – jurídica e tecnológica – dos Estados nos assuntos de uso do ciberespaço e regras humanitárias ainda heterogêneo e em fase de desenvolvimento. O incentivo à produção de normas de conduta coletiva e de interpretação do DIH, sobretudo no escopo de entidades internacionais como a CICV e ONU, pode facilitar o percurso até a construção de um entendimento uniforme sobre o uso de operações cibernéticas.

Se tal ensejo por entendimento uniforme resultará em tratado internacional sobre guerra cibernética, ou será suprido por enunciação de *opinio juris* estatal, por adoção de medidas de transparência ou outros instrumentos de diálogo internacional, cabe o aprofundamento nos fóruns subsequentes e a análise das pretensões geopolíticas dos Estados nos anos por vir.

Os passos lentos que a sociedade internacional tem dado na associação entre uso de operações cibernéticas, segurança internacional, potenciais vítimas e políticas públicas internacionais bastante reflete o misto de receio e desigualdade nas capacidades jurídica, técnica e política entre os Estados. Num futuro mais imediato, contudo, a aproximação entre teoria e realidade requererá – como já tem demandado, é o que se vê pela recente abertura do OEWG nas Nações Unidas – maior engajamento em governança cibernética e tomada de decisão estatal sobre as questões jurídicas ambíguas que dizem respeito à cibernética e conflitos armados. Aos olhos do DIH, um engajamento necessário e condizente com a sua essência, onde se reconheça que, apesar dos interesses (militares, políticos, etc.) do Estado e dos meios que resolva recorrer para alcançá-los, há a figura da pessoa humana.

REFERÊNCIAS

ABDYRAEVA, Cholpon. The use of cyberspace in the context of hybrid warfare: means, challenges and trends. **OIIP – Austrian Institute for International Affairs**, vol. 107, 2020. p. 2-36. Disponível em: <https://www.jstor.org/stable/resrep25102.7>. Acesso em 29 de ago. 2021.

ARQUILLA, John; RONFELDT, David. Cyberwar is Coming!. **In Athena's Camp**: preparing for conflict in the information age. Santa Monica: Rand Corporation, p. 23-60, 1993. Disponível em: <https://www.rand.org/pubs/reprints/RP223.html >. Acesso em 13 de jun. 2020.

ASHRAF, Cameran. Defining cyberwar: towards a definitional framework. **Defense and Security Analysis**, vol. 37, no. 3, 2021. p. 274-294. Disponível em: <https://doi.org/10.1080/14751798.2021.1959141>. Acesso em 27 de dez. 2021.

AYALEW, Y. E. Cyber Warfare: A New Hullaballoo under International Humanitarian Law. **Beijing Law Review**, vol. 6, no. 4, dez. 2015, p. 209-223. Disponível em: <http://dx.doi.org/10.4236/blr.2015.64021>. Acesso em 04 de out. 2021.

BARLOW, John Perry. A Declaration of the Independence of Cyberspace. **Duke Law & Technology Review**, vol 18, n. 1, 2019. p. 5-7. Disponível em: <https://scholarship.law.duke.edu/dltr/vol18/iss1/2/>. Acesso em 07 de ago. 2021.

BARROS, Renata Furtado de. **Guerra Cibernética:** os novos desafios do Direito Internacional. Belo Horizonte: D'Plácido, 2015.

BENDIEK, Annegret; SCHULZE, Matthias. Attribution: A Major Challenge for EU Cyber Sanctions. **Stiftung Wissenschaft und Politik Research Paper**, Berlim, n. 11, 16 dec. 2021, p. 1-46.

BIGGIO, Giacomo. Cyber Operations and The Humanization of International Humanitarian Law: Problems and Prospects. **Canadian Journal of Law and Technology**. vol. 15, n. 1, 2017, p. 41-53.

BORGES, Leonardo Estrela. **O Direito Internacional Humanitário**. Belo Horizonte: Del Rey, 2006.

BOYD, Iain. EUA, Rússia e China disputam corrida para desenvolver armas hipersônicas. **Gazeta do Povo**. Curitiba, 13 mai. 2019. Disponível em: < https://www.gazetadopovo.com.br/mundo/eua-russia-e-china-disputam-corrida-para-desenvolver-armas-hipersonicas/>. Acesso em 18 de ago. 2021.

BRASIL. **Decreto nº 10.569, de 9 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm>. Acesso em 23 de jan. 2022.

BRENNER, Susan W. At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. **Journal of Criminal Law and Criminology**. vol. 97, no. 2, 2007, p. 379 - 476.

BRODIE, Bernard. The Continuing Relevance of On War. IN: CLAUSEWITZ, Carl Von. **On War**. Princeton University Press, 1989. p. 45-58.

BROLLOWSKI, Hanna. Military Robots and the Principle of Humanity: Distorting the Human Face of the Law? IN: MATTHEE, M.; TOEBES, B.; BRUS, M. (eds). **Armed Conflict and International Law:** In Search of the Human Face. The Hague: Asser Press, 2013, p. 53-96.

BRUSTOLIN, Vitelio. Criteria for defining war, terrorism, and guerrilla warfare based on Clausewitz's concepts of the nature and essence of war. **Revista da Escola de Guerra Naval**. Rio de Janeiro, v. 25, n. 3, set./dez. 2019, p. 643-673.

CASTELLS, Manuel. A Era da Informação: Economia, Sociedade e Cultura, vol. 1. **A sociedade em rede**. 6 ed. São Paulo: Paz e Terra, 2011.

CAVELTY, Myriam Dunn. Cyberwar: concept, status quo, and limitations. **CSS Analysis in Security Policy**. Zurich: Center for Security Studies, no. 71, apr. 2010. p. 1-3.

CCDCOE – Centro de Excelência em Defesa Cibernética Cooperativa da OTAN. **CCDCOE History**. [S.l.], c2022. Disponível em: <https://ccdcoe.org/about-us/>. Acesso em 21 de jun. 2022.

_____. **The Tallinn Manual**. [S.l.], c2022b. Disponível em: <https://ccdcoe.org/research/tallinn-manual/>. Acesso em 24 de jun. 2022.

CEPIK, Marco; CANABARRO, Diego R.; FERREIRA, Thiago B. Cyberwar: Clausewitzian Encounters. **Space & Defense – USAF Academy**, vol. 8, no. 1, 2015. p. 19-33. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144752>. Acesso em 08 de jan. 2022.

CHANG, Zen. Cyberwarfare and International Humanitarian Law. **Creighton International and Comparative Law Journal**. vol. 9, no. 1, mar. 2017. p. 29-53. Disponível em: <http://dx.doi.org/10.2139/ssrn.2973182>. Acesso em 29 de jan. 2022.

CHERTOFF, Michael. The Strategic Significance of the Internet Commons. **Strategic Studies Quarterly**, vol. 8, no. 8, 2014. p. 10-16.

CHURCH, William. Information warfare. **International Review of the Red Cross**, vol. 82, no. 837, mar. 2000. p. 205-216.

CICV – Comitê Internacional da Cruz Vermelha. **Civis protegidos segundo o Direito Internacional Humanitário**. Out. 2010. Disponível em: <https://www.icrc.org/pt/doc/war-and-law/protected-persons/civilians/overview-civilians-protected.htm>. Acesso em 17 de nov. 2021.

_____. **Como o Direito Internacional Humanitário define "conflitos armados"?**, Mar. 2008. Disponível em: <https://www.icrc.org/pt/doc/assets/files/other/rev-definicao-de-conflitos-armados.pdf>. Acesso em 14 de ago. 2021.

_____. **Convenções de Genebra de 12 de agosto de 1949**. Genebra: CICV, 2016. Disponível em: <https://shop.icrc.org/icrc/pdf/view/id/2491>. Acesso em 10 de fev. 2021.

_____. **Cyberwarfare and international humanitarian law: the ICRC's position.** Jun. 2013. Disponível em: <https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf>. Acesso em 12 de jun. 2021.

_____. **ICRC statement on International Law in the second session of the OEWG on security of and in the use of information and communications technologies**. 01 apr. 2022. Disponível em: <https://www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations>. Acesso em 01 de jun. 2022.

_____. **International Humanitarian Law and Cyber Operations during Armed Conflicts**, nov. 2019. Position Paper. Disponível em: <https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf >. Acesso em 02 de out. 2020.

_____. **Protocolos Adicionais às Convenções de Genebra de 12 de agosto de 1949**. Genebra: CICV, 2017 [1949]. Disponível em: <https://shop.icrc.org/download/ebook?sku=0321/007-ebook>. Acesso em 10 de fev. 2021.

_____. **Statement by the International Committee of the Red Cross delivered by Véronique Christory, Senior Arms Control Adviser**. 15 dec. 2021a. Disponível em: <https://www.icrc.org/en/document/icrc-states-protection-civilians-data>. Acesso em 01 de jun. 2022.

_____. **Statement by the International Committee of the Red Cross, Dr. Helen Durham, Director of International Law and Policy, on Cyber Operations at the UN Security Council**. 20 dec. 2021b. Disponível em: <https://www.icrc.org/en/document/briefing-helen-durham-international-law-policy-united-nations-security-council-cyber-operations>. Acesso em 09 de mar. 2022.

_____. **Statement by the International Committee of the Red Cross to the UN Security Council Open Debate on Cyber Security, maintaining international peace and security in cyberspace**. 29 jun. 2021c. Disponível em: <https://www.icrc.org/en/document/cyber-operations-during-armed-conflict-are-not-happening-legal-void-or-grey-zone-they-are>. Acesso em 18 de ago. 2021.

_____. **Views of the International Committee of the Red Cross on autonomous weapon system.** Geneva, 11 apr. 2016. Disponível em: <https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system>. Acesso em 24 de ago. 2021.

CIJ – Corte Internacional de Justiça. **Legality of the threat or the use of nuclear weapons**. Advisory Opinion. 8 jul. 1996. Disponível em: < https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf>. Acesso em 16 de out. 2021.

CINELLI, Carlos Frederico. **Direito Internacional Humanitário:** ética e legitimidade no uso da força em conflitos armados. 2 ed. Curitiba: Juruá, 2016.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber War:** the next threat to national security and what to do about it. New York: Harper Collins, 2010.

CLAUSEWITZ, Carl Von. **Da Guerra**. Tradução de Maria Teresa Ramos. 3 ed. São Paulo: WMF Martins Fontes, 2010 [1832].

_____. **On War**. Tradução de Michael Howard e Peter Paret. 1 ed. Princeton: Princeton University Press, 1989 [1832].

CONSELHO EUROPEU. **Cybersecurity:** how the EU tackles cyber threats. [S.l.], c2022. Disponível em: <https://www.consilium.europa.eu/en/policies/cybersecurity/>. Acesso em 20 de jun. 2022.

CORN, Gary P. The potential human costs of eschewing cyber operations. **Humanitarian Law & Policy.** 31 mai. 2019. Disponível em: <https://blogs.icrc.org/law-and-policy/2019/05/31/potential-human-costs-eschewing-cyber-operations/>. Acesso em 02 de nov. 2021.

CONNELL, Michael; VOGLER, Sarah. Russia's Approach to Cyber Warfare. **Center for Naval Analyses Occasional Paper Series**, Arlington, mar. 2017, p. 1-29. Disponível em: <https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf>. Acesso em 16 de jan. 2022.

CONSELHO DA EUROPA. **Convention on Cybercrime (ETS No. 185)**. Budapest, 23 nov. 2001. Disponível em: < https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>. Acesso em 02 de jun. de 2022.

CRAWFORD, Emily; PERT, Alison. **International Humanitarian Law**. 1st ed. Cambridge: Cambridge University Press, 2015.

CYBER LAW TOOLKIT. **Scenario 12 - Cyber operations against computer data**. [S.l]: NATO CCDCOE, 2021. Disponível em: <https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data>. Acesso em 03 de mai. 2022.

DAHLBERG, Lincoln. Cyber-libertarianism 2.0: a discourse theory/critical political economy examination. **Cultural Politics**, vol. 6 (3), nov. 2010, p. 331-356. Disponível em: <https://doi.org/10.2752/175174310X12750685679753>. Acesso em 07 de ago. 2021.

DAYEM, Lina.The Ethics of Cyber Warfare. **Illini Journal of International Security**, vol. 4, no. 1, 29 mai. 2018, p. 1-16. Disponível em: <https://ugresearchjournals.illinois.edu/index.php/IJOIS/article/view/542>. Acesso em 05 de out. 2021.

DETTER, Ingrid. **The Law of War**. 3 ed. Farnham: Ashgate Publishing, 2013.

DIAMOND, Eitan. Applying International Humanitarian Law to Cyber Warfare. **Law and National Security:** Selected Issues, Tel Aviv: Institute for National Security Studies, vol. 67, no. 138, jul. 2014, p. 67-84.

DINNISS, Heather H. **Cyber Warfare and the Laws of War**. Cambridge: Cambridge University Press, 2012.

DIPLO. Geneva Internet Platform DigWatch, c2021. **Cyberconflict and warfare**. Disponível em: <https://dig.watch/topics/cyberconflict>. Acesso em 13 de jun. 2021.

_____. Geneva Internet Platform DigWatch, c2022a. **Past processes:** GGE and OEWG 2019-2021. Disponível em: <https://dig.watch/processes/un-gge#Past-processes>. Acesso em 10 de jun. 2022.

_____. Geneva Internet Platform DigWatch, c2022b. **UN GGE and OEWG**. Disponível em: <https://dig.watch/processes/un-gge>. Acesso em 14 de jun. 2022.

_____. Geneva Internet Platform DigWatch, c2022c. **UN OEWG 2021-2025 2nd substantive session.** Disponível em: <https://dig.watch/events/un-oewg-2021-2025-2nd-substantive-session>. Acesso em 15 de jun. 2022.

DROEGE, Cordula. Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. **International Review of the Red Cross**, vol. 94, no. 886, jun. 2012. p. 533-578. Disponível em: <https://doi.org/10.1017/S1816383113000246>. Acesso em 08 de mai. 2021.

DUARTE, Érico Esteves. **Conduta da guerra na Era Digital e suas implicações para o Brasil:** uma análise de conceitos, políticas e práticas de defesa. Brasília: IPEA - Instituto de Pesquisa Econômica Aplicada, 2012.

EFRONY, Dan. The UN Cyber Groups, GGE and OEWG – A Consensus is Optimal, But Time if of the Essence. **Just Security**, 16 jul. 2021. Disponível em: <https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/>. Acesso em 13 de jun. 2022.

EILSTRUP-SANGIOVANNI, Mette. Why the Word Needs an International Cyberwar Convention. **Philosophy & Technology**, vol. 31, 2017, p. 379-407. Disponível em: <https://doi.org/10.1007/s13347-017-0271-5>. Acesso em 30 de abr. 2022.

ENTENDA o caso Assange e Wikileaks fato a fato. **Carta Capital**, São Paulo, 11 abr. 2019. Disponível em: <https://www.cartacapital.com.br/mundo/entenda-o-caso-assange-e-wikileaks-fato-a-fato/>. Acesso em 24 de ago. 2021.

FINK, Jim. Researchers say Stuxnet was deployed against Iran in 2007. **Thomson Reuters**. 26 fev. 2013. Disponível em: <https://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226>. Acesso em 10 de jan. 2022.

FOUCAULT, Michel. **Em Defesa da Sociedade**. São Paulo: Martins Fontes, 2005.

GAMA NETO, Ricardo Borges. Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interação. **Revista Política Hoje**, Recife, vol. 26, no. 1, 2017, p. 201-217.

GANDHI, Robin; *et al*. Dimensions of Cyber-Attacks: social, political, economic, and cultural. **IEEE Technology and Society Magazine**, vol. 30, no. 1, spring 2011, p. 28-38. Disponível em: < https://ieeexplore.ieee.org/document/5725605>. Acesso em 24 de ago. 2021.

GEIß, Robin; LAHMANN, Henning. Protection of Data in Armed Conflict. **International Law Studies**, Newport, vol. 97, no. 556, p. 556-572, 2021. Disponível em: < https://digital-commons.usnwc.edu/ils/vol97/iss1/27/>. Acesso em 22 de mar. 2022.

GISEL, Laurent; OLEJNIK, Lukasz (eds). **The potential human cost of cyber operations**. ICRC Expert Meeting Report. Geneva: International Committee of the Red Cross, 2019. Disponível em: <https://www.icrc.org/en/document/potential-human-cost-cyber-operations >. Acesso em 19 de set. /2020.

GISEL, Laurent; RODENHÄUSER, Tilman; DÖRMANN, Knut. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. **International Review of the Red Cross**, vol. 102, no. 913, 2020. p. 287-334.

GONÇALVES, Leandro José Clemente. **A Revolução em Assuntos Militares no Contexto da Guerra de Secessão Americana (1861-1865).** Franca, 2015, 203 p. Tese (Doutorado em História), Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista Júlio de Mesquita Filho, 2015.

GRAHAM, David E. Cyber Threats and the Law of War. **Journal of National Security Law & Policy**. Washington, vol. 4, n. 1, 2010, p. 87-102. Disponível em: < https://jnslp.com/2010/08/13/cyber-threats-and-the-law-of-war/>. Acesso em 15 de out. 2021.

GREENWOOD, Christopher. Scope of application of Humanitarian Law. IN: FLECK, Dieter (ed.). **The Handbook of International Humanitarian Law**. 2nd ed. Oxford: Oxford University Press, 2008. p. 45-78.

GUERRA, Sidney. **Curso de Direito Internacional Público**. 13 ed. São Paulo: Saraiva, 2021.

HACKER tries to poison water supply of Florida city. **BBC News US & Canada**. 8 feb. 2021. Disponível em: <https://www.bbc.com/news/world-us-canada-55989843>. Acesso em 27 de nov. 2021.

HÄRMÄ, Katriina.; MINÁRIK, Tomáš. European Union equipping itself against cyber attacks with the help of cyber diplomacy toolbox. **NATO CCDCOE.** Tallinn, 18 set. 2018. Disponível em: <https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/>. Acesso em 19 de jun. 2022.

HENCKAERTS, Jean-Marie; DOSWALD-BECK, Louise (eds.). **Customary International Humanitarian Law**. vol. 1. Cambridge: Cambridge University Press, 2005.

HENCKAERTS, Jean-Marie. History and Sources. IN: SAUL, Ben; AKANDE, Dapo (eds.). **The Oxford Guide to International Humanitarian Law**. 1st ed. Oxford: Oxford University Press, 2020, p. 1-28.

HORTON, Scott. Kriegsraison or Military Necessity? The Bush Administration's Wilhelmine Attitude Towards the Conduct of War. **Fordham International Law Journal**. New York, vol. 30, no. 3, 2006. p. 576-598.

HOWARD, John D.; LONGSTAFF, Thomas A. **A Common Language for Computer Security Incidents**. United States: Sandia National Laboratories, oct. 1998. Disponível em: <https://doi.org/10.2172/751004>. Acesso em: 24 de ago. 2021.

ICTY – International Criminal Tribunal for the former Yugoslavia. **Prosecutor v. Dusko Tadic**. Decision on the defence motion for interlocutory appeal on jurisdiction. 2 oct. 1995. Disponível em: <https://www.icty.org/x/cases/tadic/acdec/en/51002.htm>. Acesso em: 22 de ago. 2021.

ISLAM, M. S. Cyber Warfare and International Humanitarian Law: A Study. **International Journal of Ethics in Social Sciences**, vol. 5, no. 1, jun. 2017. p. 101-111.

JATOBÁ, Daniel. **Teoria das Relações Internacionais**. vol. 2. São Paulo: Saraiva, 2013.

KAMINSKA, Monica; BROEDERS, Dennis; CRISTIANO, Fabio. Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone. IN: JANČÁRKOVÁ, T.; LINDSTRÖM, L.; VISKY, G.; ZOTZ, P. (eds.). **2021 13th International Conference on Cyber Conflict:** Going Viral. Tallinn: NATO CCDCOE Publications, 2021. p. 59-72. Disponível em: <https://ccdcoe.org/uploads/2021/05/CyCon_2021_book_Small.pdf>. Acesso em: 22 de jan. 2021.

KEATING, Joshua Why are nations rushing to call everything an 'act of war'?. **The New York Times**. 12 dec. 2017. Disponível em: < https://www.nytimes.com/2017/12/12/magazine/why-are-nations-rushing-to-call-everything-an-act-of-war.html>. Acesso em 10 de jan. 2022.

KEEGAN, John. **Uma história da guerra**. São Paulo: Schwarcz, 1993.

KELLENBERGER, Jakob. Armed Conflicts, International Law, and Global Security. IN: GEIß, Robin; MELZER, Nils. (eds.). **The Oxford Handbook of The International Law of Global Security.** Oxford: Oxford University Press, 2021. p. 254 - 272.

KUEHL, Daniel T.. From cyberspace to cyberpower: defining the problem. IN: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. **Cyberpower and National Security**. Washington: University of Nebraska Press, Potomac Books, 2009, p. 24-42.

LEVENSON, Eric. Florida water hack highlights risks of remote access work without proper security. **CNN US**, Atlanta, 13 Feb. 2021. Disponível em: <https://edition.cnn.com/2021/02/13/us/florida-hack-remote-access/index.html>. Acesso em 26 de nov. 2021.

LIN, Herbert. Cyber conflict and international humanitarian law. **International Review of the Red Cross**, vol. 94, n. 886, 2012. p. 515-531.

MAČÁK, Kubo; RODENHÄUSER, Tilman; GISEL, Laurent. Cyber attacks against hospitals and the COVID-19 pandemic: how strong are international law protections?. **Just Security**, New York, 27 mar. 2020. Disponível em: < https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/>. Acesso em 09 de ago. 2021.

MAČÁK, Kubo. From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers. **Leiden Journal of International Law**, Cambridge, vol. 30, no. 4, 2017. p. 877-899.

MAHADEVAN, Prem. **Cybercrime:** threats during the COVID-19 pandemic. Geneva: The Global Initiative Against Transnational Organized Crime, apr. 2020. Disponível em: <https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf>. Acesso em 20 de nov. 2021.

MAURICE, Frédéric. "Humanitarian Ambition". **International Review of the Red Cross**, n. 289, 1992. p. 363-372.

MELZER, Nils. **Cyberwarfare and International Law**. Geneva: United Nations Institute for Disarmament Research, 2011. Disponível em: <https://unidir.org/publication/cyberwarfare-and-international-law>. Acesso em 09 de out. 2021.

_____. **International Humanitarian Law:** a comprehensive introduction. Geneva: International Committee of the Red Cross, 2019.

_____. **Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law**. Geneva: International Committee of the Red Cross, 2009. Disponível em: <https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf>. Acesso em 19 de jan. 2022.

MILANOVIC, Marko; SCHMITT, Michael N. Cyber Attacks and Cyber (Mis)information Operations During a Pandemic. **Journal of National Security Law & Policy**, Washington, vol. 11, 2020, p. 247-284. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3612019>. Acesso em 20 de set. 2021.

MOTA, Rafael Gonçalves. **A Guerra Cibernética e a estrutura constitucional brasileira de proteção da soberania nacional:** Estado de Emergência Cibernética e o enfrentamento de conflitos bélicos e outras ameaças virtuais. Fortaleza, 2018. 220 p. Tese (Doutorado em Direito Constitucional), Centro de Ciências Jurídicas, Universidade de Fortaleza, 2018.

NYE JR., Joseph S. **The future of power**. New York: Public Affairs, 2011.

OLIVEIRA, Marcos Aurélio Guedes de; PORTELA, Lucas Soares. As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil. **Revista Brasileira de Estudos de Defesa**, Porto Alegre, v. 4, n. 2, dez. 2017, p. 77-99.

OPPENHEIM, Lassa F. **International Law:** a treatise. vol. 2. London: Longmans, Green and Co., 2012.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Assembleia Geral. **Resolução A/AC.290/2021/CRP.2**, Nova Iorque, 10 mar. 2021a. Disponível em: <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>. Acesso em 08 de jun. 2022.

_____. Assembleia Geral. **Resolução A/68/98***. Nova Iorque, 24 jun. 2013. Disponível em: <https://digitallibrary.un.org/record/753055>. Acesso em 12 de jun. 2022.

_____. Assembleia Geral. **Resolução A/70/174**. Nova Iorque, 22 jul. 2015. Disponível em: <https://digitallibrary.un.org/record/799853?ln=en>. Acesso em 12 de jun. 2022.

_____. Assembleia Geral. **Resolução A/76/135.** Nova Iorque, 14 jul. 2021b. Disponível em: <https://digitallibrary.un.org/record/3934214?ln=en>. Acesso em 13 de jun. 2022.

_____. Assembleia Geral. **Resolução A/76/187.** Nova Iorque, 19 jul. 2021c. Disponível em: < https://digitallibrary.un.org/record/3940878?ln=en>. Acesso em 19 de jun. 2022.

_____. Assembleia Geral. **Resolução n. 2.444 (XXIII)**, Nova Iorque, 19 dez. 1968. Disponível em: <https://ihl-databases.icrc.org/ihl/INTRO/440>. Acesso em 08/10/2021

_____. Assembleia Geral. **Resolução n. 3.314 (XXIX)**, Nova Iorque, 14 dez. 1974. Disponível em: <https://undocs.org/en/A/RES/3314(XXIX)>. Acesso em 05 de out. 2021.

_____. UN Office for Disarmament Affairs. c2022a. **Group of Governmental Experts**. Disponível em: < https://www.un.org/disarmament/group-of-governmental-experts/>. Acesso em 11 de jun. 2022.

_____. UN Office for Disarmament Affairs. c2022b. **Open-ended Working Group on security of and in the use of information and communications technologies**. Disponível em: <https://meetings.unoda.org/meeting/oewg-ict-2021/>. Acesso em 15 de jun. 2022.

_____. UN Office for Disarmament Affairs. c2020. **UK response to Chair's initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security**. Disponível em: <https://www.un.org/disarmament/open-ended-working-group/ >. Acesso em 29 de out. 2021.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). Comissão Jurídica Interamericana. **CJI/RES. 260 (XCVII-O/20)**. [s.l.], 7 ago. 2020a, p. 1-2. Disponível em: <https://www.oas.org/en/sla/iajc/docs/direito_internacional_e_operacoes_ciberneticas_do_estado_publicacion.pdf>. Acesso em 11 de jun. 2022.

_____. Comissão Jurídica Interamericana. **Direito Internacional e Operações Cibernéticas do Estado:** Melhoria da Transparência – Quinto Relatório. [s.l.], 7 ago. 2020b, p. 3-35. Disponível em: <https://www.oas.org/en/sla/iajc/docs/direito_internacional_e_operacoes_ciberneticas_do_estado_publicacion.pdf>. Acesso em 11 de jun. 2022

_____. Comissão Jurídica Interamericana. c2022a. **Current Agenda**. Disponível em: <https://www.oas.org/en/sla/iajc/current_agenda.asp>. Acesso em 11 de jun. 2022.

_____. c2022b. **Segurança Cibernética**. Disponível em: <https://www.oas.org/pt/topicos/seguranca_cibernetica.asp>. Acesso em 14 de jun. 2022.

PARET, Peter. The Genesis of On War. IN: CLAUSEWITZ, Carl von. **On War**. Princeton University Press, 1989. p. 1-25.

PASSOS, Rodrigo Duarte Fernandes dos. Maquiavel e Clausewitz: da arte da guerra à política por outros meios. IN: SALATINI, Rafael; DEL ROIO, Marcos. **Reflexões sobre Maquiavel**. Marília: Cultura Acadêmica, 2014, p. 145-156. Disponível em: < https://www.researchgate.net/publication/269818847_Maquiavel_e_Clausewitz_Da_arte_da_guerra_a_politica_por_outros_meios>. Acesso em 14 de jul. 2021

PETITEVILLE, Franck.; SMITH, Andy. Analyser les politiques publiques internationales. **Revue Française de Science Politique**. [S.l.], vol. 56, no. 3, 2006. p. 357-366. Disponível em: <https://doi.org/10.3917/rfsp.563.0357>. Acesso em 28 de mai. 2022.

PICTET, Jean. **Humanitarian Law and the Protection of War Victims**. Geneva: Henry Dunant Institute, 1975.

PINHEIRO, Alvaro de Souza. A Tecnologia da Informação e a Ameaça Cibernética na Guerra Irregular do Século XXI. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, vol. 11, no. 18, 2018, p. 4-11.

PINTO, Danielle Jacon A.; PAGLIARI, Graciela de C.; GRASSI, Jéssica M (orgs.). **A Geopolítica das Estratégias em Defesa Cibernética**. 1 ed. Rio de Janeiro: Alpheratz, 2021.

POLÍCIA Civil investiga exibição de vídeo pornográfico para alunos do 6º ano durante aula online no DF. **Portal G1**, Distrito Federal, 07 de abril de 2021. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/2021/04/07/policia-civil-investiga-exibicao-de-video-pornografico-para-alunos-do-6o-ano-durante-aula-online-no-df.ghtml>. Acesso em 15 de set. 2021.

POLIDO, Fabrício Bertini Pasquot. Por que o Brasil deve urgentemente aderir à Convenção de Budapeste. **Revista Consultor Jurídico**, 5 de julho de 2021. Disponível em: <https://www.conjur.com.br/2021-jul-05/polido-brasil-urgentemente-aderir-convencao-budapeste>. Acesso em 22 de ago. 2021.

RAPOPORT, Anatole. Prefácio. IN: CLAUSEWITZ, Carl von. **Da Guerra**. São Paulo: WMF Martins Fontes, 2010. p. XI-LXXXVI.

REINO UNIDO. Ministério da Defesa. **Defence Technology Framework:** Defence Science and Technology. 9 sep. 2019. Disponível em: <https://www.gov.uk/government/publications/defence-technology-framework>. Acesso em 30 de out. 2021.

RID, Thomas. **Cyber war will not take place**. Oxford: Oxford University Press, 2013.

RIVIÈRE, Philippe. Iran's Stuxnet affair. **Le Monde diplomatique**. mar. 2011. Disponível em: <https://mondediplo.com/2011/03/09stuxnet>. Acesso em 22 de set. 2021.

SANDOZ, Yves; SWINARSKI, Christophe; ZIMMERMANN, Bruno (eds). **Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949**. International Committee of the Red Cross. Geneva: Martinus Nijhoff, 1987.

SASSÒLI, Marco. **International Humanitarian Law**: rules, controversies, and solutions to problems arising in warfare. Cheltenham: Edward Elgar, 2019.

SCHMITT, Michael N. Cybersecurity and International Law. IN: GEIß, Robin; MELZER, Nils. (eds.). **The Oxford Handbook of The International Law of Global Security.** Oxford: Oxford University Press, 2021a. p. 661-678.

_____. Foreign Cyber Interference in Elections. **International Law Studies**, Newport, vol. 97, no. 739, p. 739-764, 2021b. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3816748>. Acesso em 20 de set. 2021.

_____. International Humanitarian Law and the Conduct of Hostilities. IN: SAUL, Ben; AKANDE, Dapo (eds.). **The Oxford Guide to International Humanitarian Law**. 1st ed. Oxford: Oxford University Press, 2020, p. 147-174.

_____. Rewired warfare: rethinking the law of cyber attack. **International Review of the Red Cross**, vol. 96, no. 893, 2014a. p. 189-206.

_____. **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**. Cambridge: Cambridge University Press, 2017.

_____. The Law of Cyber Warfare: Quo Vadis?. **Stanford Law & Policy Review**, vol. 25, 2014b. p. 269-300.

_____; BILLER, J. The NotPetya Cyber Operation as a Case Study of International Law. **EJIL: Talk!**, 11 jul. 2017. Disponível em: <https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/>. Acesso em 22 de jan. 2022.

_____; FAHEY, Sean. WannaCry and the International Law of Cyberspace. **Just Security**, New York, 22 dec. 2017. Disponível em: <https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/>. Acesso em 13 de jan. 2022.

_____. Wired warfare 3.0: Protecting the civilian population during cyber operations. **International Review of the Red Cross**, vol. 101, no. 910, abr. 2019, p. 333-355. Disponível em: <https://international-review.icrc.org/articles/wired-warfare-30-protecting-civilian-population-during-cyber-operations>. Acesso em 14 de out. 2021.

SECCHI, Leonardo. **Políticas Públicas**: Conceitos, Esquemas de Análise, Casos Práticos. São Paulo: Cengage Learning, 1 ed., 2012.

SHAKARIAN, P., SHAKARIAN, J.; RUEF, A. **Introduction to cyber-warfare:** A multidisciplinary approach, Waltham: Syngress, 2013.

SILVA, Rodrigo Cardoso; SILVA, Eliza Odila Conceição. O Dilema do *Jus ad Bello* e *Jus in Bellum* na Guerra Cibernética: como aplicar o direito da guerra na era digital?. IN: JUBILUT, L. L.; et al. **Direitos Humanos e Vulnerabilidade e o Direito Humanitário**. Boa Vista: Universidade Federal de Roraima, 2019, p. 125-153.

SINGER, P.W.; FRIEDMAN, A. **Cybersecurity and cyberwar:** What everyone needs to know, Oxford: Oxford University Press, 2014.

SOSSAI, Mirko. International Disarmament and Arms Control. IN: GEIß, Robin; MELZER, Nils. (eds.). **The Oxford Handbook of The International Law of Global Security.** Oxford: Oxford University Press, 2021. p. 310-327.

STEED, Danny. The strategic implications of cyber warfare. IN: GREEN, James A. (ed). **Cyber Warfare:** a multidisciplinary analysis. New York: Routledge, 2016, p. 73-95.

STIENNON, Richard. A short history of cyber warfare. IN: GREEN, James A. (ed). **Cyber Warfare:** a multidisciplinary analysis. New York: Routledge, 2016, p. 7-32.

STINISSEN, Jan. A Legal Framework for Cyber Operations in Ukraine. IN: GEERS, K. (ed). **Cyber War in Perspective:** Russian agression against Ukraine. Tallinn: NATO CCDCOE Publications, 2015. p. 123-134. Disponível em: <https://ccdcoe.org/uploads/2018/10/Ch14_CyberWarinPerspective_Stinissen.pdf>. Acesso em 18 de jan. 2022.

SWANSON, Lesley. The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. **Loyola of Los Angeles International and Comparative Law Review.** Los Angeles, vol. 32, no. 2, 2010. p. 303-333.

THÜRER, Daniel. **International Humanitarian Law:** theory, practice, context. Hague Academy of International Law, 2011.

UKRAINE cyber-attack: Russia to blame for hack, says Kyiv**. BBC News Europe**. 14 jan. 2022. Disponível em: <https://www.bbc.com/news/world-europe-59992531>. Acesso em 17 de jan. 2022.

UNIÃO EUROPEIA (UE). Comissão Europeia. **Estratégia da União Europeia para a cibersegurança:** Um ciberespaço aberto, seguro e protegido. Bruxelas, 07 de fev. 2013. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013JC0001&from=EN>. Acesso em 20 de abr. 2022.

_____. Delegation of the European Union to the United Nations in New York. **EU Statement – United Nations Open-Ended Working Group on ICT:** Capacity-building. New York, 16 dez. 2021. Disponível em: <https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-united-nations-open-ended-working-group-ict-capacity_en?s=63>. Acesso em 20 de jun. 2022.

_____. Tribunal de Contas Europeu. **Desafios à eficácia da política de cibersegurança da UE:** Documento Informativo. Luxemburgo: março de 2019. Disponível em: <https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PT.pdf>. Acesso em 09 de jun. 2022.

VAN DEN BOOGAARD, Jeroen C. Fighting by the Principles: Principles as a Source of International Humanitarian Law. IN: MATTHEE, M.; TOEBES, B.; BRUS, M. (eds). **Armed Conflict and International Law:** In Search of the Human Face. The Hague: Asser Press, 2013, p. 3-31.

VISACRO, Alessandro. **A Guerra na Era da Informação**. São Paulo: Contexto, 2019.

WHETHAM, David; LUCAS JR., George R. The relevance of the Just War Tradition to cyber warfare. IN: GREEN, James A. (ed). **Cyber Warfare:** a multidisciplinary analysis. New York: Routledge, 2016, p. 160-173.

WIENER, Norbert. **Cibernética e Sociedade:** o uso humano de seres humanos. Tradução de José Paulo Paes. 2 ed. São Paulo: Editora Cultrix, 1965.

WIENER, Norbert. **Cybernetics:** or the control and communication in the animal and the machine. Massachussets: MIT - Massachusetts Institute of Technology, 1948.

GLOSSÁRIO

Ataque cibernético (ciberataque)

Em amplo aspecto, refere-se a todas as ameaças proferidas por meio do espaço cibernético, em qualquer escala.

No escopo do DIH, o Manual de Tallinn 2.0 oferece uma definição: "uma operação cibernética, seja ofensiva ou defensiva, na qual é razoavelmente esperado que se cause ferimento ou morte a pessoas ou danos ou destruição a objetos" (SCHMITT, 2017, p. 415, tradução nossa). Tal definição não é livre de controvérsias ou de discussões, especialmente sobre o que exatamente englobaria "danos ou destruição a objetos".

Ataque cinético

Refere-se aos ataques armados, nos termos do *jus in bello*, em que há uso de armas de força cinética (tradicionais, como bombas e mísseis) – quais sejam aquelas cujo dano ou destruição decorre da energia cinética (movimento).
À luz do PA I, art. 49 (1), os atos de violência (cinética), sejam eles ofensivos ou defensivos.

Atos de guerra

[...] todas as medidas de força que uma parte, usando instrumentos militares de poder, implementa contra outra parte em um conflito armado internacional. Estes incluem ações de combate destinadas a eliminar as forças armadas adversárias e outros objetivos militares. (GREENWOOD, 2008, p. 57, tradução nossa).

Cibernética

Refere-se à comunicação e controle, sistemas de comunicação, sua regulação e interação. Em específico, relativo aos recursos de Tecnologia da Informação e Comunicações, às ações provenientes de comandos a computadores, sistemas e infraestruturas que permitem a troca de informações. O uso do campo eletromagnético a partir de computadores ou dispositivos diversos

	ligados à tecnologia da informação, às redes, etc.
Espaço cibernético (ciberespaço)	"um domínio global dentro do ambiente da informação, cujo caráter distinto e único é moldado pelo uso da eletrônica e do espectro magnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas usando tecnologias de informação e comunicação" (KUEHL, 2009, p. 27, tradução nossa). Espaço virtual, onde constam dados digitalizados, como extensão da tecnologia informacional.
Guerra cibernética (ciberguerra)	Uso de operações cibernéticas em situação de conflito armado internacional. "Meios e métodos de guerra que consistem em operações cibernéticas equivalentes ou conduzidas no contexto de conflito armado, na acepção do DIH" (CICV, 2013, p.1, tradução nossa).
Guerra cinética (guerras "tradicionais")	Conflitos armados onde meios ou métodos tradicionais de guerra são usados; uso da força armada em sua acepção originária.
Infraestrutura cibernética	"Os dispositivos de comunicação, armazenamento e computação sobre os quais os sistemas de informação são constituídos e operam" (SCHMITT, 2017, p. 564, tradução nossa). Maiormente, o *hardware* e o *software*.
Infraestrutura crítica	"Sistemas e ativos físicos ou virtuais de um Estado que são tão vitais que sua incapacitação ou destruição pode debilitar a segurança, a economia, a saúde ou a segurança pública de um Estado ou o meio ambiente" (SCHMITT, 2017, p. 564, tradução nossa).

Meios de guerra	Refere-se às armas e seus sistemas associados.
Métodos de guerra	Refere-se às táticas, técnicas e procedimentos em que as hostilidades são conduzidas.
Objetivos militares	Segundo o art. 52 (2) do PA I, aqueles cuja "natureza, localização, destino ou utilização, contribuem efetivamente para a ação militar e assim sua distribuição total ou parcial, sua captura ou neutralização oferecem, nestes casos, uma vantagem militar precisa" (CICV, 2017, p. 40).
Objetos civis (bens civis)	Por critério negativo, aqueles que não coadunem como objetivos militares.
Operação militar	"Todos os movimentos e atos relacionados às hostilidades empreendidos pelas forças armadas" (SANDOZ; SWINARSKI; ZIMMERMAN, 1987, p. 597, tradução nossa). Tais atos podem ser de natureza ofensiva ou defensiva.
Operações cibernéticas	Operações militares com emprego de meios ou métodos cibernéticos.
Operações cinéticas	Operações militares com emprego de armas de energia cinética, ou de métodos onde o uso do ciberespaço não seja predominante.
Vítima	Aquele que sofre em consequência de um conflito armado.