ESCOLA DE GUERRA NAVAL

CC MARCIO JORGE DOS SANTOS

O DIREITO INTERNACIONAL E A GUERRA CIBERNÉTICA:

a aplicação do *jus ad bellum* e do *jus in bello na 5ª Dimensão da Guerra*.

Rio de Janeiro

2019

CC MARCIO JORGE DOS SANTOS

O DIREITO INTERNACIONAL E A GUERRA CIBERNÉTICA:

a aplicação do *jus ad bellum* e do *jus in bello na 5ª Dimensão da Guerra*.

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CMG (RM1-FN) Wagner da S. Reis

Rio de Janeiro
Escola de Guerra Naval
2019

AGRADECIMENTOS

À minha esposa Cristiane Will e ao meu filho Júlio Cesar pelo apoio incondicional que envolveu suportar, com paciência e amor, mais um período de ausência.

Ao CMG (RM1-FN) Wagner pelas valiosas orientações que balizaram o caminho da produção acadêmica.

Muito obrigado.

RESUMO

O objetivo deste trabalho é analisar o ordenamento jurídico da guerra e identificar se os seus artigos e cláusulas, tais quais redigidos, são suficientes para suportar as características particularmente disruptivas da Guerra Cibernética. A relevância do tema para as Forças Armadas evidencia-se quando são revisitadas as campanhas militares recentes e percebe-se que em todas, ao menos em alguma fase do conflito, houve o uso da Guerra Cibernética. Compreender as nuances jurídicas particulares que envolvem o seu emprego fornecerá aos planejadores ferramentas para explorar as suas potencialidades, sem agredir os Tratados Internacionais internalizados pelo Brasil. Para alcançar esse objetivo foi empregado um desenho de pesquisa contextual em que buscou-se entender as condições particulares da Guerra Cibernética, que dificultam a sua aplicação direta ao ordenamento jurídico da guerra, dentro do Direito Internacional Público. O trabalho apoiou-se na Carta das Nações Unidas e no Direito Internacional Humanitário como bases teóricas e procurou abordar o espaço cibernético em uma visão prioritariamente estatal de seu emprego. Foram confrontados os entendimentos jurídicos do conceito de legítima defesa e dos princípios da necessidade militar, humanidade, limitação, distinção e proporcionalidade, com as características da ciberguerra, sendo possível, ao fim, concluir que a Carta das Nações Unidas expressa-se plenamente suficiente para regular o *jus ad bellum* nos casos de Guerra Cibernética, e que no âmbito do *jus in bello*, há uma limitação parcial no alcance dos princípios da distinção e da proporcionalidade, em função da dificuldade de controle sobre a amplitude das consequências dos ataques cibernéticos, ressaltando-se, entretanto, não ser esta limitação, de tal ordem, que comprometa a atemporalidade e aderência do Direito da Guerra a qualquer dos domínios da guerra existentes ou ainda a serem concebidos.

Palavras-chave: Direito da Guerra. Guerra Cibernética. Legítima Defesa. Distinção. Proporcionalidade.

LISTA DE ABREVIATURAS E SIGLAS

C2	Comando e Controle
CICV	Comitê Internacional da Cruz Vermelha
CIJ	Corte Internacional de Justiça
DICA	Direito Internacional dos Conflitos Armados
DIH	Direito Internacional Humanitário
DIP	Direito Internacional Público
EUA	Estados Unidos da América
IDH	Índice de Desenvolvimento Humano
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence (Centro de Exceleência em Defesa Cibernética Cooperativa da OTAN)
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
SCADA	*Supervisory Control and Data Acquisition* (Sistema de Supervisão e Aquisição de Dados)
STIC2	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações
TPI	Tribunal Penal Internacional

SUMÁRIO

1 INTRODUÇÃO

O século XX foi um período de intensas transformações na sociedade dos homens. As mudanças, em todas as áreas do conhecimento, foram inúmeras e significativas.

No âmbito do Direito Internacional Público (DIP), o ramo do Direito da Guerra[1] foi um destes a sofrer muitas mudanças. Com o impulso dos flagelos gerados pelas guerras, em especial a II Guerra Mundial (1939-1945), observou-se o alvorecer do pensamento focado em uma jurisdição internacional que regulasse a guerra. A criação da Organização das Nações Unidas (ONU), em 1945, foi o ponto alto dessa ideia e o seu texto constitutivo traduz este direcionamento na medida em que tem a manutenção da paz como esteio.

Esta evolução do ordenamento jurídico afeto à guerra convergiu ainda para o estabelecimento de uma série de princípios que, somados aos seus protocolos adicionais, ficaram enfim consagrados como o Direito Internacional Humanitário (DIH). Destinado ao disciplinamento normativo da condução das hostilidades, o DIH trouxe, por fim, humanidade à guerra.

Entretanto, com o passar dos anos, um novo fato nesta corrente de transformações veio causar disruptura na abrangência desse arcabouço jurídico. O desenvolvimento dos computadores e da internet fez surgir uma realidade em que o horizonte é, ao mesmo tempo, desconhecido e ambíguo em suas potencialidades. As ferramentas que tanto facilitam a vida e o trabalho das pessoas também se prestam ao combate. Em suma, o desenvolvimento tecnológico trouxe, a partir do final do século XX e início do século XXI, a 5ª dimensão da guerra[2]: a guerra cibernética. Uma nova modalidade de combate, com características únicas, que transcende os conceitos tradicionais de fronteiras e corrompe o entendimento da temporalidade e alcance de um ataque.

1 Para melhor contextualização, ver APÊNDICE.

2 A literatura internacional nos apresenta as chamadas "dimensões da guerra", inicialmente em um total de três: a guerra naval, a guerra aérea e a guerra terrestre. Durante a Guerra Fria (1947-1989) observou-se o surgimento da 4ª dimensão, a guerra espacial e atualmente presencia-se a consolidação da 5ª dimensão, a guerra cibernética.

Essa nova realidade traz interpretações difusas uma vez que, se por um lado a conceituação do que é Guerra Cibernética não se consolidou ainda como uma categoria de análise da Ciência Política e das Relações Internacionais, por outro o potencial militar da Guerra Cibernética está no despertar do desenvolvimento de suas capacidades. Nesse sentido, essa nova dimensão da guerra poderá ensejar novas interpretações do DIH, a criação de regras adicionais ou mesmo uma nova legislação inteira específica para regular a condução do combate cibernético dos conflitos armados.

Sem a pretensão de ser uma obra técnica no âmbito do espaço cibernético, serão evitadas abordagens detalhadas sobre as questões tecnológicas, que não as eminentemente necessárias para a contextualização da Guerra Cibernética frente ao Direito da Guerra.

Por conseguinte, utilizando como arcabouço teórico a Carta das Nações Unidas e outros instrumentos internacionais, fontes do DIH, e a melhor doutrina, este trabalho se propõe a alcançar o objetivo de analisar o ordenamento jurídico da guerra e identificar se os seus artigos e cláusulas, tais quais redigidos, são suficientes para suportar as características particularmente disruptivas da Guerra Cibernética e, a partir de um desenho de pesquisa contextual, responder a seguinte questão de pesquisa: "Em que proporção a Carta das Nações Unidas e o DIH estabelecem fundamentação jurídica suficiente para regular as ações dos Estados no *jus ad bellum*[3] *e no jus in bello*[4], nos casos de Guerra Cibernética?". Para tal, além desta introdução, esta obra foi organizada em mais quatro capítulos que serão brevemente apresentados nos próximos parágrafos.

O segundo capítulo se debruçará sobre o Direito da Guerra com foco nos aspectos

3 "Direito da Guerra" ou "Direito do uso da força". Segundo o Comitê Internacional da Cruz Vermelha (CICV) é afeto a limitação do recurso do uso da força entre os Estados, conforme previsto no artigo Art. 2º, para. 4º da Carta das Nações Unidas que estabelece que os Estados devem abster-se de ameaçar ou usar a força contra a integridade territorial ou a independência política de outro Estado. As exceções serão apresentadas no capítulo 2.

4 "Direito na Guerra". No entendimento do CICV, regula os aspectos do conflito que são de preocupação humanitária, limitando o sofrimento causado pela guerra. Aborda a realidade de um conflito sem considerar os motivos ou a legalidade de recorrer à força, e suas disposições se aplicam às partes beligerantes independentemente do motivo para o conflito ou da causa defendida pelas partes.

fundamentais que permitirão a compreensão referente ao direito de um Estado iniciar um conflito armado e a condução das hostilidades em si, a fim de que sejam estabelecidas as bases teóricas que sustentarão o objetivo maior de contextualizar a Guerra Cibernética no ordenamento jurídico internacional.

O terceiro capítulo versará sobre a Guerra Cibernética. Serão apresentados conceitos e definições importantes ao seu entendimento, uma análise da questão do paradigma do desenvolvimento digital e uma contextualização sobre como os Estados entendem e empregam a Guerra Cibernética. Permeado de casos reais exemplificativos, o capítulo pretende expor o que de fato é tão específico nesta nova modalidade de combate a ponto de levantar interrogações sobre a validade do emprego do ordenamento jurídico em vigor.

Após isso, espera-se que no quarto capítulo seja possível trazer a tona, primeiramente, um confronto entre a guerra cibernética e o *jus ad bellum*, abordando as questões de soberania, atividades preparatórias para o combate (como as de inteligência) e legítima defesa; e, posteriormente, uma análise mais aprofundada sobre a guerra cibernética e o *jus in bello*, expondo os problemas principais da distinção e da proporcionalidade na seleção de alvos e danos colaterais.

Por fim, os principais e mais importantes aspectos desta obra serão consolidados em uma conclusão que refletirá a compreensão obtida sobre a proporção do alcance do *jus ad bellum* e do *jus in bello* para a regulação das ações dos Estados, no combate cibernético.

O tema reveste-se de relevância para as Forças Armadas quando observa-se que as campanhas militares recentes, em alguma fase do conflito, contaram com ações de Guerra Cibernética. Compreender as nuances jurídicas particulares que envolvem o seu emprego trará aos planejadores, em todos os níveis, ferramentas para explorar as suas potencialidades, sem ferir os Tratados Internacionais internalizados pelo Brasil.

2 DO DIREITO DA GUERRA

A guerra sempre fez parte da realidade dos homens. Ao longo do tempo o ser humano guerreou por sobrevivência, por território, por religião, por ideologia. E o fez de forma bárbara. Os níveis de violência observados sempre foram elevados. Um mundo de paz plena, com ausência de conflitos, nunca foi uma realidade. Em prol de seus interesses, indivíduos subjugaram outros indivíduos. Ao evoluir para as sociedades tribais e, posteriormente, para as grandes civilizações, reinos e impérios; nada mudou: tribos passaram a subjugar outras tribos, impérios passaram a subjugar impérios. A partir do Tratado de Westfália (1648) e o surgimento do Estado Moderno, os conflitos passaram a estar cada vez mais organizados e abrangentes, com exércitos nacionais mais bem treinados e preparados. Tal evolução foi sentida diretamente também nos meios e métodos de guerrear. Se no início os homens lutavam com as mãos, rapidamente aprenderam que a lança poderia ser muito mais efetiva. Forja e espadas, pólvora e armas de fogo, química e armas biológicas. A engenhosidade humana potencializou a capacidade de causar dor e sofrimento. A recente evolução computacional e informacional remete novamente a este cenário no contexto da Guerra Cibernética.

Mas os novos Estados soberanos não evoluíram somente em seus métodos e formas de guerra: a crescente interação comercial, econômica e cultural fazia surgir entre eles a necessidade de regras que orientassem suas relações. Os acordos se tornavam cada vez mais frequentes e necessários, ao passo que os Estados entendiam a nova realidade mundial. A consolidação do conceito de soberania vagarosamente fez os Estados caminharem para a produção de mecanismos que regulassem e fornecessem alguma garantia ao produto de suas interações. Não foi diferente com os conflitos armados.

Neste capítulo será feita a análise de um dos ramos do DIP, o Direito da Guerra, a fim de identificar as bases teóricas úteis ao avanço para o objetivo de contextualizar o

regramento jurídico internacional aplicável à guerra cibernética. Para tal, na primeira seção serão vistos os fatos e acontecimentos que conduziram a sociedade dos homens até a confecção dos dois principais instrumentos jurídicos, que atualmente regulam o fenômeno da guerra: a Carta das Nações Unidas, no tocante ao Direito dos Estados de ir a guerra, e o Direito Internacional Humanitário (DIH) no que se refere, de fato, à condução das hostilidades. Nas duas seções seguintes pretende-se propor um olhar ainda mais detalhado sobre os instrumentos jurídicos supracitados, destacando suas particularidades nos aspectos que guardam relevância com as questões suscitadas pela Guerra Cibernética.

Ao término, espera-se que estejam consolidados os aspectos relevantes atinentes ao Direito da Guerra que servirão de fundamentação para a análise necessária à contextualização da 5ª dimensão da guerra junto ao *jus ad bellum* e ao *jus in bello.*

2.1 A CONSOLIDAÇÃO DO DIREITO DA GUERRA: DE GENEBRA A ROMA.

"Para o correto conhecimento […] do direito internacional, é indispensável o estudo histórico de sua evolução" (ACCIOLY; SILVA; CASELLA, 2008, p.24), pois "as leis da guerra são tão antigas como a própria guerra, e a guerra, tão antiga quanto a vida na Terra" (Pictet[5], 1997, *apud* FERNANDES, 2006, p.23). Nesse contexto, apresenta-se um delineamento histórico sintético de como os povos agregaram, de forma distinta, suas contribuições ao direito consuetudinário da guerra: "os sumérios combatiam (…) respeitando regras como a declaração de guerra, a imunidade parlamentar e o tratado de paz. Os egípcios reconheciam a necessidade de se tratar o oponente com clemência, dando-lhe alimentos, roupas e remédios" (FERNANDES, 2006, p. 24).

Além dessas e de outras contribuições dos costumes, houve pensadores que teorizaram a questão da guerra e da legalidade. Dentre eles são relevantes: Santo Agostinho e

5 PICTET, Jean S. *Desarrollo y principios del Derecho Internacional Humanitário*. 2. ed. Santafé de Bogotá: Tercer Mundo, 1997.

São Tomáz de Aquino, que difundiram o entendimento do conceito de Guerra Justa[6]; Hugo Grócio que, por sua vez, agregou restrições à conduta da guerra, que atualmente integram normas do DIH; e Jean-Jacques Rousseu que rebateu o conceito de Guerra Justa e formulou a base, a partir do seu entendimento do "soldado cidadão", daquela que talvez seja hoje a maior contribuição do DIH, a diferenciação entre o combatente e o não-combatente.(ACCIOLY; SILVA; CASELLA, 2008; BEST, 1994)

Contudo, apesar das contribuições históricas da Idade Antiga, Idade Média e Idade Moderna, foi apenas na Idade Contemporânea que o Direito da Guerra se consolidou. A forma de início, de condução e, principalmente, as consequências da Grande Guerra (1914-1918) e da II Guerra Mundial foram determinantes para tal consolidação. Nesse contexto as grandes convenções internacionais de Genebra (1864, 1925, 1949 e 1977) e Haia (1899, 1907 e 1954), e os pactos da Liga das Nações (1919) e de Briand-Kellog (1928), foram os grandes fóruns para discussão e aprofundamento do tema, e permitiram amalgamar todo esse ordenamento jurídico para o estabelecimento dos quatro pilares do Direito da Guerra: o direito de Genebra, o direito de Haia, o direito de Nova Iorque e o direito de Roma. Segundo Fernandes (2006) o direito de Genebra está para a proteção às vítimas de combate, tal qual o de Haia está para as restrições à condução das hostilidades; e assim como o Direito de Nova Iorque pode ser traduzido nos direitos humanos nos conflitos armados, o de Roma está expresso no Tribunal Penal Internacional (TPI).

Outrossim, há uma relação estreita entre estes quatro pilares. No eixo Genebra -Haia, ao serem examinadas as convenções, "comprova-se que não existe nenhuma linha divisória claramente definida […], senão que se trata de uma continuidade de normas,

6 Conforme entendem Accioly, Silva e Casella, (op. cit.), a "Guerra Justa" seria um conflito armado legitimado por uma justa causa. Concebida pelos seguidores romanos do estoicismo, foi retomada por Santo Agostinho e São Tomás de Aquino, na Idade Média e por Francisco Vitória e Francisco Soarez, na Idade Moderna.

agrupadas sob dois nomes distintos" (BUGNION, 2001, tradução nossa)[7]. Este elo reaparece no direito de Nova Iorque que "contribuiu para a confluência do direito de Genebra e do direito de Haia – já que se ocupou de questões relativas à salvaguarda de vítimas e aos meios e métodos de combate –, além de acrescentar novos aspectos à normativa humanitária […]" (FERNANDES, 2006, p. 39). Da mesma forma, no direito de Roma esta ligação volta a surgir, uma vez que "o direito de Nova Iorque contribui decisivamente para o aparecimento do TPI" (FERNANDES, 2006, p. 39).

Portanto, conclui-se que a partir da consolidação de tal compêndio legislativo, passou a estar limitado o uso da força para a solução de controvérsias e a condução da guerra recebeu leis derivadas do direito consuetudinário internacional e dos tratados internacionais. As partes signatárias se comprometiam a obedecer os princípios básicos da necessidade militar e da humanidade, de modo que só fossem conduzidas as hostilidades suficientes para a derrota do oponente, vedando as ações que causassem sofrimentos ou perdas desnecessárias. Ao longo da segunda metade do século XX notou-se um Conselho de Segurança das Nações Unidas (CS) atuante (mesmo que de forma controversa em alguns momentos) e o aumento da cobertura do manto desta segurança jurídica às pessoas com status de não-combatentes e aos bens protegidos.

Apesar da existência da Carta das Nações Unidas e do DIH não serem, por si só, suficientes para impedir violações aos seus textos, é fato que os Estados têm agora limitações nas condicionantes para usar a força, os crimes de guerra estão tipificados e há um Tribunal específico, previamente constituído e com credibilidade para os seus julgamentos.

Após essa contextualização sobre a evolução do Direito da Guerra, as próximas seções trarão um maior aprofundamento sobre os mecanismos do Direito Internacional que servirão de suporte teórico para este trabalho, inciando pela Carta das Nações Unidas.

---

7 Texto original em espanhol: "Si se examina la distinción entre el derecho de Ginebra y el derecho de La Haya, se comprueba que no existe ninguna línea divisoria claramente definida entre esas dos normativas, sino que se trata de un *continuum* de normas, agrupadas bajo dos nombres distintos."

2.2 CARTA DAS NAÇÕES UNIDAS

Antes da adoção da Carta das Nações Unidas, em 1945, o direito internacional impunha poucos limites ao recurso às armas. Esta percepção era decorrente da concepção reinante da inevitabilidade do fenômeno da guerra. Sobre isso, Ávila e Rangel (2009, p. 118) já identificavam que era pacífica a ideia de que "a guerra era algo que deveria ser esperado tal qual uma praga ou um desastre natural […]. Assim, era necessária não uma legislação internacional proibindo-a, mas, sim, uma normatização e uma prática que inibissem seus excessos". Dessa forma, por muitos anos a guerra foi compreendida como algo extralegal, extrajudicial. O direito não poderia conformá-la (DINSTEIN, 2004).

Se por um lado o status jurídico da guerra pendia para o reforço da soberania estatal e confirmava a afirmação de que o exercício do direito de ir à guerra era a mais plena demonstração do poder de um Estado, por outro, tal instabilidade desequilibrava o sistema internacional e causava receios a uma corrente cada vez maior de interessados em promover o desenvolvimento de um Direito Internacional que regulasse as relações estatais conflituosas. Enfim, sendo a guerra um fenômeno social, *ubi societas, ibi jus.*[8]

A Carta das Nações Unidas foi de fato a concretização do desejo dos povos que, "resolvidos a preservar as gerações vindouras do flagelo da guerra, que por duas vezes, no espaço da nossa vida, trouxe sofrimentos indizíveis à humanidade" (NAÇÕES UNIDAS, 1945), estabeleceram pelo Artigo 2 (4), que o uso da força é proibido. Os Estados poderiam empregar a força somente no exercício do direito inerente de legítima defesa individual ou coletiva, ou sob a autoridade de um mandato do Conselho de Segurança (FLECK, 2008). Ao mesmo tempo em que proibia o uso da força, a Carta apresentava as duas exceções em que seu emprego poderia ocorrer.

Neste momento é preciso analisar o termo "força". Ele deve ser entendido de

8 Onde há sociedade, há direito.

forma ampla. Naturalmente, a força com o adjetivo “armada” está abarcada, o que não significa que outras formas de “força” não estão. As pressões diplomáticas, econômicas, psicológicas, ou outras formas de boicote, apesar de não estarem transcritas literalmente, devem ser consideradas. Dinstein ajuda a elucidar este entendimento quando observa que a solução para esta questão reside na legalidade: “para uma ameaça ser ilícita, a força por si própria deve ser ilegal”. (DINSTEIN, 2004, p.122)

Neste contexto, cabem ainda duas observações que evidenciam a natureza diferenciada da Carta: primeiramente a questão de que o seu texto expressa claramente precedência sobre qualquer outro tratado, indicando que nenhum Estado pode arvorar-se de suas cláusulas. Por fim, “também é de opinião geral que a norma consuetudinária que proíbe o emprego da força, cristalizada na Carta da ONU, adquiriu status de *jus cogens*[9]” (BYERS, 2007, p. 17).

Após esta contextualização, avançar-se-á aos pontos determinantes para este trabalho no que se refere ao direito de um Estado iniciar a guerra: as exceções a proibição do uso da força. Elas serão, com efeito, os objetos suscitadores de questionamentos e interpretações difusas da Guerra Cibernética perante o *jus ad bellun*. Por conseguinte, é fundamental a compreensão das suas nuances.

2.2.1 A legalização do uso da força: a legítima defesa e a autorização do Conselho de Segurança

Inicialmente, apreciar-se-á dois artigos da Carta das Nações Unidas que apresentam considerações sobre as exceções ao uso da força:

> A fim de assegurar pronta e eficaz ação por parte das Nações Unidas, seus membros conferem ao Conselho de Segurança a principal responsabilidade na manutenção da paz e da segurança internacionais e concordam em que no cumprimento dos deveres impostos por essa responsabilidade o Conselho de Segurança aja em nome deles. (NAÇÕES UNIDAS, 1945)

9 Normas derivadas do direito consuetudinário que adquiriram condição de natureza imperativa, mesmo que não contidas em tratados. Estão entre elas as proibições de genocídio, escravidão e tortura.

> Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais. (NAÇÕES UNIDAS, 1945)

Percebe-se que não há definição sobre o que é legítima defesa de fato ou quais seriam os critérios que levariam o Conselho de Segurança a decidir por agir. Tal subjetividade, antes de ser entendida como negligência, deve ser entendida como proposital. A tentativa de definições precisas neste campo não tem sido bem-sucedidas.

Por outro lado, esta subjetividade cobra seu preço quando observa-se que tanto a autorização do Conselho de Segurança quanto à legítima defesa são instrumentos jurídicos que carregam paradigmas entre a legalidade e o poder. Conforme explicam Brigagão e Júnior (2004), a definição do que é um motivo real para uma reação com o uso da força pode ser vista como “volátil” a depender dos atores envolvidos. Tal condição está diretamente ligada ao poder. Quanto maior for o poder do ator envolvido, maior será a sua capacidade de reescrever o entendimento do ordenamento jurídico de forma a torná-lo favorável às suas intenções, seja influenciando as decisões do Conselho de Segurança, seja valendo-se do direito de legítima defesa de forma questionável. Isso é parte do Sistema Internacional e seria de pouco rigor crítico acreditar que todos os Estados relacionam-se em pé de igualdade.

Com relação a legítima defesa, esta situação se torna mais agravante quando vista sob a ótica da legítima defesa coletiva. De foma mais prática: quando um Estado sai “em defesa” de um ou mais Estados, normalmente há interesses outros além da pura vontade de frear uma suposta injustiça. Interesses ideológicos, econômicos, políticos ou religiosos, por exemplo, podem vir antes da promoção da paz.

Exemplos recentes desta relação frágil entre o direito de fazer a guerra e o poder podem ser observados no contexto da chamada “Guerra ao Terror” promovida pelos Estados

Unidos da América (EUA) após os ataques, cuja autoria foi reivindicada pelo grupo Al-Qaeda, ocorridos em 11 de setembro de 2001. A alegação de legítima defesa individual e coletiva para a quebra da soberania do Afeganistão e de Estados vizinhos, na busca pelos arquitetos dos ataques, foi facilmente aceita face ao impacto dos ataques ao World Trade Center na percepção de ameaça do ocidente. Não houve autorização do CS para a coalização liderada pelos EUA inciarem, em 07 de outubro de 2001, a invasão do Afeganistão. Mas o fato é que, apesar de todo o imbróglio jurídico, ela ocorreu, evidenciando a questão do poder e dos interesses como mecanismos de manipulação da legalidade que envolve a ida de um Estado à guerra.

Uma outra dinâmica particular da legítima defesa é, via de regra, identificável em todos os conflitos. Invariavelmente as partes envolvidas num conflito, sejam em caráter individual ou coletivo, avocam a legítima defesa. Logo, suas reivindicações são mutuamente exclusivas (DINSTEIN, 2004). Significa dizer que um dos beligerantes está sendo autêntico e o outro dissimulado. Dito isso, cabe a pergunta: quem estará de fato sendo verdadeiro? A relatividade da verdade se fará presente e o poder dos beligerantes de influenciar a opinião pública será determinante. Havendo a permanência dessa postura, torna-se necessária uma heterocomposição para estabelecer quem se encontra no verdadeiro exercício da legítima defesa, remetendo mais uma vez ao CS.

Por fim, cabe uma última observação sobre a legítima defesa, reforçando o aspecto de que ela é de direito, não de obrigação. É uma opção recorrer a um contra-ataque, não um dever. Um Estado pode abster-se desse direito caso assim o deseje. Por acreditar ser inferior ou por qualquer outro motivo.

Feita essa contextualização sobre a Carta das Nações Unidas e os aspectos legais de se fazer a guerra, cabe uma consideração: uma vez iniciada a guerra, qual a legalidade envolta na sua condução? Este será o tema da próxima seção.

2.3 DIREITO INTERNACIONAL HUMANITÁRIO

"Direito Internacional Humanitário", "Direito Humanitário (DH)" ou "Direito Internacional dos Conflitos Armados (DICA)" são sinônimos encontrados na literatura. Na Academia, nas Organizações Internacionais e nos Estados as duas primeiras modalidades são mais observadas. Já nos meios militares é mais comum a aplicação da terceira modalidade. Entretanto, mais determinante do que a terminologia é a abrangência do DIH. Ele tem aplicação igualitária sobre todos os Estados envolvidos em um conflito armado. Independente de qual das partes foi a responsável pelo início das hostilidades. O DIH abrange todo o conjunto de leis que servem à proteção do homem em conflitos armados. Swinarski cunhou uma definição mais completa:

> O direito internacional humanitário é o conjunto de normas internacionais, de origem convencional ou consuetudinária, especificamente destinado a ser aplicado nos conflitos armados, internacionais ou não-internacionais. E que limita, por razões humanitárias, o direito das Partes em conflito de escolher livremente os métodos e os meios utilizados na guerra, ou que protege as pessoas e os bens afetados, ou que possam ser afetados pelo conflito. (SWINARSKI, 1996, p. 8)

A análise de Krieger (2004) sobre esta definição identifica a aplicação do DIH em quatro tipos de ações complementares: ações preventivas, ações reparadoras, ações de intervenção e ações punitivas. Preventivas quando atreladas ao desenvolvimento e estudo deste ramo do direito internacional e a sua aplicação pelos combatentes; reparadora para as vítimas quando trabalha na redução das consequências de sua violação; intervencionista quando tem foco na cessação imediata de violações em curso; e punitiva por ocasião da apuração e aplicação de sanções aos culpados.

Para cumprir tais ações o DIH é pautado sobre princípios derivados, em sua maioria, dos costumes do direito internacional consuetudinário e que depois foram positivados através dos tratados, protocolos multilaterais e convenções humanitárias. A observância de tais princípios é a garantia mínima de que, em tempos de conflito armado,

haverá proteção para as pessoas que não participam ou que tenham deixado de participar diretamente das hostilidades, além da promoção da restrição igualitária entre os meios e métodos de guerra. Nesta obra os princípios do DIH serão apesentados conforme a seguinte terminologia: humanidade, necessidade militar, proporcionalidade, distinção e limitação.

Nas próximas três subseções ver-se-á o aprofundamento do entendimento dos princípios do DIH, a ampliação da compreensão do conceito de "objetivo militar", e a apresentação da "cláusula Martens" e do "Manual de Tallin"; concluindo assim a inserção no arcabouço jurídico com o qual será contextualizada a guerra cibernética na seção 4.

2.3.1 Os princípios do DIH

Conforme afirma Bandeira de Mello, "o princípio é um mandamento nuclear de um sistema, disposição fundamental que se irradia sobre diferentes normas […] servindo de critério para a sua exata compreensão e inteligência, exatamente para definir a lógica e racionalidade do sistema normativo […] (MELLO, 2015, p. 54). Internalizada essa compreensão da profundidade dos princípios para o entendimento jurídico, será visto a seguir como estes estão inseridos no DIH.

Além das próprias codificações encontradas no Protocolo Adicional I de 1977, o "Manual de Emprego do Direito Internacional dos Conflitos Armados nas Forças Armadas – MD34-M-03", publicado pelo Ministério da Defesa do Brasil, em 2011, apresenta definições sobre os princípios do DIH, e Krieger avança no detalhamento destes princípios. A partir destas três referências seguir-se-á no entendimento dos princípios do DIH.

O princípio da **Humanidade** trata de, indistintamente e em todas as circunstâncias, evitar e aliviar o sofrimento humano por meio da proteção à vida e do respeito ao ser humano em sua nacionalidade, raça, religião ou aspectos políticos. (KRIEGER, 2004)

Por sua vez, o princípio da **Necessidade Militar** passa por limitar as ações

militares a um objetivo cujo ataque apresente o menor perigo para as pessoas civis ou bens de caráter civil. (KRIEGER, 2004) O uso da força deve corresponder à vantagem militar que pretende-se obter. A Necessidade Militar está diretamente ligada à escolha dos alvos e ao conceito de objetivo militar, que será visto na próxima seção.

O princípio da **Proporcionalidade** estabelece que os meios e métodos de guerra empregados devem ser proporcionais à vantagem militar concreta e direta (BRASIL, 2011). Em outras palavras, um ataque deve ser realizado somente se a vantagem militar for superior aos danos colaterais. Quaisquer alvos, inclusive militares, somente devem ser atacados se a dor e os prejuízos causados forem inferiores aos ganhos militares que se espera da ação.

Uma observação detalhada sobre esta definição permite concluir que, atualmente, uma dificuldade no estabelecimento do princípio da Proporcionalidade reside nas disparidades, notadamente as tecnológicas, existentes nas capacidades bélicas dos beligerantes. Se um Exército reage com carros de combate a um ataque desferido por uma tropa de infantaria convencional, em uma análise fria, isso não deveria ser motivo de crítica. Afinal, não há dolo em ter maior capacidade. Entretanto, se este contexto considerar que eram apenas 15 militares e que a reação causou mortes desnecessárias de 200 não-combatentes e a destruição de um bem protegido, tem-se aí uma clara violação ao princípio da proporcionalidade. Em suma, observa-se que relativizar o entendimento do que é "proporcional" ou do que é uma "vantagem militar superior" pode ser um caminho não ético para justificar descumprimentos deste princípio.

Já o princípio da **Distinção** tem sua ideia central apoiada na diferenciação clara e objetiva que os beligerantes devem ter entre combatentes e não-combatentes, e entre bens de caráter civil e objetivos militares (BRASIL, 2011). O cerne é assegurar o respeito e a proteção da população civil e os bens de caráter civil. Conforme pontua Krieger (2004, p. 251) "um dos grandes desafios do DIH é a efetiva proteção aos não-combatentes, pois estão cobertos de

uma gama de normas do DIH, mas são a maioria das vítimas nos conflitos armados da atualidade".

Guerras recentes, como a do Iraque (2003-2011), permitem observar que uma dificuldade para a aplicação do princípio da Distinção ocorre em conflitos em que um dos beligerantes não é uma força convencional estatal, como nos casos de insurgências, revoltas ou revoluções, principalmente em ambientes urbanos. Como distinguir combatentes de não-combatentes quando não há visualmente nada que os diferencie? O ônus dessa dúvida recai sobre a força estatal formalmente constituída, agregando complicadores ao planejamento e a execução das operações.

Por fim, o princípio da **Limitação** é afeto a escolha, pelos beligerantes, dos meios para causar danos ao inimigo. Este direito de escolha não é ilimitado. (BRASIL, 2011) É imperiosa a exclusão de armas, projéteis, materiais e métodos que levem ao sofrimento e danos desnecessários, inclusive danos extensos, duráveis e graves ao meio ambiente natural. Exemplos dessas armas proibidas são as minas terrestres, armas incendiárias e armas que causem cegueira. A lista completa pode ser encontrada no Protocolo Adicional I de 1977.

Mediante o exposto observa-se que o entendimento pleno e a aplicação dos cinco princípios do DIH são fundamentais para o alcance de uma "guerra humanizada", aquela em que os beligerantes conduziriam suas hostilidades sem causar sofrimento desnecessário. Antes de entender os princípios e o próprio DIH como limitadores ao combate, cabe ao bom planejador e ao bom combatente entender o propósito de cada linha do DIH e pautar seus planos e ações em conformidade ao arcabouço jurídico.

A fim de auxiliar neste entendimento, a próxima subseção trará uma abordagem mais detalhada sobre o conceito de "objetivo militar", termo recorrente durante a exposição dos princípios do DIH. Ele será útil para o confronto das particularidades da Guerra Cibernética com o arcabouço jurídico da guerra a ser realizado no capítulo 4.

2.3.2 Objetivo militar

Para efeito do DIH, a definição de objetivo militar pode ser encontrada no Artigo 52 do Protocolo Adicional I, de 1977: os "objetivos militares são limitados aos que, por natureza, localização, destino ou utilização contribuem efetivamente para a ação militar e assim sua destruição [...], captura ou neutralização oferecem [...] uma vantagem militar precisa" (BRASIL, 1993). Dessa definição retiram-se os dois elementos determinantes de um objetivo militar: a efetiva contribuição para a ação militar e o oferecimento de uma vantagem militar precisa.

A efetiva contribuição deve ser entendida como "efetiva" quando é de fato, não apenas potencial, e "contribuinte" de modo direto ou mesmo indireto para a ação militar. Para tal, um objetivo militar precisa atender ao menos uma das condições, expressas em formas de indicadores objetivos: a "natureza", ou seja, se o bem é militar ou civil; a "localização"; a "utilização", que representa o uso atual do bem; e o "destino", que expressa o uso futuro do bem.

Já o adjetivo "precisa", atrelado ao oferecimento de uma vantagem militar significa que esta vantagem deve ser concreta, não apenas possível.

Por ocasião da definição dos alvos, o planejador militar deverá considerar estes dois elementos a fim de concluir se um objetivo militar é legítimo ou não. A prática mostra que, uma vez que contribuam efetivamente para a ação militar do inimigo, e sua destruição, captura ou neutralização, ofereça vantagem militar precisa, alvos civis podem sim ser definidos como objetivos militares legítimos.

Melhor compreendidas as particularidades do conceito de objetivo militar, seguir-se-á para a última subseção que abordará outras ferramentas afetas ao entendimento do objeto de estudo, a Cláusula Martens e o Manual de Tallinn.

2.3.3 Perspectivas adicionais: Cláusula Martens e Manual de Tallin

Friedrich Von Martens foi o delegado russo nas Conferências de Paz de Haia de 1899. Ele fez constar, no preâmbulo da Convenção em Respeito ao Direito e Costumes da Guerra Terrestre, a cláusula que herdou seu nome:

> Até que um código mais completo das leis de guerra seja estabelecido, as altas partes contratantes consideram conveniente declarar que, em casos não incluídos nas regulamentações por elas adotadas, os civis e beligerantes permanecem sob a proteção e a regulamentação dos princípios do direito internacional, uma vez que estes resultam dos costumes estabelecidos entre povos civilizados, dos princípios da humanidade e dos ditames da consciência pública. (SCHINDLER; TOMAN, 2004, p. 61, tradução nossa)[10]

Em 1996, a Corte Internacional de Justiça (CIJ) emitiu um Parecer Consultivo relativo a "Legalidade do uso ou da ameaça de armas nucleares"[11] que evidenciou a importância da cláusula, ressaltando que ela é um meio efetivo de se abordar a rápida evolução da tecnologia militar. As palavras de Krieger (2004, p.245) de que a cláusula Martens é, "[…] em caso de lacuna do direito positivo, um caminho a ser trilhado para fins de proteção do ser humano junto ao DIH […]", reforçam este entendimento.

Ainda em 1996, a CIJ estabeleceu que o texto do Protocolo Adicional I seria uma visão moderna da cláusula, adaptada à realidade atual. Nessa nova redação tem-se que "nos casos não previstos no presente Protocolo ou em outros acordos internacionais, as pessoas civis e os combatentes permanecem sob a proteção e o domínio dos princípios do Direito Internacional". (BRASIL, 1993)

Assim, este instrumento jurídico do DIH apresenta-se adequado para emprego nos casos cibernéticos. Ele transcende as eventuais dificuldades de aplicação dos demais princípios, advindas das barreiras geradas pelas disparidades tecnológicas, e traz à razão o

10 Texto original em inglês: "Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience".

11 Disponível em <https://www.icj-cij.org/files/case-related/95/7497.pdf>. Acesso em 08 de agosto de 2019.

cerne do DIH: proteção as pessoas, sejam elas combatentes ou não-combatentes.

Em 2009, o Centro de Excelência em Defesa Cibernética Cooperativa da OTAN (NATO CCD COE, na sigla em inglês), baseado em Tallinn, capital da Estônia, convidou um grupo independente de especialistas para produzir um manual de leis aplicadas a guerra cibernética. O produto deste trabalho foi publicado em 2013 e traz um compêndio de 95 regras que abordam tópicos como soberania, responsabilidade do Estado, o *jus ad bellum*, o DIH e a lei da neutralidade. Cada regra é acompanhada de um comentário que explica a sua base legal, suas implicações práticas, a maneira como os especialistas interpretaram as normas aplicáveis no contexto cibernético e descreve as divergências ocorridas dentro do grupo quanto à aplicação de cada regra. (SCHMITT, 2013)

Em 2017 foi publicado o Manual de Tallinn 2.0 que ampliou a influência da primeira edição trazendo 154 regras que estenderam a cobertura da lei internacional que rege a guerra cibernética a regimes legais em tempo de paz. Embora o manual represente os pontos de vista dos especialistas, desta vez o projeto beneficiou-se da contribuição não oficial de muitos Estados e de mais de 50 revisores. (SCHMITT, 2017)

A despeito da qualidade de seus textos e de suas análises contundentes poderem se prestar a clarificação do entendimento de aplicabilidade legal do direito internacional nos casos de guerra cibernética, o Manual de Tallinn é um documento acadêmico não vinculativo e não constitui base legal por não ter força de um tratado reconhecido internacionalmente. Em virtude disso, não será considerado nesta obra como parte do arcabouço jurídico internacional para o ordenamento da guerra.

Dessa forma, foi apresentado o arcabouço que se prestará a contextualização jurídica da Guerra Cibernética a ser realizada na seção 4. Entretanto, permanece a carência de um melhor entendimento sobre as particularidades da Guerra Cibernética. Esta é a proposta para a próxima seção deste trabalho.

3 DA GUERRA CIBERNÉTICA

Se existe uma certeza quando se trata de Guerra Cibernética é a de que não há unanimidade no seu entendimento. Academia, militares, políticos e imprensa especializada digladiam-se sobre o que seria, de fato, a Guerra Cibernética e mesmo se o termo é adequado. Conforme afirma Carreiro (2012), questiona-se o emprego do termo guerra, afirmando que não se trata de uma dimensão da guerra; o uso exagerado do adjetivo cibernético atrelado a qualquer ocorrência de natureza tecnológica ou virtual; e a abrangência do seu alcance e das suas capacidades. James Lewis, do *think-thank* Center of Strategic International Studies; Howard Schmidt, coordenador de cibersegurança da Casa Branca em 2009; jornalistas como Mike Masnick, do Tech Dirt; e acadêmicos como Jerry Brito e Peter Sommer estão entre os mais proeminentes nestas críticas e questionamentos. Graham, R. (2010, tradução nossa)[12] acusa à crescente militarização da internet apontando o que chama de "absurdo técnico" do conceito de guerra cibernética: "O que me surpreende é que ninguém parece perceber que a guerra cibernética é uma história fictícia.[...] Colocar 'ciber' na frente de algo é só um meio para as pessoas compreenderem conceitos técnicos [...]". Realmente há exageros. Leigos, ou apenas pessoas ávidas por aumentar o alarde sobre o seu "produto", valem-se do adjetivo cibernético, ou do termo guerra cibernética (e suas derivações), indevidamente.

Os erros são compreensíveis. Com efeito, não há diferença entre o *modus faciendi* de uma invasão empreendida por um criminoso comum, a conta-corrente de uma pessoa qualquer, para furtar dinheiro, quando comparada à de um Estado contra o sistema de segurança de outro Estado, para obter dados de uma central nuclear, por exemplo. Ambas se valerão dos mesmos artifícios, em maior ou menor escala, com maiores ou menores consequências. Essa proximidade, normalmente é apontada como a causadora destes erros de

12 Texto original em inglês: "What astounds me is that nobody seems to realize that "cyberwarfare" is a fictional story […] Putting "cyber" in front a something is just way for people to grasp technical concepts [...]".

interpretação.

A despeito destas batalhas conceituais, ver-se-á neste capítulo que o que não se pode é minimizar ou negar a existência e a letalidade potencial da guerra cibernética. Há sim uma nova dimensão da guerra, a 5ª, e ela já é uma realidade. Quem primeiro a compreender e usá-la a seu favor terá vantagens no jogo de poder do sistema internacional.

A fim de evitar estes equívocos de entendimento, a primeira seção trará inicialmente conceitos e definições necessários para balizar como os termos devem ser compreendidos nesta obra. Na sequência será analisado o complexo paradigma do desenvolvimento cibernético e às suas consequências sobre as decisões estatais. Por fim, a terceira seção abordará o uso hodierno da guerra cibernética pelos Estados e como isso reflete a questão do poder. Ao término deste capítulo espera-se que estejam esclarecidos os aspectos da Guerra Cibernética necessários a este trabalho.

3.1 CONCEITOS E DEFINIÇÕES

Em 27 abril de 2007, sites do governo, dos bancos e dos jornais da Estônia sofreram uma série de pedidos de informações. Tal quantidade superou a capacidade dos servidores e interrompeu a infraestrutura estoniana de informações e serviços eletrônicos. Esse modo de ataque cibernético é conhecido como de negação de serviço (DDOS, na sigla em inglês) e a investigação posterior indicou que ele foi conduzido a partir de uma rede de computadores alojada em toda a sorte de países (que mal tinham a ideia de participar do episódio). A amplitude dos ataques combinados e a coordenação observada não eram comparáveis a qualquer outra ocorrência que algum Estado já houvesse sofrido. Essa foi a data do surgimento do que hoje se chama de Guerra Cibernética (TIKK; TALIHÃRM, 2010; NETO, 2017).

O parágrafo anterior apresenta termos como “ataque cibernético” e “guerra

cibernética". Adiante serão apresentadas as definições para estes e outros termos comuns a guerra cibernética.

Diversos autores, organizações e órgãos governamentais, de diversas nacionalidades, cunharam suas definições para a Guerra Cibernética. Cada uma delas guarda sua peculiaridade e não é escopo deste trabalho tentar definir qual seria a mais completa ou abrangente. O Ministério da Defesa brasileiro estabelece que a Guerra Cibernética "corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou **destruir** capacidades de C2[13] do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar" (BRASIL, 2015, grifo nosso). Uma análise dessa definição, feita com foco no verbo "destruir", evidencia a letalidade intrínseca da Guerra Cibernética e rebate os argumentos de Graham, R., anteriormente citados. E, se em um primeiro momento a definição pode indicar-se frágil quando limita a Guerra Cibernética ao contexto de um planejamento operacional ou tático, ou ainda a uma operação militar, uma vez que os exemplos demostram que as ações cibernéticas podem ser cumpridas a partir de uma necessidade estratégica (de uma informação, por exemplo), ou levadas adiante por entes não estatais; na verdade está sendo mais assertiva pois dirime os erros de interpretação que levam hacktivismo[14] ou espionagem a serem tratadas como Guerra Cibernética.

Aprofundando um pouco mais a análise, nota-se que a Guerra Cibernética compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Estas ações são comumente traduzidas como Ações Cibernéticas e a

13 Comando e Controle.

14 Hacktivismo é a "manipulação da informação digital a fim de promover uma mudança política ou social. Os atos de ativismo cibernético buscam resultados similares aos obtidos pelo ativismo regular ou atos de desobediência civil, por meio de ataques de negação de serviço ou protestos efetuados via alteração de sítios da Internet". (NUNES, 2015, p.59)

possibilidade de emprega-las está diretamente relacionada ao nível de dependência do inimigo às questões de TI, conforme será apresentado na próxima seção deste capítulo. (BRASIL, 2014)

Naturalmente, tais ações possuem caráter ofensivo ou defensivo, conforme a situação. Nunes (2015) sugere que ambas seriam realizadas por meio de redes de computadores e se diferenciariam no propósito. Ações Ofensivas de Guerra Cibernética visariam interromper, negar, degradar, corromper ou destruir a informação contida em computadores, redes e/ou sistemas de TI inimigos; e as Defensivas intencionariam proteger, monitorar, analisar, detectar e responder à atividade não autorizada em computadores e/ou redes, de modo a garantir o uso continuado e a inviolabilidade dos próprios sistemas de TI. Em suma, por meio de uma rede de computadores, atacar os recursos inimigos ou defender-se de ataques desferidos contra os próprios recursos.

Das definições acima depreende-se que tanto as Ações Ofensivas quanto as Defensivas possuem como alvo os sistemas de TI inimigos. Não poderia ser diferente: mesmo que o objetivo principal seja causar um efeito físico no mundo real, no ambiente cibernético este ataque estará limitado a alterar a estrutura de um determinado programa ou manipular dados e então, a partir daí, causar o efeito cinético. Dessa forma, o objetivo de primeiro nível de um ataque é o sistema de TI inimigo.

Tais Ações Cibernéticas ocorrem em um ambiente operacional muito particular, diferente em sua natureza e abrangência dos tradicionais ambientes terrestre, marítimo, aéreo e espacial. O Espaço Cibernético é o local no qual as Ações Cibernéticas se desenvolvem. Ele é altamente fluido e permeia todos os quatro outros ambientes operacionais. É um “espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas” (BRASIL, 2015). O Espaço Cibernético é um ambiente artificial, criado pelo homem e, por esta razão, sujeito a

alterações constantes. Da sua instabilidade característica derivam a incerteza e a não padronização dos resultados dos ataques cibernéticos que serão abordados no capítulo 4.

Considerando que o Espaço Cibernético é criação humana, não seria incorreto afirmar que todas as suas partes estão sob o controle de alguém. Há controle sobre cada uma das redes que são potenciais caminhos para uma arma cibernética atingir seu alvo. Não há rede sem "dono". Toda a informação trafegada pelo Espaço Cibernético está situada em uma rede de propriedade de alguém e que possui hospedagem em algum Estado do globo. (LEWIS, 2009). A questão reside na medida desse controle. Ele é limitado, não sendo possível supor que este alcance (do controle) ocorresse nos níveis observados nos demais ambientes. A soberania no Espaço Cibernético limita-se pela incapacidade de ser exercida na plenitude.

Na análise das causas desta limitação do controle percebe-se que a inexistência de fronteiras no Espaço Cibernético é uma responsável direta. Aprofundando mais essa abordagem, nota-se que no Espaço Cibernético não há a exigência de desembarcar o "soldado digital" na praia inimiga e que, pior, não há necessidade de proximidade física para o desenvolvimento das ações. Em outras palavras, as distâncias e as fronteiras inexistem.

Um segundo aspecto surge quando iluminam-se as consequências dos ataques cibernéticos em comparação aos provenientes dos embates ditos tradicionais. Ambos podem gerar desdobramentos sociais e políticos mundiais, vide os gerados pelos ataques nucleares de Hiroshima e Nagasaki ou pelo holocausto vivido pelos judeus na II GM. Mas o fato é que os danos físicos dos ataques cinéticos limitam-se, efetivamente, ao local onde ocorrem. Não é possível guardar tal certeza quando se trata de um ataque no Espaço Cibernético. A evolução tecnológica ainda é frágil no controle a proliferação de *worms* e *trojans*[15], por exemplo.

Com relação a essas ameaças cibernéticas, diversos autores se propuseram a

15 Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo, de computador para computador. Trojan é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.

estabelecer uma taxonomia. Nessa obra adotar-se-á como referência aquela desenhada por Cornish, Hughes e Livinsgtone (2009) que apresentam as ameaças cibernéticas divididas em quatro domínios: ataques cibernéticos patrocinados por Estados; extremismo ideológico e político; crimes graves e organizados; e crimes de baixo nível ou individuais (também conhecido pelo termo em inglês "*hacking*"). Apesar de as próprias descrições dos domínios, conforme cunhadas pelos autores, serem autoexplicativas, é salutar apresentar uma ampliação no entendimento, principalmente no que se refere ao domínio dos ataques patrocinados por Estados, enfoque principal deste trabalho.

Em linhas gerais, os quatro domínios de ameaças cibernéticas entregam uma ampla gama de riscos, frequentemente interligados, com os quais os responsáveis pela formulação de políticas de segurança devem lidar.

O *Hacking* é uma atividade de nível relativamente baixo e desorganizada, mas que pode ter consequências de alto nível e também se destaca por poder estar presente em outros domínios de ameaças.

O uso criminoso grave e organizado da infraestrutura global de tecnologia da informação e comunicações está, quantitativa e qualitativamente, aumentando a um custo considerável para a economia global.

Já os extremistas ideológicos e políticos encontraram na rede mundial de computadores o ambiente perfeito para a divulgação de suas ideias, cooptação e reivindicação de suas exigências. Esse domínio abrange os midiaticamente chamados "terroristas cibernéticos" e os "hacktivistas".

Finalmente, no nível de Estados e governos, observa-se o uso dual da rede: se por um lado ela é cada vez mais vista em termos diretos e familiares, como um ativo estratégico a ser explorado para fins de segurança nacional, por outro apresenta-se a ótica da rede como um campo de batalha, onde o conflito pode ser decidido (CORNISH; HUGHES;

LIVINGSTONE, 2009).

Nesse contexto, é normal o surgimento de um questionamento: seria razoável reduzir o nível de dependência tecnológica dos serviços e atividades de um Estado e assim diminuir as suas vulnerabilidades, ou a digitalização e a interatividade são um caminho sem retorno? Tal paradigma entre desenvolvimento tecnológico e vulnerabilidade será o tema da próxima seção.

3.2 O PARADIGMA DO DESENVOLVIMENTO DIGITAL

> De forma notável, os setores privados controlam perto de 90% da estrutura crítica dos EUA, e as firmas por trás deles usam o ciberespaço para, entre outras coisas, dosar os níveis de cloração da água da sua cidade, controlar o fluxo de gás que aquece sua casa, e executar as transações financeiras que mantém os preços estáveis. (SINGER; FRIEDMAN, 2017, p. 25)

O avanço tecnológico de um Estado é um indicador de seu nível de desenvolvimento social, econômico, educacional e industrial. Uma boa mensuração de como o Estado se relaciona com a tecnologia, como a emprega em seus processos, como oferece os seus serviços aos cidadãos, como insere a tecnologia na educação, no controle de suas indústrias e equipamentos de defesa, como aborda a pequisa e o desenvolvimento de novas tecnologias, como a sociedade usa a internet no dia a dia, do sistema bancário as redes sociais, pode indicar o quão avançado é o Estado e, por outro lado, o quão dependente do Espaço Cibernético ele o é.

Nesse contexto, há uma corrida silenciosa entre o desenvolvimento de aparatos de segurança digitais e formas de quebrar estas seguranças, gerando avanços contínuos nos "firewalls" e antívirus[16] ao mesmo passo que se percebe o desenvolvimento de maiores e mais poderosas ameaças. Como visto na seção anterior, a balança onde repousa a capacidade de controle ainda pende para o lado das ameaças. Constata-se que quanto mais "conectado" for

16 Firewall é um dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores. O antivírus é um tipo de ferramenta contra softwares maliciosos (malwares) desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código maliciosos.

um Estado, em todas as suas expressões de poder, maior impacto ele tenderá a sofrer em caso de ataque, pois há potencial para que mais estruturas sejam afetadas, que maiores danos sejam causados ao dia a dia da população e que ocorra uma infecção em grande escala.

Diversas organizações buscam fazer essa mensuração, cada uma com propósitos distintos. Anualmente a ONU divulga o Relatório de Desenvolvimento Humano contendo o Índice de Desenvolvimento Humano (IDH) de cada Estado. O Relatório consolida indicadores socioeconômicos e revela o grau de penetração da internet. Islândia, Noruega, Luxemburgo, Suécia e Dinamarca estão entre os Estados mais conectados do mundo, no relatório publicado em 2017[17]. Sob o enfoque econômico, o Global Connectivity Index[18], estudo divulgado anualmente pela Huawei, avalia a conectividade e o preparo para a economia digital. Nos dados de 2018, os EUA aparecem na liderança, seguidos por Cingapura, Suécia, Suiça e Reino Unido. Em uma tentativa de traduzir indicadores estatísticos diversos em níveis de poder, a consultoria britânica Portland divulga anualmente o seu ranking "The Soft Power 30"[19] em que apresenta os trinta Estados com maior *soft power*[20]. Dentre os indicadores utilizados para quantificar o poder está a capacidade de influenciação digital do Estado. Nos dados de 2018, os dez primeiros são, pela ordem, EUA, França, Reino Unido, Alemanha, Coréia do Sul, Canadá, Singapura, Japão, Suécia e Austrália.

Entretanto, mais importante do que os rankings em si, é conseguir depreender dos números o grau de dependência e penetração das redes nas infraestruturas de um Estado, principalmente nas chamadas infraestruturas críticas[21] (IC). De fato, essa não é uma abordagem simples pois ela carece de uma análise holística do problema, uma vez que características políticas, econômicas, sociais e culturais estarão diretamente ligadas à questão digital em tal análise.

17 Disponível em: <www.br.undp.org/content/brazil/pt/home/idh0.html>. Acesso em 01 de agosto de 2019.
18 Disponível em: <www.huawei.com/minisite/gci/en/index.html>. Acesso em 01 de agosto de 2019.
19 Disponível em: <www.softpower30.com>. Acesso em 01 de agosto de 2019.
20 Ver glossário.
21 Instalações, serviços, bens e sistemas que, se interrompidos ou destruídos, causarão grande impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade.

Diferente do que uma análise breve possa indicar, não se propõe que os Estados neguem o avanço tecnológico e mantenham-se obsoletos em nome de proteção contra ataques cibernéticos. O desenvolvimento cibernético deve sim ser buscado pois dele advirá maior produtividade, ganhos econômicos e melhorias sociais. Entretanto, crescer com segurança é uma aspiração que custa caro e drena recursos dos Estados. Essa corrida pelo desenvolvimento das capacidades de ataque e defesa cibernéticas pode, em menor escala, ser comparada a outras corridas armamentistas já observadas ao longo da história (SINGER; FRIEDMAN, 2017). A grande diferença desta vez é que hoje, não só um engenheiro militar está dedicando-se a descobrir vulnerabilidades de um possível oponente. Um jovem, do fundo de sua garagem, com recursos limitados e muita vontade, pode ser o primeiro a alcançar tal objetivo, tal qual apresentado no domínio da ameaça dos crimes de baixo nível. Essa característica peculiar da Guerra Cibernética evidencia traços de todas as expressões de poder de um Estado como seu desenvolvimento econômico, militar, cultural e sua inserção digital; e expõe uma abrangência de possibilidades de exploração do espaço cibernético. A questão do poder na Guerra Cibernética será tema da próxima seção.

3.3 O USO ESTATAL DA GUERRA CIBERNÉTICA E A QUESTÃO DO PODER

Uma vez compreendido que negar o desenvolvimento tecnológico não é uma opção razoável para um Estado, e que a Guerra Cibernética tem a potencialidade de definir um conflito (CORNISH; HUGHES; LIVINGSTONE, 2009), cabe aos planejadores, em todos os níveis de decisão, pensar na utilização otimizada dos recursos cibernéticos. A profundidade do alcance desse emprego será reflexo direto do poder do Estado no sistema internacional.

Atualmente os Estados exploram as vulnerabilidades cibernéticas de seus oponentes em todos os seus níveis de decisão, desde o nível político, passando ao estratégico, ao operacional, e até ao tático. A Operação Pomar, conduzida em 2007, pelas Forças Armadas

israelenses é plenamente adequada para ilustrar tal situação.

Em 2006, durante uma visita diplomática a Londres, um funcionário do governo sírio descuidou-se e saiu do seu hotel para um breve passeio deixando seu *laptop* exposto sobre a bancada do quarto. Agentes do Mossad, o serviço de inteligência israelense, acessaram o quarto e instalaram um cavalo de Troia[22] na máquina do funcionário sírio. A análise dos arquivos do disco rígido do *laptop* identificou, entre plantas de construção e fotos de tubos usados para trabalho com material físsil, uma fotografia na qual era possível identificar um dos líderes do programa nuclear norte-coreano e o diretor da Comissão de Energia Atômica da Síria. Eles estavam no deserto, em uma localidade síria chamada al Kibar. A análise forense dos arquivos concluiu que os sírios, com a ajuda da Coreia do Norte, estavam avançados na construção de uma instalação de processamento de plutônio, passo necessário para o desenvolvimento de uma bomba atômica. (SINGER; FRIDEMAN, 2017; MARR, 2019)

Essa descoberta foi analisada pelo governo israelense até a decisão de se empreender uma ação militar. Em setembro de 2007 foi desferida a Operação Pomar. Aeronaves israelenses de ataque ao solo penetraram no espaço aéreo sírio e bombardearam o complexo de al Kibar. O detalhe dessa ação é que em nenhum momento as aeronaves foram detectadas pelos radares de vigilância aérea sírios. Para obter esta vantagem Israel se valeu de uma ação cibernética: invadiu a rede de computadores militares síria e fez com que os operadores dos radares enxergassem uma reprodução não verdadeira do céu sírio. (SINGER; FRIDEMAN, 2017; MARR, 2019)

As ações de espionagem conduzidas pelo Mossad e os ataques, virtual e cinético, da Operação Pomar, ocorreram sem baixas e com o emprego de uma força pequena. Um

22 Cavalo de Tróia: é um tipo de malware normalmente disfarçado de software legítimo. Uma vez ativados, os cavalos de Troia permitem acesso ao sistema infectado trazendo abertura ao invasor para conduzir ações diversas que podem incluir a exclusão, o bloqueio a modificação e a cópia de dados. Diferentemente dos vírus e worms, os cavalos de Troia não conseguem se replicar automaticamente.

breve exercício imaginativo permite desenhar um cenário em que tais ações, sendo conduzidas sem o componente cibernético, gerariam maiores gastos, maiores possibilidades de baixas e maior desgaste político internacional.

O relato dos fatos envolvendo a Operação Pomar expõe, na prática, algumas possibilidades de uso do espaço cibernético. A busca por informações, popularmente tratada como espionagem, pode ser empregada em todos os níveis e para os mais variados fins estatais, como, por exemplo, conhecer a rotina de um físico nuclear ou descobrir a frequência de operação dos mísseis do oponente.

Uma outra possibilidade identificada no caso em estudo é a capacidade de invasão da rede oponente, seja militar ou não. O ardil empregado pelos israelenses para enganar os operadores sírios pode ser extrapolado para muitas outras aplicações: sistema eletrônico de controle de aeronaves, link de dados entre meios operativos, controle de veículos não tripulados, sistemas de controle de centrais nucleares, sistemas de controle de mísseis de defesa e outras.

Percebe-se assim que o domínio do Espaço Cibernético abre um leque de oportunidades a ser limitado somente pelas capacidades dos beligerantes. Entretanto, há outro fator a considerar. Efetivar tais ações, principalmente em casos de conflito não declarado, sem que isso custe um desgaste significativo, é função direta do nível de influência que o Estado exerce no sistema internacional, ou seja, do seu poder. Corroborando o entendimento da relação entre a capacidade precípua da guerra cibernética de obter o dado negado e a questão do poder, Barros (2015, p. 81) argumenta que “não é novidade que a informação tem sido utilizada como fonte de poder para o estabelecimento de quais seriam os Estados (…) mais influentes no âmbito internacional. A informação é uma das fontes de poder do Estado (…)”. Dessa forma, percebe-se que há uma relação de consequência entre uma maior capacidade cibernética, que gera mais acesso a informações privilegiadas, que permite moldar a

compreensão da situação, que eleva o poder. E o ciclo se reinicia com a capacidade cibernética potencializada pelo maior poder.

A expressão “espionagem” usada no parágrafo anterior pode ser traduzida, em termos de uma campanha militar, para “preparação para o combate” ou “preparação do campo de batalha”. Desde o início do século, o Pentágono tem usado o subterfúgio de classificar qualquer ação secreta como apenas preparação do campo de batalha, reduzindo sua importância. Não é difícil perceber que a citada preparação ganha flexibilidade e subjetividade uma vez que o combate não precisa ser iminente e ter local definido, tornando qualquer tempo e local possíveis campos de batalha. (CLARK; KNAKE, 2015)

Concluindo, a Guerra Cibernética evoluiu as capacidades de exploração do terreno inimigo, das suas condutas e doutrinas; além de ter aberto um campo fértil para o desenvolvimento de novas táticas de guerra. Nesse escopo, a despeito da potencialidade no âmbito da espionagem, com efeito, a maior expressão do uso estatal da Guerra Cibernética ocorre quando, de fato, o ataque cibernético resulta em danos físicos a pessoas e instalações, em uma pura demostração de *hard power*[23]. Na transição do virtual para o cinético verifica-se a questão central de pesquisa desta obra. O próximo capítulo trará esta análise.

23 Ver glossário.

4 A GUERRA CIBERNÉTICA E O DIREITO DA GUERRA

O segundo capítulo desta obra apresentou o Direito da Guerra sob os enfoques do direito de iniciar uma guerra e de, uma vez iniciada, como conduzi-la. No terceiro, por sua vez, foram vistos alguns aspectos que caracterizam a Guerra Cibernética e que permitem melhor compreendê-la. Portanto, já há elementos suficientes para realizar uma confrontação entre àquele ordenamento jurídico e a realidade da Guerra Cibernética, analisar seus resultados e a partir de então verificar em que proporção o Direito da Guerra se constitui em arcabouço jurídico para a análise legal dos casos de Guerra Cibernética. Essa é a proposta deste quarto capítulo.

Ver-se-á nas subseções seguintes o quanto os efeitos reais das ações cibernéticas podem de fato agredir os preceitos do Direito da Guerra. Diferente do que suas características possam sugerir, é um erro acreditar que a guerra cibernética é mais branda, tal como alertado por Barros:

> Talvez pela extensão do domínio no qual o conflito ocorre e pela habilidade dos atores de esconderem seus efeitos reais, ela tenha a aparência de menos lesiva ao Direito Internacional, mas suas consequências e sua abrangência podem ser ainda mais nefastas. Esse fato pode, inclusive, fazê-la mais violadora de direitos que a própria guerra tradicional, uma vez que os atores contando com a dificuldade de identificação dos criminosos, acreditam na impunidade e agem, cada vez mais utilizando-se da força, de forma ilegal, no ciberespaço. (BARROS, 2015, p.118)

A agressão aos preceitos jurídicos apontada, será analisada com base no *jus ad bellun* e no *jus in bello*. Uma resposta cinética a um ataque cibernético viola o princípio da proporcionalidade na legítima defesa? É possível aplicar os conceitos de combatentes e não-combatentes na Guerra Cibernética? Em suma, é possível usar a força na guerra cibernética em conformidade as leis do Direito Internacional, uma vez que foram pensadas em uma realidade anterior à da atual evolução digital, ou há uma "zona cinza" provocada pela disruptura advinda do desenvolvimento tecnológico?

As análises destas e de outras questões serão apresentadas nas seções a seguir.

4.1 GUERRA CIBERNÉTICA X *JUS AD BELLUM*

Na subseção 2.2.1 foram expostas as duas formas previstas no ordenamento jurídico internacional para a exceção a proibição de se fazer a guerra. Para os conflitos armados conduzidos sob mandato do CS, não há considerações a fazer nesta obra. Nesses casos a Guerra Cibernética é só mais uma das dimensões da guerra e não há de se questionar a sua aplicação no que se refere ao *jus ad bellun.* Já no atinente ao direito de legítima defesa a análise se torna mais complexa. Com o objetivo de minimizar essa complexidade, será conduzida a abordagem a partir de uma situação fictícia descrita a seguir.

Considerando dois Estados em uma disputa fronteiriça mas sem conflito declarado, a realização, por um dos Estados, de uma ação cibernética em que, de forma coordenada, ocorra a invasão da rede militar de defesa do oponente a fim de obter a localização de alvos militares e o acesso aos sistemas de controle das duas principais centrais de distribuição de energia, causando apagões intermitentes no país a fim de causar caos e reduzir a credibilidade do governo local, pode, sob a ótica jurídica, ser considerada similar a uma invasão empreendida por tropas regulares pela fronteira terrestre, o que por sua vez poderia ser a justificativa para uma reação, com o uso da força, apoiada no direito de legítima defesa; ou por não envolver tropas tem menor implicação?

Antes de responder a questão acima cabe observar algumas outras particularidades.

A prática dos Estados transcende a ótica jurídica e remete novamente a questão do poder e das vulnerabilidades vista no capítulo anterior: os Estados que sofrem ações cibernéticas, como as indicadas no exemplo acima, normalmente não reconhecem oficialmente pois isso exporia suas fragilidades. Da mesma forma, tais ações não são, via de regra, assumidos pelos autores. Barros, Gomes e Freitas (2011) apresentam exemplos de episódios que corroboram estas afirmativas, como os ocorridos entre 2003 e 2006, quando

diversas instalações estratégicas estadunidenses, detentoras de conhecimentos sensíveis, foram alvos de tentativas de invasão em suas redes, ou ainda os de julho de 2009, ocasião em que a Coreia do Sul e os EUA tiveram importantes sítios eletrônicos atacados e ainda teria ocorrido uma tentativa de invasão no sistema de fornecimento de energia elétrica estadunidense. Em ambas as oportunidades não houve reconhecimento formal pelos atacados ou manifestação de autoria pelos eventuais atacantes.

Em adição ao contexto, o histórico de decisões do CS mostra que estas (decisões) ocorrem após extensas e morosas deliberações, e que, mesmo assim, ainda estão sob risco de veto por um de seus membros permanentes. Tal situação é conflitante com a velocidade dos ataques cibernéticos. Nesses casos é razoável assumir que um Estado escolherá lidar com os ataques cibernéticos fazendo uso do seu direito de legítima defesa. (GRAHAM, D., 2010)

Por isso, um caminho que vem sendo trilhado pelos Estados é o de tentar equiparar os ataques cibernéticos aos ataques cinéticos para assim poderem, valendo-se da legitima defesa, usar a força. Mas mesmo o ataque cinético pode suscitar questões de entendimento sobre o quê o definiria. Pictet (1952) consagrou um método segundo a qual o uso da força precisa atender a um teste de escopo, duração e intensidade suficiente para ser considerado um ataque armado. Nesse sentido, Graham, D. (2010) propõe uma ampliação destes aspectos, correlacionando os critérios de Pictet a uma abordagem instrumental, uma outra baseada em seus efeitos e uma abordagem apoiada na responsabilidade do atacante. Os próximos parágrafos trarão um maior detalhamento desta forma de análise.

A abordagem instrumental tem o foco em identificar se o dano proveniente do ataque poderia ter sido causado apenas por um ataque cinético. Essa abordagem pode ser melhor compreendida a partir da Operação Pomar citada no capítulo anterior: o ataque ao sistema de radares da defesa aérea, antes do desenvolvimento das capacidades de ataques cibernéticos, requereria um bombardeio ou algum outro tipo de força cinética para sua

consecução.

Já a abordagem baseada nos efeitos fundamentando-se no efeito global do ataque cibernético. Essa abordagem fica evidente nos casos de ataques a infraestruturas de uso dual (militar e civil) como instituições financeiras e infraestruturas críticas (centrais termoelétricas ou usinas nucleares), por exemplo. A interrupção ou manipulação degradante destes pode ser equiparado a um ataque armado já que impactará no bem-estar econômico e social dos afetados.

Por fim, a abordagem sobre a estrita responsabilidade apregoa que qualquer ataque a qualquer infraestrutura crítica, independente do modo ou dos efeitos, seria equiparado a um ataque armado, em virtude das consequências danosas que tal ataque pode trazer.

Face ao exposto, observa-se que a partir da condução dos testes de Pictet e Graham, D. é sim possível equiparar um ataque cibernético a um ataque cinético.

Aprofundando a análise, Schmitt (2012) desenvolveu seis requisitos para delimitar a coerção política e econômica a partir do uso da força, mas que são plenamente aplicáveis aos ataques cibernéticos: severidade, imediatismo, diretividade, invasividade, mensurabilidade e legitimidade presuntiva. Quanto mais próximo do atendimento pleno destes requisitos, mais equivalentes aos ataques cibernéticos serão dos ataques cinéticos. A fim de clarificar a compreensão, serão apresentadas breves considerações sobre tais requisitos.

A **severidade** traz a ideia de que os ataques armados geram perdas de vidas e destruição de bens em grau mais elevado que outras formas de coerção. O **imediatismo** está ligado a maior rapidez com que os efeitos negativos de um ataque armado, ou a ameaça de empreendê-lo, ocorrem em comparação a outras formas de coerção. Por sua vez, a **diretividade** é um requisito afeto as características objetivas do ataque, ou seja, o que foi feito e como foi feito. Nesse viés, não há considerações sobre o que se desejava fazer, retirando

qualquer caráter subjetivo. A **invasividade** traduz-se na força que invade a fronteira nacional, enquanto que os ataques não cinéticos como os cibernéticos e os econômicos geralmente ocorrem fora das suas fronteiras. A **mensurabilidade** relaciona-se a extensão das consequências de um ataque armado uma vez que estes são usualmente fáceis de verificar enquanto as consequências das formas não cinéticas são mais difíceis de estabelecer. Por fim, a **legitimidade presuntiva** está atrelada a questão de que o uso da força é presumivelmente ilegal, salvo, no caso do direito da guerra, nas exceções já conhecidas.

Após essas considerações já é possível responder a questão proposta a partir da situação fictícia: em uma análise a luz do ordenamento jurídico, é possível sim que um Estado sob ataque cibernético avoque o instrumento da legítima defesa e faça uso da força. A legalidade desta resposta residirá: na avaliação prévia dos requisitos de equiparação entre um ataque cinético e o ciberataque, e na condução, de tal emprego da força, apoiado, conforme explicam Arnold e Quénivet (2008), na necessidade (a verificação de que não há uma solução outra para o conflito, que não uma resposta armada) e na proporcionalidade (a verificação da simetria de grandeza e efeitos entre o ataque ilegal e a resposta legal).

Compreendida a possibilidade de legítima defesa a partir de um ataque cibernético, cabe prosseguir na análise da guerra cibernética frente ao ordenamento jurídico internacional analisando-a no contexto do *jus in bello*.

4.2 GUERRA CIBERNÉTICA X *JUS IN BELLO*

Conforme visto no segundo capítulo, a condução da guerra pelos Estados tem como balizador jurídico o DIH. Os combates nos ambientes “convencionais” da guerra (marítimo, terrestre, aéreo e espacial), já tem tal documento como realidade e se desenvolvem sobre seus preceitos. Já o ambiente cibernético possui características particulares que o fazem naturalmente dissonante ao ordenamento jurídico e apesar de “a discussão sobre a

aplicabilidade da lei dos conflitos armados para os ataques cibernéticos não ser recente em si, uma vez que obras substanciais sobre o tema datam do final dos anos 90" (TIKK; KASKA; VIHUL, 2010, p.79, tradução nossa)[24], muito ainda carece ser discutido. Em face do exposto, esta seção se propõe a analisar as características da guerra cibernética sugeridas por Nunes (2015) que guardam, de fato, influências frente ao *jus in bello:* a temporalidade dos efeitos de um ataque cibernético, a imprevisibilidade destes efeitos e a questão da presença de não-combatentes no espaço cibernético.

A temporalidade pode ser traduzida na dificuldade de determinação do momento do ataque e da efetivação do seu efeito. Um ataque cibernético pode ser desferido hoje e ter seu resultado efetivo sobre o alvo designado daqui a três meses, por exemplo. E, este resultado sobre o alvo pode, após mais dois meses, estender-se para sistemas de TI diferentes do alvo inicial, já trazendo a tona a característica da imprevisibilidade dos efeitos de um ataque.

Um bom exemplo desta imprevisibilidade pode ser visto no caso do vírus Stuxnet. Criado para agir sobre sistemas SCADA[25] de centrífugas de centrais nucleares iranianas, estima-se que tenha infectado mais de 60.000 computadores, e apesar de mais da metade dessas máquinas estarem no Irã, a lista de países infectados inclui Índia, Indonésia, China, Azerbaijão, Coreia do Sul, Malásia, EUA, Austrália, Finlândia e Alemanha (FARWELL; ROHOZINSKI, 2011). Tal exemplo mostra a dificuldade de se prever a extensão do alcance do ataque cibernético. A probabilidade de causar danos colaterais é real e deve ser sopesada pelo planejador do ataque.

Os danos colaterais citados no parágrafo anterior remetem-se diretamente a terceira característica a ser considerada, a presença de não-combatentes no ambiente cibernético. Naturalmente que nos demais ambientes de guerra também há a presença de não-

24 Texto original em inglês: "The discussion on the applicability of the law of armed conflict to cyber attacks is not recent in itself: substantial works on the topic already date from the late 1990s."

25 Sistemas de controle de automação e monitoramento industrial.

combatentes, mas tal condição é levada ao extremo no espaço cibernético uma vez que nele não existem barreiras. Ainda no exemplo do vírus Stuxnet, a extensão do dano ganha contornos complexos quando se considera que dentre os atingidos colateralmente pela propagação do vírus, estão não-combatentes localizados em Estados não envolvidos nas hostilidades.

A presença de não-combatentes carrega ainda a necessidade de se considerar o aspecto da responsabilidade estatal. A possibilidade de um cidadão, de qualquer Estado, mesmo não envolvido em hostilidades, poder interferir em um conflito por meio de uma ação cibernética; por um lado expõe a abrangência do problema do controle, no contexto do paradigma do desenvolvimento digital, e por outro abre uma oportunidade de ocultação das ações estatais.

Ampliadas as características da guerra cibernética de interesse, será retomada a análise sob o arcabouço dos princípios do DIH apresentados no capítulo 2.

Iniciando pelo princípio da necessidade militar, uma revisita ao seu cerne mostra que ele é diretamente ligado a escolha dos alvos e ao conceito de objetivo militar. Nesse contexto, tem-se que este princípio é indiferente a realização de um ataque em um domínio terrestre, marítimo, aéreo, espacial ou cibernético.

Entretanto, apesar de a Guerra Cibernética diretamente não indicar contrariedade ao princípio da necessidade militar, pode-se identificar que uma dificuldade surgirá na escolha dos alvos e na categorização desse alvo como objetivo militar ou não, pois neste momento evidencia-se a característica da guerra cibernética de imprevisibilidade nas consequências dos ataques. De forma mais específica, a possibilidade dos danos colaterais se propagarem de forma descontrolada e a possibilidade de isto afetar pessoas e bens protegidos pelo DIH, agrega dificuldades na formulação da lista de alvos.

Passando ao princípio da Humanidade, cabe relembrar o âmago deste princípio

que é evitar e aliviar o sofrimento humano através da proteção à vida e do respeito ao ser humano. Nesse contexto, é possível identificar que, tal qual observado no princípio da necessidade militar, o problema reside na escolha dos alvos e na mensuração dos danos colaterais. E nesta mensuração tem-se uma grande limitação no ambiente cibernético.

Mais uma vez pode-se recorrer ao caso do vírus Stuxnet para reforçar o entendimento: “ao contrário de tentar se disseminar ao máximo possível, como era o objeto dos *worms* do passado, o Stuxnet permitia que cada computador infectado o transmitisse para não mais do que três computadores” (SINGER; FRIEDMAN, 2017, p. 135) mas mesmo assim houve, conforme visto anteriormente, a infecção de mais de 60.000 máquinas. Tal exemplo evidencia que, mesmo com arquitetura avançada e alvos, teoricamente, bem estabelecidos, há o risco de infecção indiscriminada podendo gerar sofrimento humano ou destruição de bens.

A abordagem introduzida acima remete ao princípio da distinção, já que evidencia-se, por um lado, a diferenciação fundamental a ser feita entre os bens civis e os bens militares, e a dificuldade inerente de se levar a efeito tal distinção no ambiente cibernético. No seio desse princípio está enraizada a crença de que a guerra deve ser eficaz, e não punitiva aos não-combatentes, uma vez que possuem o direito à vida protegido, mesmo na guerra.

Entretanto, como realizar a distinção entre não-combatentes e combatentes em um ambiente de uso eminentemente dual? De fato, não há resposta assertiva para esta questão e a clarificação das razões para isso passam por resgatar entendimentos apresentados no capítulo anterior sobre o ambiente cibernético, o uso hodierno dos recursos de TI pelas pessoas comuns, pelas corporações e pelos Estados. Considerando que a tecnologia para os ataques cibernéticos hoje, apesar de sofisticadas, ainda não são capazes de garantir limitação de danos colaterais, é fato que os não-combatentes estão expostos, direta e indiretamente aos efeitos

dos ataques, segundo Schmitt e O'Donnell esclarecem:

> Finalmente, há o sério dilema dos alvos de uso dual. Este é novamente um problema de distinção entre objetos militares e civis. Decorre da infraestrutura conjunta das economias modernas. Instalações militares e civis compartilham a necessidade de eletricidade, gás natural e petróleo para sustentar seus serviços básicos. Raramente existe uma infraestrutura dedicada exclusivamente as instalações militares. Desabilitar as instalações que sustentam um adversário militar pode inevitavelmente onerar as populações civis locais. (SCHMITT; O'DONNELL, 2002, p. 224, tradução nossa)[26]

Esta análise pode ficar mais rica a partir da observação da crise da Rússia com a Ucrânia (2013-2014), pela posse da Crimeia. Iniciada em novembro de 2013, teve grande uso de ataques cibernéticos. As forças ucranianas acusam a Rússia de ter bloqueado as comunicações celulares do país e realizado ataques do tipo negação de serviço a páginas virtuais de serviços na região da Crimeia. A autoria é negada pelo governo russo (GEERS, 2015). A partir deste caso, propõe-se a seguinte suposição: em virtude da indisponibilidade de telefonia, uma senhora não consegue solicitar socorro para seu marido idoso e o homem morre. O sofrimento imposto ao casal de idosos poderia ser tratado como agressivo ao princípio da distinção ou seria aceitável frente aos objetivos militares buscados com o ataque? Invariavelmente a resposta remeterá ao entendimento de que deve haver algum equilíbrio entre a vantagem do esforço de guerra para a destruição de um alvo, e o dano colateral a bens e pessoas protegidas. Essa relação é o âmago do próximo princípio do DIH a ser confrontado com a guerra cibernética, a proporcionalidade.

Um bom termo é entender a proporcionalidade como uma balança, com o peso relativo do ganho militar em um prato e o dano colateral no outro. Eles trazem complexidade a este equilíbrio que envolverá abordagens afetas tanto ao campo de batalha, em si, quanto a ética. Conforme afirmam Schmitt e O'Donnell (2002), o limite deste equilíbrio estará na admissão de que uma vantagem militar efêmera não poderá superar um dano colateral

26 Texto original em inglês: "Finally, there is the serious dilemma of dual-use targets. This is again a problem of distinction between military and civilian objects. It stems from the joint infrastructure of modem economies. Military and civilian facilities share a need for electricity, natural gas, and oil to sustain their basic services. Rarely is there a dedicated infrastructure exclusively serving military facilities. To disable the facilities that sustain a military adversary may unavoidably burden the local civilian populations."

enorme.

O Artigo 51 (b) do Protocolo Adicional I, considera um ataque indiscriminado se "for causar perda acidental de vidas civis, ferimentos a civis, danos a objetos civis, ou uma combinação destes, que seria excessiva em relação a uma vantagem militar concreta e direta antecipada" (BRASIL, 1993). Confrontando essa definição tradicional com as características da guerra cibernética, observa-se que todas contribuem para tornar nebulosa a avaliação da proporcionalidade no ambiente cibernético. A presença de pessoas e bens civis no mesmo ambiente do combate, a temporalidade indefinida dos efeitos dos ataques, e a imprevisibilidade das consequências dos ataques fazem a balança da proporcionalidade ter equilíbrio dificultado.

Em evolução a esta visão, Schmitt e O'Donnell (2002) ensinam que a proporcionalidade teve seu entendimento modificado nas negociações de Roma para o estabelecimento de uma corte criminal internacional. O TPI ampliou a abordagem do princípio em lide, observando que a vantagem militar deve ser avaliado no contexto de uma campanha militar global, permitindo aos comandantes militares basear sua análise em um contexto mais amplo. Por exemplo, uma vantagem militar não precisa estar relacionada temporal e geograficamente ao alvo. Admite-se agora uma vantagem militar futura ou em local diferente, e que para haver a transgressão do princípio da proporcionalidade, deverá haver um claro excesso no desbalanceamento entre a vantagem militar e os danos causados as pessoas e bens protegidos. Com efeito, face as características da guerra cibernética já estudadas, não será tarefa simples definir este excesso.

Assim, resta um último elemento a ser considerado nesta abordagem sobre a proporcionalidade: o conhecimento, a consciência situacional. A avaliação do beligerante atacante estará pautada nas informações que ele dispõe no momento. Ele terá infringido o DIH se, sabendo que os danos seriam claramente excessivos, tiver prosseguido no ataque. Do

contrário, não há razões para responsabilizá-lo. Uma análise destes termos, sob a ótica da guerra cibernética é que, face a imprevisibilidade dos ataques cibernéticos, esta responsabilização jurídica tornar-se-á de pouca clareza.

Finalmente, o princípio da limitação encerrará esta abordagem sobre os princípios do DIH e a sua aplicabilidade na guerra cibernética. Afeto aos meios de se fazer a guerra, ou seja, a limitação ao uso de armas, projéteis, materiais e métodos que levem ao sofrimento e danos desnecessários, inclusive os extensos, duráveis e graves ao meio ambiente natural, este princípio não indica sofrer incoerências no tocante as capacidades de ataques cibernéticos. Não que tais efeitos não possam ser alcançados a partir de ataques cibernéticos. Sim, podem. O que se deseja mostrar com esta análise é o fato de não serem as armas cibernéticas em si a raiz do problema, e sim o seu emprego sem a correta avaliação de danos, retornando, dessa forma, aos princípios da distinção e da proporcionalidade anteriormente abordados.

Face ao exposto, é possível concluir que, ante as peculiaridades características da guerra cibernética e as incertezas que elas trazem, a análise dos princípios da distinção e da proporcionalidade pode tornar-se mais nebulosa em comparação a outros ambientes de guerra. Entretanto, cabe a ressalva de que a "zona cinza"[27] criada não é suficiente para invalidar os princípios de ordem humanitária da distinção e da proporcionalidade. A observância deles pelos beligerantes, ou a caracterização do descumprimento de algum destes princípios nos casos dos crimes de guerra, é sim possível e advirá de uma análise holística das nuances de cada caso.

27 Zona de incertezas.

5 CONCLUSÃO

Este trabalho se propôs a analisar o ordenamento jurídico da guerra e identificar se os seus artigos e cláusulas, tais quais redigidos, são suficientes para suportar as características particularmente disruptivas da Guerra Cibernética. Nesse escopo, foi formulada a seguinte questão de pesquisa: "Em que proporção a Carta das Nações Unidas e o DIH estabelecem fundamentação jurídica suficiente para regular as ações dos Estados no *jus ad bellum* e no *jus in bello*, nos casos de Guerra Cibernética?"

Para alcançar tal propósito e responder a questão proposta, precipuamente foi empreendida uma imersão no ramo do direito internacional objeto de estudo. Foram identificadas as raízes históricas do Direito da Guerra que nos permitem compreender o seu formato e abrangências atuais. A partir do entendimento dos direitos de Haia, Genebra, Nova Iorque e Roma; foi possível avançar para a compreensão do *jus ad bellum,* principalmente no tocante a legitimidade do uso da força; e para o *jus in bello,* alcançando a compreensão dos princípios do DIH e expondo, ao fim, que antes de uma limitação ao combate, estes constituem-se, na verdade, em balizadores igualitários para a condução das hostilidades.

Na sequência, o foco do trabalho foi direcionado à Guerra Cibernética. O espaço cibernético, repleto de particularidades e potencialidades não exploradas ou ainda não descobertas, foi apresentado em diversas facetas. Com prioridade para seu uso estatal, mas sem desconectar-se da dualidade resultante das vertentes civil e militar, a Guerra Cibernética foi descortinada, trazendo à análise, entre outros temas, a decisão a ser tomada, a nível estatal, referente ao paradigma do desenvolvimento digital; o poder que pode advir do desenvolvimento das capacidades cibernéticas, através da obtenção do dado negado; e, principalmente, a sua potencialidade destrutiva. Nesse ponto, em que o virtual se torna cinético e observam-se efeitos fisicamente danosos de um ciberataque, notou-se que reside a máxima expressão do uso militar da Guerra Cibernética por um Estado.

Dessa forma, passou-se ao exame efetivo da relação Direito da Guerra e Guerra Cibernética. Esta análise foi conduzida em uma forma esquemática na qual foram individualmente contrastados o *jus ad bellum* e o *jus in bello* frente a essa nova dimensão da guerra.

No âmbito do direito de um Estado ir à guerra, reduziu-se a abordagem a questão da legitima defesa e a possibilidade de avocação desse direito a partir de um ataque cibernético, uma vez que não há o que se considerar quando de uma decisão do CS. A análise foi então conduzida a um ponto fulcral em que, uma vez que um ataque cibernético reúna as características de escopo, duração e intensidade necessárias para definir o uso da força, ele pode sim ser equiparado a um ataque cinético e, a partir de então, originar todas as reações que dele poderiam advir.

Identificou-se que a ausência de fronteiras físicas no espaço cibernético e o compartilhamento de redes e infraestruturas pelos Estados sempre será um ponto de questionamento em termos de ameaça às soberanias. Nesse contexto, sem se distanciar da realidade das relações estatais, ficou em evidência a questão do poder e a forma como ele pode alterar ou reescrever o entendimento jurídico, reforçando a importância da necessidade do fortalecimento constante do DIP e das instituições como forma de reduzir as injustiças e distorções na compreensão da realidade.

Por fim, a análise do *jus in bello* trouxe a contrastação dos princípios do DIH perante a temporalidade dos efeitos de um ataque cibernético, a imprevisibilidade destes efeitos e o problema da presença de não-combatentes no espaço cibernético.

Na análise dos princípios da humanidade, da necessidade militar e da limitação, a pesquisa realizada permitiu concluir que não há uma relação direta de contrariedade entre estes princípios e a guerra cibernética. Apesar de a guerra cibernética possuir potencialidade para agredir tais princípios, isto ocorreria em função de um desdobramento da dificuldade na

mensuração dos danos gerada pelas características da guerra cibernética. De fato, em alguma medida, os princípios da humanidade, da necessidade militar e da limitação são afetados por consequências da não observação dos princípios da distinção e da proporcionalidade.

Nesse diapasão, o entendimento alcançado foi de que a dualidade do ambiente cibernético é claramente perceptível como contrariante ao princípio da distinção, tal qual a temporalidade e a imprevisibilidade dos efeitos dos ciberataques são ao princípio da proporcionalidade. Entretanto, tal contrariedade não é absoluta. Apesar de agregarem complexidade ao estabelecimento da distinção e da proporcionalidade, isso não é de proporções tais que signifique a não aderência da 5ª dimensão da guerra a estes princípios. Em suma, pode-se concluir que, a depender do caso concreto, a proporcionalidade e a distinção terão limitações no seu alcance.

Ademais, resta a essa análise, agregar, mais uma vez, a questão do poder. Sendo o Direito uma ciência humana, não estará ela jamais desarraigada das vicissitudes das relações interestatais, concluindo-se que a definição se um ataque foi ou não proporcional, ou obedeceu ou não o princípio da distinção, trará influências dos pesos relativos dos atores envolvidos. Nesse contexto, surge como louvável a iniciativa do Manual de Tallinn em buscar uma compreensão universal sobre a aplicação do Direito da Guerra a ciberguerra. Espera-se que a iniciativa ganhe mais adesão e solidez ao longo dos anos, de modo que possa vir a se tornar parte do ordenamento jurídico vigente, mesmo que de forma consuetudinária.

A conclusão do estudo realizado nesta obra é que a Carta das Nações Unidas expressa-se plenamente suficiente para regular o *jus ad bellum* nos casos de Guerra Cibernética, e que no âmbito do DIH há uma limitação parcial no alcance dos princípios da distinção e da proporcionalidade.

Tal limitação, entretanto, não significa fragilidade dos princípios. Na verdade, deverá o beligerante, deparado com a decisão de empreender um ataque cibernético em que o

potencial danoso proveniente da impossibilidade de estabelecimento preciso da extensão, no tempo e na força, dos efeitos do ataque, e do alcance desses efeitos aos não-combatentes; buscar outras formas de conduzir o combate ou predispor-se a arcar com o ônus político ou ético dos seus atos.

Nesse contexto, cabe ressaltar a Cláusula Martens como ferramenta jurídica do DIH, adequada para suportar as eventuais lacunas não preenchidas, acentuando como ela se presta adequadamente a amparar as inseguranças resultantes da rápida evolução da tecnologia, tal qual ocorrido no advento das armas nucleares.

Enfim, todo o arcabouço jurídico construído teve como alvo livrar a humanidade do flagelo da guerra e de suas consequências nefastas. Cada um dos artigos do Direito da Guerra foi escrito e discutido de modo a obter um produto final atemporal e aderente a qualquer dos domínios da guerra existentes ou ainda a serem concebidos. A Guerra Cibernética, mesmo que reservando peculiaridades, deve ser tratada em conformidade com as normas do *jus ad bellum* e do *jus in bello*.

Como sugestões para futuras linhas de pesquisa, apresentam-se como oportunidades, uma pesquisa exploratória referente as perspectivas de evolução, nos aspectos técnico-científicos do espaço cibernético, que permitam o incremento da capacidade de controle dos Estados sobre a amplitude das consequências dos ataques cibernéticos, impactando diretamente nos aspectos que hoje causam limitação no alcance dos princípios da proporcionalidade e da distinção; e uma outra abordagem focada na dualidade do espaço cibernético e na responsabilidade dos Estados na defesa da soberania no espaço cibernético, considerando a possibilidade de desferimento de ataques cibernéticos, por entes não estatais, a partir de suas fronteiras.

REFERÊNCIAS

ACCIOLY, Hildebrando; SILVA, G. E. do Nascimento; CASELLA, Paulo Borba. **Manual do Direito Internacional Humanitaro.** 16. ed. São Paulo: Saraiva, 2008. 916 p.

ARNOLD, Roberta; QUÉNIVET, Noelle. **International Humanitarian Law and Human Rights Law: towards a new merger in International Law.** Leiden: Martinus Nijhoff Publishers, 2008. 596 p.

ÁVILA, Rafael; RANGEL, Leandro de Alencar. **A guerra e o direito internacional.** Belo Horizonte: Del Rey, 2009. 176 p.

BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de. (Org.). **Desafios estratégicos para segurança e defesa cibernética.** Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. 216 p.

BARROS, Renata Furtado de. **Guerra Cibernética: os novos desafios do Direito Internacional.** Belo Horizonte: Editora D'Plácido, 2015. 178 p.

BEST, Geoffrey. **War and Law Since 1945.** New York: Oxford University Press, 1994. 434 p.

BRASIL. **Decreto nº849 de 25 de junho de 1993**. Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados. Brasília, 1993.

BRASIL. Ministério da Defesa. MD34-M-03. **Manual de Emprego do Direito Internacional dos Conflitos Armados nas Forças Armadas**. 1. ed. Brasília: 2011

BRASIL. Ministério da Defesa. MD31-M-07. **Doutrina Militar de Defesa Cibernética**. 1. ed. Brasília, 2014.

BRASIL. Ministério da Defesa. MD35-G-01. **Glossário das Forças Armadas**. 5. ed. Brasília: 2015.

BRIGAGÃO, Clóvis; JÚNIOR, Domício Proença. **Panorama Brasileiro de paz e segurança.** São Paulo: Hucitec; Rio de Janeiro: Fundação Konrad Adenauer, 2004. 348 p.

BUGNION, François. **El derecho de Ginebra y el derecho de La Haya.** 2001. Disponível em: <https://www.icrc.org/es/doc/resources/documents/misc/5tdqeh.htm>. Acesso em: 01 ago. 2019.

BYERS, Michael. **A Lei da Guerra.** Tradução de Clóvis Marques. Rio de Janeiro: Record, 2007. 263 p.

CARREIRO, Marcelo. A Guerra Cibernética: cyberwarfare e a securitização da internet. **Revista Cantareira.** n. 17, p. 123-137, 2012. Disponível em: <http://www.historia.uff.br/cantareira/v3/?cat=5/>. Acesso em: 05 ago. 2019.

CLARK, Richard A.; KNAKE, Robert K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito.** Tradução de Bruno Salgado Guimarães, et al. Rio de Janeiro: Brasport, 2015. 241 p.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **O DIH e outros regimes legais – jus ad bellum e jus in bello**. Disponível em <https://www.icrc.org/pt/doc/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm>. Acesso em: 23 julho 2019.

CORNISH, Paul; HUGHES, Rex; LIVINGSTONE, David. **Cyberspace and the National Security of the United Kingdom: Threats and Responses.** Londres: Chatam House, 2009. Disponivel em: <https://www.chathamhouse.org/publications/papers/view/ 109020>. Acesso em 09 jul. 2019.

DINSTEIN, Yoram. **Guerra, Agressão e Legítima Defesa.** 3. ed. Barueri: Editora Manole, 2004. 470 p.

FARWELL, James P; ROHOZINSKI, Rafal. Stuxnet and the Future of Cyber War. **Survival – global politics and strategy.** EUA, v. 53, p. 23-40, 2011. Disponível em: <https:/ /doi. Org/10.1080/00396338.2011.555586>. Acesso em: 31 jul. 2019.

FERNANDES, Jean Marcel. **A promoção da paz pelo Direito Internacional Humanitário.** Porto Alegre: Sergio Antonio Fabris Ed., 2006. 166 p.

FLECK, Dieter. **The Handbook of International Humanitarian Law**. 2. ed. New York: Oxford University Press Inc., 2008. 770 p.

GEERS, Kenneth. (Ed.). **Cyber War in Perspective: Russian Agression Against Ukraine.** Tallinn: NATO CCD COE publications, 2015. 175 p.

GRAHAM, David E. Cyber threats and the law of war. **Journal of National Security Law & Policy**, EUA, v. 4, p. 87-102, 2010. Disponível em: < http://jnslp.com/wp-content/uploads / 2010/08/07_Graham.pdf>. Acesso em: 13 jul. 2019

GRAHAM, Robert. **Cyberwar is Fiction**. In Errata Security, 07 de junho de 2010. Disponível em: <http://erratasec.blogspot.com/2010/06/cyberwar-is-fiction.html>. Acesso em: 29 jul. 2019

KRIEGER, César Amorim. **Direito internacional humanitário: o precedente do Comitê Internacional da Cruz Vermelha e o Tribunal Penal Internacional.** 1. ed. Curitiba: Juruá, 2004. 362 p.

LEWIS, James A. **The korean cyber attacks and their implications for cyber conflict**. Washington, EUA: Center for Strategic and International Studies, 2009. Disponível em: <http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for _Cyber_Conflict.pdf>. Acesso em: 05 de julho de 2019.

MARR, Carson. **Cyberwarfare and Applied Just War Theory: Assessing the Stuxnet Worm through Jus ad Bellum and Jus in Bello.** Pennsylvania: Student Perspectives on Institutions, Choices and Ethics, v. 14. 2019. Disponível em: < https://repository.upenn.edu /spice/vol14/iss1/2 >. Acesso em 10 jul. 2019.

MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo**. 32 ed. São Paulo: Malheiros, 2015, p.1150.

NETO, Ricardo Borges Gama. Guerra cibernética/Guerra eletrônica – conceitos, desafios e espaços de interação. **Revista Política Hoje.** Recife, v. 26, n. 1, p. 201-218, 2017.

NUNES, Luiz Artur Rodrigues. **Guerra cibernética e o Direito Internacional – Aplicabilidade do jus ad bellum e do jus in bello.** 2015. 59 f. Monografia (Curso de Altos Estudos de Política e Estratégia) - Escola Superior de Guerra, Rio de Janeiro.

NYE JR, Joseph S. **Soft Power: the means to success in world politcs**. New York: PubllicAffairs, 2005. 192 p.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Assembleia Geral. **The Charter of the United Nations.** Nova Iorque, ONU, 1945. Disponível em: <http://www.un.org/en/documents/charter/index.shtml>. Acesso em: 20 jul. 2019.

PICTET, Jean S. **The Geneva Conventions of 12 August 1949 Commentary Volume I_ For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field.** Genebra: International Comitee of the Red Cross, 1952. 466 p.

SCHINDLER, Dietrich; TOMAN, Jiri (Ed.). **The Laws of Armed Conflicts.** 4. ed. Leiden: Martinus Nijhoff Publishers, 2004. 1493 p.

SCHMITT, Michael N. **Essays on law and war at the fault lines.** Haia: Asser Press, 2012. 637 p.

SCHMITT, Michael N. (Ed.). **Tallinn manual on the international law applicable to cyber warfare.** New York: Cambridge University Press, 2013. 282 p.

SCHMITT, Michael N. (Ed.). **Tallinn manual 2.0 on the international law applicable to cyber operations.** New York: Cambridge University Press, 2017. 598 p.

SCHMITT, Michael N; O'DONNELL, Brian T. (Ed.). Computer Network Attack and International Law. **International Law Studies.** Newport: Naval War College, v. 76. 2002. Disponível em: <https://digital-commons.usnwc.edu/ils/vol76/iss1/1/>. Acesso em: 23 jul. 2019

SINGER, Peter W; FRIEDMAN Allan. **Segurança e guerra cibernéticas: o que todos precisam saber.** Tradução de Geraldo Alves Portilho Júnior. Rio de Janeiro: Biblioteca do Exército, 2017. 360 p.

SWINARSKI, Christophe. **Introdução ao Direito Internacional Humanitário.** Brasília: Instituto Interamericano de Direitos Humanos, 1996. 41 p.

TIKK, Eneken; KASKA, Kadri; VIHUL, Liss. **International Cyber Incidents: legal considerations.** Tallinn: NATO CCD COE publications, 2010. 130 p.

TIKK, Eneken; TALIHÃRM, Anna-Maria. **International Cyber Security: legal & policy proceedings 2010.** Tallinn: NATO CCD COE publications, 2010. 144 p.

GLOSSÁRIO

Bens protegidos: bens culturais, obras indispensáveis a sobrevivência da população civil, meio ambiente natural e obras e instalações contendo forças perigosas.

Ciberataque: ataque cibernético.

Ciberguerra: guerra cibernética.

Combatente: deve estar inserido em uma estrutura de comando, portar sinais distintivos, portar armas visivelmente e cumprir as regras do DIH.

Hard Power: é o uso de meios militares e econômicos para influenciar o comportamento ou interesses de outros entes políticos. De natureza coercitiva, esta forma de exercício do poder é mais imediatamente efetiva quando imposta por um corpo político sobre outro de menor poder militar e (ou) econômico.

Não-combatente: gozam de proteção especial pelo DIH os prisioneiros de guerra, feridos, náufragos, enfermos, integrantes das equipes de saúde, defesa civil, religiosos e jornalistas; civis, mulheres, crianças e neutros.

Soft Power: expressão cunhada pelo professor Joseph Nye em sua obra "Soft Power: the means to succcess in world Politcs" e pode ser traduzida como o poder suave. É uma expressão usada nas relações internacionais para descrever a habilidade de um Estado para influenciar o comportamento ou interesses de outros, por meios culturais ou ideológicos. Desde a sua criação, no início dos anos 80, a expressão passou a fazer parte do discurso político como uma maneira de distinguir os efeitos sutis de culturas, valores e ideias no comportamento de outros.

APÊNDICE

O Direito da Guerra no ordenamento jurídico internacional