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

Márcio Lima Moreira Filho Ten Cel Int

Guerra cibernética no contexto do Direito Internacional dos Conflitos Armados

Rio de Janeiro
2021

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

Márcio Lima Moreira Filho Ten Cel Int

Guerra cibernética no contexto do Direito Internacional dos Conflitos Armados

Trabalho de conclusão de curso apresentado ao Curso Avançado de Comando e Estado-Maior da Escola de Comando e Estado-Maior da Aeronáutica.
Linha de Pesquisa: Poder Militar.
Orientador: Coronel-Aviador R/1 Luiz Gustavo Schenk.

Rio de Janeiro
2021

RESUMO

A sociedade contemporânea vem experimentando um ritmo de mudanças jamais visto. Em todas as áreas do conhecimento humano, estão ocorrendo incontáveis revoluções, as quais alteram a maneira tradicional de compreender o mundo. Diferente não seria em relação aos assuntos militares e aos aspectos jurídicos do Direito Internacional Humanitário em face das novas ameaças impostas pelas operações cibernéticas. Esta pesquisa buscou enfrentar dois problemas: em primeiro lugar, determinar em que medida as ações ocorridas no ambiente virtual, em contexto de guerra cibernética, podem constituir infração ao Direito Internacional dos Conflitos Armados (DICA) e, em segundo lugar, discutir a possibilidade de aplicar tal regramento jurídico às ciberoperações realizadas em tempo de paz. Para tanto, partiu-se de discussão acerca do enquadramento das operações cibernéticas na categoria de conflito armado, o que nos levou a revisar os institutos pertinentes às ações no ambiente virtual e contrastá-los com os princípios do Direito Internacional Humanitário. Finalmente, a pesquisa nos mostrou que tão somente as ciberoperações realizadas dentro do espectro dos conflitos armados internacionais ou não internacionais e passíveis de serem classificadas como ataque à luz do Direito Internacional dos Conflitos Armados serão governadas por esse regime jurídico.

Palavras-chave: Guerra cibernética; DICA; Direito Internacional dos Conflitos Armados; Direito Internacional Humanitário

ABSTRACT

Contemporary society has been experiencing a pace of change never seen before. In all areas of human knowledge, countless revolutions are taking place, which alter the traditional way of understanding the world. It would not be different in relation to military affairs and the legal aspects of International Humanitarian Law in the face of new threats posed by cyber operations. This research sought to face two problems: firstly, to determine to what extent actions that took place in the virtual environment, in the context of cyber warfare, may constitute an infringement of the International Law of Armed Conflict (LOAC) and, secondly, to discuss the possibility of applying such legal regulation to cyber operations carried out in peacetime. For that, a discussion was started about the classification of cybernetic operations in the category of armed conflict, which led us to review the institutes relevant to actions in the virtual environment and contrast them with the principles of International Humanitarian Law. Finally, the research has shown us that only cyber operations carried out within the spectrum of international or non-international armed conflicts and which are likely to be classified as an attack under the Law of Armed Conflict will be governed by this legal regime.
Keywords*: Cyber Warfare; LOAC; Law of Armed Conflict; International Humanitarian Law.*

SUMÁRIO

1 INTRODUÇÃO

As ações cibernéticas cada vez mais vêm oferecendo riscos à soberania do Estado Brasileiro. Exemplo disso é o recente vazamento de dados, que atingiu mais de 200 milhões de CPFs no país, como foi amplamente divulgado pela imprensa. Operações desse tipo comprometem sobremaneira a segurança e a defesa nacional, ainda que ocorram em tempos de paz e não se apresentem como conflitos declarados. Do ponto de vista jurídico, poderiam tais operações, realizadas no espaço virtual em tempos de paz, ser consideradas atos de guerra cibernética? Em caso positivo, constituiriam uma infração aos princípios do Direito Internacional dos Conflitos Armados (DICA)? A essas questões este trabalho buscará responder.

Compreender as operações cibernéticas e o modo como elas se inter-relacionam com a guerra cibernética e o DICA num cenário de inexistência de violência cinética – ou seja, fora do espectro do conflito armado tradicional – será o nosso ponto de partida. O entendimento da OTAN (Organização do Tratado do Atlântico Norte), consubstanciado no Tallinn Manual 2.0 on the International Law applicable to cyber operations[1], norteará nossas reflexões.

Este artigo não possui a pretensão de esgotar o tema, cuja discussão ainda é incipiente no país. Objetiva, isto sim, estimular um debate necessário no campo conceitual e indicar um caminho a ser perseguido no tratamento de questão sensível.

1.1 Contextualização fática

No mundo contemporâneo, os modos de atacar a soberania de outros Estados adquiriram um novo campo de atuação, o ciberespaço. Ataques cibernéticos são uma realidade que se impõe. Mesmo em situações de aparente paz entre nações, operações realizadas no ciberespaço podem atentar contra a soberania de um Estado. Por esse motivo, as normas que regem os conflitos armados devem abarcar a guerra cibernética e, de algum modo, apresentar uma regulação mesmo em tempos de paz.

---

1 Cf. SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017

No cenário internacional, as operações cibernéticas começaram a despertar o interesse da comunidade jurídica no fim dos anos 1990. Mais precisamente, foi no ano de 1999 que o United States Naval War College realizou a primeira grande conferência jurídica referente ao tema. O Reino Unido, entre outros países, posicionou o ataque cibernético, ao lado do crime organizado e do terrorismo, entre as quatro ameaças de primeiro nível à segurança.

As medidas que, em face das operações realizadas no ambiente virtual, se tornam necessárias para proteger a sociedade civil devem ser pautadas pela limitação dos meios e dos métodos empregados no combate cibernético. Quaisquer ações deverão observar rigorosamente as normas e preceitos internacionais que regem os conflitos armados, evitando o repúdio da comunidade internacional e até embargos econômicos.

Na atual conjuntura das novas guerras, ditas guerras de quarta geração, o ciberespaço ganha relevância ímpar na atuação dos Estados no cenário internacional, tanto na defesa de sua soberania quanto no ataque a grupos militares com atuação irregular, bem como a outros atores que constituam ameaça aos poderes constituídos.

O entendimento jurídico das normas internacionais que regulam os conflitos armados e sua relação com a guerra cibernética deve, portanto, receber atenção das Forças Armadas Brasileiras e, em especial, do Comando da Aeronáutica. É preciso compreender como se dão as operações realizadas no ciberespaço, no contexto de guerra cibernética, e em que medida podem constituir uma infração ao Direito Internacional de Conflitos Armados.

1.2 Objetivos da pesquisa

O presente artigo apresenta como objetivo geral determinar em que medida as operações realizadas no ciberespaço, no contexto de guerra cibernética, podem constituir uma infração ao DICA. Para alcançá-lo, será necessário discorrer sobre os seguintes objetivos específicos:

i) definir a guerra cibernética enquanto guerra;

ii) identificar a guerra cibernética nos mecanismos normativos do DICA; e

iii) contrastar as possibilidades de guerra cibernética com os princípios do DICA.

Em seguida, examinaremos a hipótese de aplicar tal regramento jurídico às ciberoperações realizadas em tempo de paz.

1.3 Justificativa do estudo

O estudo da guerra cibernética e de sua relação com os conflitos armados, à luz do Direito Internacional Humanitário, reveste-se de importância ímpar no âmbito dos altos estudos das Escolas Militares. É, afinal, fora de dúvida que quaisquer ações de defesa ou de resposta a ataques no ambiente virtual devem seguir os mesmos princípios que regem os conflitos armados convencionais.

As operações realizadas no ciberespaço devem, portanto, estar pautadas em regras, alinhadas às normas e aos costumes praticados pela comunidade internacional, de modo a proteger a sociedade civil.

Operações malsucedidas e/ou sem respaldo legal podem levar o país a sofrer sanções econômicas ou até embargos e, no limite, podem deflagar um conflito armado com emprego de força cinética.

2 METODOLOGIA

O presente artigo nasceu basicamente de pesquisa bibliográfica, segundo os critérios de Gil (2006). Foi a contribuição de diversos autores, bem como o exame atento da doutrina, das normas, das legislações e da jurisprudência, que nos permitiu avançar nas reflexões aqui propostas.

O Manual Tallinn serviu-nos de referência em toda a condução do trabalho, mas outros autores nos socorreram sobretudo na definição de conceitos. Prevaleceu na dinâmica de investigação adotada a metodologia de síntese teórica de Jaakkola (2020), que propõe alcançar a integração conceitual entre as correntes da literatura.

Dessa forma, tentamos consolidar e agrupar conceitos estanques, que, em conjunto, apresentam relevante potencial de aplicabilidade na Força Aérea Brasileira.

Diferentemente de trabalhos empíricos, a pesquisa conceitual funda-se em um processo de assimilação e combinação de evidências na forma de conceitos e

teorias previamente pesquisados em outros trabalhos científicos. Essa constitui a base de validação deste artigo, que se insere no campo da pesquisa teórica.

Por fim, a pesquisa orientou-se nos questionamentos de validade do trabalho científico propostos por Jaakkola (2020), que ressalta a importância do rigor na seleção de fontes de informação e do método de análise, bem como o papel de cada conceito na formulação de hipóteses e de respostas a elas. Afinal, a criação do conhecimento só e possível quando se observam com rigor os princípios metodológicos.

3 REFERENCIAL TEÓRICO

O presente trabalho será conduzido à luz dos entendimentos alicerçados no Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, sendo esta a versão atualizada do conceituado Manual Tallinn. A nova versão da obra incluiu os regramentos internacionais dos conflitos armados aplicados à guerra cibernética para regimes jurídicos em tempos de paz. Além disso, expandiu as regras de "black letter" de 95 para 154, sendo esse o resultado de vários anos de trabalho realizado por um grupo de renomados especialistas no assunto.

A primeira edição do Manual Tallinn, de 2013, restringiu-se ao uso da força no Direito Internacional e ao Direito Internacional Humanitário. O avanço das ações ofensivas no âmbito da guerra cibernética, entretanto, levaria os Estados a discutir o tema a fim de encontrar soluções jurídicas específicas, que fossem além daquelas aplicadas aos conflitos travados com força cinética.

Assim, o Manual Tallinn, especialmente em sua versão de 2017, lança luz sobre tal controvérsia, tentando nortear a atuação dos Estados na busca de soluções jurídicas apropriadas para combater, perseguir e punir pessoas, grupos ou até Estados que se valem da guerra cibernética para atentar, de modo irregular, contra a soberania de outras nações.

Embora o Manual Tallinn consolide as conclusões mais importantes até o momento e apresente caminhos válidos para enfrentar o problema, nossa proposta é revisar os conceitos que o embasam, o que nos levou a investigar várias outras fontes, as quais estão arroladas na seção de referências deste trabalho.

4 ANÁLISE

O mundo contemporâneo vem sofrendo transformações em ritmo e amplitude nunca vistos. No bojo dos avanços tecnológicos que têm revolucionado as mais diversas áreas do conhecimento humano, o segmento de atuação de militares por todo o globo vem experimentando sensíveis alterações no modo de conduzir as hostilidades entre países. Em outras palavras, as guerras convencionais ou, pelo menos, a manutenção de equipamentos bélicos para fins dissuasórios ainda se manterá viva, entretanto as guerras de quarta geração de Lind (2005) parecem trazer de volta situações do passado: os Estados vêm perdendo, relativamente, o monopólio das guerras, com o surgimento de atores não estatais, bem como de novos meios e métodos de se portar num conflito armado.

Nesse novo cenário, o emprego das operações cibernéticas pelos mais diversos atores, estatais e não estatais, oferece diferentes perspectivas para a atuação dos operadores jurídicos quanto à aplicação do Direito Internacional dos Conflitos Armados. Ainda mais complexo se apresenta quando as ações cibernéticas ocorrem em situação de aparente paz entre os atores envolvidos.

Observando o problema sob esse ângulo, procuramos esclarecer o seguinte objetivo geral: determinar em que medida as operações realizadas no ciberespaço, no contexto de guerra cibernética, podem constituir uma infração ao DICA. Igualmente, buscamos responder à hipótese de pesquisa: poderiam as operações realizadas no ciberespaço em tempos de paz ser enquadradas na classificação de guerra cibernética? Dessa indagação advém necessariamente um segundo ponto: em caso positivo, tais ações constituiriam uma infração ao DICA? Para empreender tal discussão, tivemos de observar os seguintes passos: (i) definir a guerra cibernética enquanto guerra; (ii) identificar a guerra cibernética nos mecanismos normativos do DICA; e (iii) contrastar as possibilidades de guerra cibernética com os princípios do DICA.

4.1 Classificação das Operações Cibernéticas

Preliminarmente, deve ser esclarecido que o termo “guerra”, no âmbito do direito internacional, tem sido comumente substituído pela expressão “conflito

armado”[2]. Esta guarda em si um sentido mais amplo e mais adequado ao momento atual, todavia, neste trabalho, as duas expressões serão tratadas como sinônimos.

Ultrapassado esse breve esclarecimento, adentra-se o cerne desta seção. Classificar o conflito é fundamental para a realização de qualquer análise à luz do Direito Internacional dos Conflitos Armados, tendo em vista que a sua natureza determina o regime jurídico aplicável[3]. Considerado o fato de que *guerra cibernética* é espécie do gênero *guerra*, cabe definir tal conceito.

Clausewitz, em sua obra “Da Guerra”, considera-a um “... ato de força para obrigar o nosso inimigo a fazer a nossa vontade”. Lassa Oppenheim a entende como “uma contenda entre dois ou mais Estados por meio de suas Forças Armadas, com o propósito de se sobreporem e imporem as condições de paz que agradem ao vencedor”[4] (tradução nossa).

Os conceitos de autores do passado são mais bem aplicados quando da ocorrência da guerra convencional, apenas entre atores estatais. Para tratar de situações mais complexas, como as do mundo contemporâneo, em que os atores nem sempre são estatais, o Comitê Executivo da International Law Association (ILA, 2010) propõe o entendimento de que:

> [...] conflito armado deve ser diferenciado de "incidentes"; "confrontos de fronteira"; "distúrbios e tensões internas, como motins, atos isolados e esporádicos de violência"; "banditismo, desorganizado e de curta duração insurreições ou atividades terroristas” e “agitação civil, [e] atos únicos de terrorismo”. A distinção entre essas situações e o conflito armado é alcançada com base nos critérios de organização e intensidade.[5] (tradução nossa)

Ainda nesse sentido, cabe clarificar que o conflito armado pode ser subdividido em internacional e não internacional. Em apertada síntese, este ocorre

---

2 Cf. International Law Asssociation, Final Report on the Meaning of Armed Conflict in International Law (ILA 2010). Disponível em: http://www.rulac.org/assets/downloads/ILA_report_armed_conflict_2010.pdf. Acesso em: 4 jul.2021.

3 SCHMITT N., Michael. Classification of Cyber Conflict. **Journal of Conflict and Security Law.** v. 17, 2 ed., 2012. pp 245–260. Disponível em: https://doi.org/10.1093/jcsl/krs018. Acesso em: 2 maio 2021.

4 Ibidem. No original*: “[…] is a contention between two or more States through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases”.*

5 No original: *“[…] armed conflict is to be distinguished from ‘incidents’; ‘border clashes’; ‘internal disturbances and tensions such as riots, isolated and sporadic acts of violence’; ‘banditry, unorganised and short lived insurrections or terrorist activities’ and ‘civil unrest, [and] single acts of terrorism’. The distinction between these situations and armed conflict is achieved by reliance on the criteria of organisation and intensity*”. Cf. International Law Asssociation, Final Report on the Meaning of Armed Conflict in International Law (ILA 2010). Disponível em: http://www.rulac.org/assets/downloads/ILA_report_armed_conflict_2010.pdf. Acesso em: 4 jul.2021.

quando da presença de atores estatais e não estatais, desde que atendidas as condições acima apontadas pelo Comitê Executivo da International Law Association; ao passo que aquele tem ocorrência quando o conflito acontece entre Estados-Nações, sendo que o Tribunal Criminal Internacional para a antiga Iugoslávia define conflito armado como o "recurso à força armada entre Estados sem reconhecer nenhum limite para a duração ou intensidade das hostilidades"[6] (tradução nossa).

Na mesma linha de raciocínio, deve ser esclarecido que o regime jurídico do Direito Internacional dos Conflitos Armados incide tanto sobre o conflito armado internacional quanto sobre o não internacional. No que se refere à contenda entre Estados, fica clara a aplicação ao regime do DICA; vale, no entanto, ressaltar que o conflito armado não internacional também goza da mesma proteção. Saxon (2016) apresenta o comentário do Comitê Internacional da Cruz Vermelha (CICV) ao artigo 3º Comum das Convenções de Genebra de 1949 sobre os conflitos armados não internacionais:

> [...] são confrontos armados prolongados que ocorrem entre forças governamentais e as forças de um ou mais grupos armados, ou entre tais grupos que surgem no território de um estado [parte das Convenções de Genebra]. O confronto armado deve atingir um nível mínimo de intensidade e as partes envolvidos no conflito devem mostrar um mínimo de organização.[7] (tradução nossa)

Portanto, valendo-se de qualquer dos conceitos e obedecendo a seus requisitos, as operações cibernéticas poderiam ser classificadas como guerra e, por consequência, ser submetidas ao regime do Direito Internacional dos Conflitos Armados.

Tais conceitos, entretanto, são genéricos. Faz-se necessário um exame do conceito de conflito cibernético ou guerra cibernética, que ganha diversas

---

6 No original: *"[…] armed conflict as the "resort to armed force between States" without recognizing any threshold for the duration or intensity of hostilities".* In: SCHMITT N., Michael. Classification of Cyber Conflict. **Journal of Conflict and Security Law**, v. 17, n. 2, 2012. pp 245–260. Disponível em: https://doi.org/10.1093/jcsl/krs018. Acesso em: 2 maio 2021.

7 No original: *"[…] are protracted armed confrontations occurring between governmental forces and the forces of one or more armed groups, or between such groups arising on the territory of a state [party to the Geneva Conventions.] The armed confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum of organization".* In: SAXON, Dan. Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions. **Journal of Conflict and Security Law**, v. 21, n. 3, 2016. pp. 555–574. Disponível em: https://academic.oup.com/jcsl/article-abstract/21/3/555/2567000?redirectedFrom=fulltext Acesso em: 2 maio 2021.

interpretações. No Brasil, o Ministério da Defesa adota o seguinte entendimento de guerra cibernética:

> [...] uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e 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. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC". (BRASIL, 2016)

A seu turno, Saxon (2010) descreve a guerra cibernética como em evento que:

> [...] desafia nossa compreensão do conflito armado e da aplicação do Direito Internacional Humanitário. Ao contrário dos sistemas de armas cinéticas, as armas cibernéticas não são máquinas compostas de muitos componentes físicos; eles são coleções de dados usados para comunicar instruções ao software ou hardware. Além de sua complexidade técnica, uma qualidade totalmente evidente das armas cibernéticas é (ironicamente) sua invisibilidade. Esta característica do código de software, combinada com o vasto anonimato e "interconectividade" do ciberespaço, apresenta desafios profundos para o julgamento de indivíduos responsáveis por crimes de guerra cometidos com armas cibernéticas.[8] (tradução nossa).

Dinstein (2012) conclui que a guerra cibernética, em sua essência, não diverge de qualquer outro tipo de conflito armado. Há, no entanto, certos desafios para a caracterização das operações cibernéticas como conflito armado, os quais residem, inicialmente, na identificação dos atores envolvidos e, posteriormente, na análise de elementos como intensidade, tempo de duração e nível de organização desses atores.

Antes de prosseguirmos nesta análise, será necessário proceder ao exame de alguns mecanismos normativos do Direito Internacional dos Conflitos Armados. Na próxima seção, portanto, serão visitados os conceitos de ataque, soberania,

8 No original: *"[…] challenges our understanding of armed conflict and the application of international humanitarian law. Unlike kinetic weapon systems, cyberweapons are not machines composed of many physical components; they are collections of data used to communicate instructions to software or hardware. In addition to their technical complexity, one starkly evident quality of cyberweapons is (ironically) their invisibleness. This characteristic of software code, combined with the vast anonymity and 'interconnectivity' of cyberspace, presents profound challenges for the prosecution of individuals responsible for war crimes committed with cyberweapons*". In: SAXON, Dan. Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions. **Journal of Conflict and Security Law**, v. 21, n. 3, 2016. pp. 555–574. Disponível em: https://academic.oup.com/jcsl/article-abstract/21/3/555/2567000?redirectedFrom=fulltext Acesso em: 2 maio 2021.

campo de batalha e responsabilidade internacional dos Estados, todos no âmbito das operações cibernéticas.

4.2 Elementos Normativos do DICA

No âmbito normativo do Direito Internacional dos Conflitos Armados, muitos mecanismos poderiam relacionar-se com o conflito cibernético, porém, em nosso entendimento, os quatro mecanismos a seguir são adequados para bem entender a interação da guerra cibernética com o DICA.

4.2.1 ATAQUE

Conforme estabelece a Regra 92 do Manual Tallinn 2.0[9], o "ataque cibernético é uma operação cibernética, seja ofensiva seja defensiva, que provavelmente causará ferimentos ou morte a pessoas ou danos ou destruição de objetos"[10]. (tradução nossa).

Ainda nesse sentido, uma vez caracterizada a ação cibernética como um ataque, tal ato sofre as limitações e as restrições específicas do Direito Internacional dos Conflitos Armados, ou seja, civis e objetos civis estão sob proteção de ataques dessa natureza. Em outras palavras, os atos de violência não devem ser limitados às atividades militares que liberem força cinética; nessa esfera estão inseridos os ataques químicos, biológicos ou radiológicos, que, geralmente, não produzem efeitos cinéticos contra os alvos, mas, ainda assim, "é universalmente aceito que eles constituem ataques por questões legais"[11]. (tradução nossa)

---

9 Cf. SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017.

10 No original: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects". In: SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017.

11 No original (Regra 92.3): *"[…] is universally agreed that they constitute attacks as a matter of law".* In: SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017.

4.2.2 SOBERANIA

Os conceitos de soberania que conhecemos hoje tiveram início com a definição de razão de Estado, inaugurada pelo cardeal de Richelieu. Tal construção consistia na concepção de que o Estado não segue regras morais; os limites de sua atuação de Estado devem fundar-se, unicamente, no que é melhor para a manutenção da soberania estatal.

Nesse contexto, a chamada Paz de Vestfália retira o poder do Sacro Império Romano Germânico, consolidando os princípios da não intervenção e da autodeterminação na soberania dos Estados.

Segundo o princípio da não intervenção, um Estado não pode intervir na soberania de outro. O Estado e a sociedade nele existente podem conduzir a administração interna como melhor lhes convier.

Por outro lado, o princípio da autodeterminação introduz o conceito de Estado-Nação. Tal conceito é encarnado por uma comunidade que não só divide um mesmo território como se sente parte indivisível dessa porção de terra, partilhando de uma mesma história, bem como de um sentimento de pertencimento. Segundo esse princípio, cada nação tem o direito de se governar.

O Manual de Tallinn 2.0 ressalta que as atividades cibernéticas não estão além do alcance do princípio da soberania, pois “os Estados gozam da soberania sobre qualquer infraestrutura cibernética localizada em seu território e sobre as atividades associadas a essa infraestrutura”[12] (tradução nossa).

> Uma definição bem-aceita de “soberania” foi estabelecida na sentença arbitral da Ilha de Palmas de 1928. Ela estabelece que: “Soberania nas relações entre Estados significa independência. Independência em relação a uma parte do globo é o direito de exercer nela, com exclusão de qualquer outro Estado, as funções de um Estado.[13] (tradução nossa).

12 No original (Regra 1.1): *“[…] States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure”.* In: SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017.

13 No original (Regra 1.2): *“A well-accepted definition of 'sovereignty' was set forth in the Island of Palmas arbitral award of 1928. It provides that: 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State”.* In: SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017.

Portanto, as ações cibernéticas de um Estado devem respeitar os limites determinados pela soberania de outros Estados, tomando o cuidado de abster-se de executar ações dirigidas à infraestrutura cibernética localizada em território soberano.

4.2.3 CAMPO DE BATALHA

O termo *ciberespaço* ganhou notoriedade nas palavras do escritor William Gibson em sua obra “Neuromancer”; entretanto, para fins deste trabalho, serão apresentadas três definições dele: (i) segundo o dicionário Oxford, o ciberespaço é o local onde nos comunicamos por meio de uma rede de computadores interligados; (ii) nessa mesma linha, David Clark, do Instituto de Tecnologia de Massachusetts, conceitua ciberespaço como *“*um conjunto de computadores ligados em rede, na qual é eletronicamente armazenada e utilizada informação, onde tem lugar a comunicação”; (iii) por fim, o Departamento de Defesa dos Estados Unidos considera, além da internet, os sistemas de computadores, processadores e controladores como parte integrante do ciberespaço[14].

No que concerne às limitações geográficas, a Regra 81 do Manual Tallinn 2.0 estabelece que as “operações cibernéticas estão sujeitas a limitações geográficas impostas pelas disposições relevantes do direito internacional aplicável durante um conflito armado”[15] (tradução nossa). As questões legais de maior relevância incidem sobre a localização, seja das operações lançadas, seja do aparato instrumental utilizado, seja dos sistemas cibernéticos alvejados. De modo geral, as “operações cibernéticas podem ser realizadas *a partir de, em* ou *com efeitos em* todo o território das partes no conflito, águas internacionais ou espaço aéreo e, sujeito a certas limitações, espaço sideral”[16] (tradução nossa).

---

14 DIONÍSIO, Cátia S. Guerreiro. **A responsabilidade internacional dos Estados e operações cibernéticas**. Dissertação (mestrado em Direito), Universidade de Lisboa. Lisboa, 2018. Disponível em: https://repositorio.ul.pt/bitstream/10451/37376/1/ulfd136516_tese.pdf. Acesso em: 11 out. 2020.

15 No original: *“Cyber operations are subject to geographical limitations imposed by the relevant provisions of international law applicable during an armed conflict”.* In: SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017.

16 No original (Regra 81.1) *“[…] cyber operations may be conducted from, on, or with effects in the entire territory of the parties to the conflict, international waters or airspace, and, subject to certain limitations, outer space”.* In: SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017.

Deve ser salientado que as operações cibernéticas só devem produzir efeitos sobre os Estados envolvidos em conflito, devendo ser observado o princípio da neutralidade. Em outras palavras, como apresentado na Regra 151 do Manual Tallinn 2.0, o mero trânsito de dados em áreas vetadas à realização de operações cibernéticas não constitui uma ilicitude.

4.2.4 RESPONSABILIDADE INTERNACIONAL DOS ESTADOS

Tal responsabilidade pode ser considerada um princípio geral do Direito Internacional, ou seja, um Estado deverá assumir suas responsabilidades perante a comunidade internacional em consequência de conduta ilícita, a qual pode decorrer de delito ou violação a tratados e outras violações de um dever jurídico.[17]

Outra definição interessante ocorreu no julgamento do caso das reclamações britânicas relativas à zona espanhola de Marrocos, no qual o TPJI afirmou: “A responsabilidade é o corolário necessário de um direito. Todos os direitos de carácter internacional implicam responsabilidade internacional. Se a obrigação em causa não for cumprida, a responsabilidade acarreta o dever de reparação”[18].

Os Estados possuem, portanto, responsabilidade internacional por qualquer ação cibernética que constitua violação da obrigação legal internacional, conforme dispõe a Regra 14 do Manual Tallinn 2.0.

Como pudemos perceber, é clara a relação dos citados elementos normativos do Direito Internacional dos Conflitos Armados com as operações cibernéticas, estando guardada entre eles relevante sintonia. O exame não pode, contudo, esgotar-se nesses elementos. Constitui passo fundamental para perseguir o entendimento aqui buscado a realização de uma análise dos princípios do DICA, o que será objeto da próxima seção.

4.3 Princípios do DICA

Doravante, serão examinados os princípios norteadores do Direito Internacional dos Conflitos Armados, que, como bem leciona Cinelli (2011) “retiram

17 DIONÍSIO, Cátia S. Guerreiro. **A responsabilidade internacional dos Estados e operações cibernéticas**. Dissertação (mestrado em Direito), Universidade de Lisboa. Lisboa, 2018. Disponível em: https://repositorio.ul.pt/bitstream/10451/37376/1/ulfd136516_tese.pdf. Acesso em: 11 out. 2020.
18 Ibidem.

sua valoração de um único fundamento, síntese de toda a vida ética: a dignidade da pessoa humana". Sob esse mesmo ângulo, Cinelli (2011, apud Comparato, 2006, pp.481-484) também argumenta que:

> [...] a excelência do homem no mundo foi justificada a partir de três perspectivas, complementares e não excludentes: a religiosa, a filosófica e a científica. Na religiosa, o monoteísmo foi o que mais realçou a dignidade da pessoa humana. Na antropologia filosófica, a dignidade humana está ligada à sua condição de animal racional, nas diferentes manifestações da razão - especulativa, técnica, artística e ética e à consciência dessa sua singularidade no mundo. Na perspectiva científica, a espécie humana representa, sem contestação, o ápice do processo evolutivo. A dignidade da pessoa humana é o fundamento de toda a vida ética. Dela decorrem normas universais de comportamento, as quais representam a expressão dessa dignidade em todos os tempos e lugares, e têm por objetivo preservá-la. Elas atuam como o espírito que vivifica o corpo social e dá legitimidade a todas as estruturas de poder.

Com base nas ideias apresentadas por Cinelli (2011), estabeleceremos relações entre as operações cibernéticas e os princípios da (i) humanidade; da (ii) necessidade militar; da (iii) proporcionalidade; da (iv) limitação; e da (v) distinção.

4.3.1 PRINCÍPIO DA HUMANIDADE

O presente princípio apresenta como finalidade precípua evitar e/ou aliviar todo sofrimento humano decorrente dos efeitos da guerra, como analisa Borges (2006). Esse é considerado por muitos doutrinadores o princípio basilar do Direito Internacional dos Conflitos Armados. Nesse sentido, leciona Cinelli (2016):

> [...] nem mesmo o princípio do nullum crimen sine lege (não há crime sem lei anterior que o defina como tal) pode ser invocado por alguém que tenha cometido delitos contra o âmago da dignidade humana. Até mesmo Lênin o manteve em vigência após a Revolução Bolchevique de 1917, por considerá-lo "parte do patrimônio comum da humanidade".

Assim como os demais princípios do Direito Internacional dos Conflitos Armados, os ataques perpetrados no ciberespaço devem respeitar os limites da humanidade e evitar o sofrimento desnecessário. O Manual Tallinn 2.0 comunga desse entendimento quando, na Regra 104, condena as lesões supérfluas ou o sofrimento desnecessário, trazendo os seguintes dizeres em seu caput: "É proibido empregar meios ou métodos de guerra cibernética que possam causar ferimentos supérfluos ou sofrimento desnecessário[19]" (tradução nossa).

19 No original: *"It is prohibited to employ means or methods of cyber warfare that are of a nature to*

Exemplifica Cinelli (2016) que um consagrado dispositivo desse princípio é a Cláusula de Martens, a qual foi introduzida no preâmbulo da IV Convenção de Haia, de 1907, e reafirmada posteriormente no Protocolo Adicional I (1977) art. 1º:

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

4.3.2 PRINCÍPIO DA NECESSIDADE MILITAR

Como bem examina Lin (2012), o princípio da necessidade militar é antecedido pelo *jus in bello*, logo as operações de caráter militar devem ter como objetivo a derrota do inimigo no conflito e, portanto, servirem aos propósitos militares de maneira concreta e objetiva. Nessa mesma linha de raciocínio, Cinelli (2016) argumenta que esse princípio deve ser utilizado para conseguir a rendição ou degradação das forças do inimigo, contudo não deve ser tomado como absoluto, devendo haver uma ponderação entre os meios e métodos e a necessidade militar a ser buscada, conforme dispõe o art. 54 do Protocolo Adicional I de 1977:

> É proibido utilizar a fome dos civis como método de guerra. É proibido atacar, destruir, retirar ou pôr fora de uso bens indispensáveis à sobrevivência da população civil, tais como os gêneros alimentícios e as zonas agrícolas que os produzem, colheitas, gado, instalações e reservas de água potável e obras de irrigação, com o objetivo específico de privar a população civil ou a parte adversa de seu valor de subsistência, qualquer que seja o motivo que inspire aqueles atos. […] São permitidas a uma parte em conflito, em território sob seu controle, derrogações das proibições […] se necessidades militares imperiosas assim o exigirem.

Em outras palavras, a necessidade militar não pode ser uma “carta branca” para a utilização de quaisquer meios e métodos julgados necessários para alcançar o objetivo militar no conflito; deve, isto sim, ser conjugada com os demais princípios do Direito Internacional dos Conflitos Armados, como bem esclarecido por Dinstein (2012):

> [...] nem todos os objetivos militares são necessariamente de alto valor militar. No caso Blaskic, de 2000, um Tribunal de Julgamento do ICTY considerou que o “uso vigoroso” da artilharia, a fim de capturar aldeias

---

cause superfluous injury or unnecessary suffering”. In: SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017.

> habitadas principalmente (embora não exclusivamente) por civis, era "desproporcional à necessidade militar" devido à morte de civis e à destruição que estava prestes a ocorrer.[20] (tradução nossa)

O Manual Tallinn 2.0, em sua Regra 72, positiva a necessidade militar como um pilar a ser observado nas operações cibernéticas, pois "o uso da força envolvendo operações cibernéticas conduzidas por um Estado no exercício de seu direito de legítima defesa deve ser necessário e proporcional"[21] (tradução nossa).

4.3.3 PRINCÍPIO DA PROPORCIONALIDADE

O princípio da proporcionalidade, esclarece Cinelli (2016), é bem observado quando a ação militar não produz vítimas nem danos civis excessivos, isto é, os meios e métodos utilizados devem ser proporcionais à vantagem militar obtida, sendo que tal princípio pode ser observado no art. 57 do Protocolo Adicional I:

> (iii) abster-se de lançar um ataque do qual se possa esperar que venha a causar acidentalmente perdas de vidas humanas na população civil, ferimento nos civis, danos nos bens de caráter civil ou uma combinação dessas perdas e danos que seriam excessivos relativamente à vantagem militar concreta e direta esperada [...] Quando for possível escolher entre vários objetivos militares para obter uma vantagem militar equivalente, a escolha deverá recair sobre o objetivo cujo ataque seja susceptível de apresentar o menor perigo para as pessoas civis ou para os bens de carácter civil.

Como bem observa Jensen (2013), muitos princípios norteadores do Direito Internacional Humanitário são aplicáveis somente às operações militares, tais como os ataques num conflito armado. A esse grupo pertence o princípio da proporcionalidade.

Nem todos os ataques cibernéticos, todavia, podem ser classificados como ataques à luz do DICA. Dinstein (2012) mostra que os ataques às redes de computadores não estão automaticamente caracterizados como operações militares

---

20 No original: "But not all military objectives are necessarily of high military value. In the Blaskic case of 2000, an ICTY Trial Chamber held that the 'vigorous use' of artillery, in order to seize villages inhabited mostly (although not exclusively) by civilians was 'out of all proportion to military necessity' due to the civilian deaths and destruction that was bound to occur". In: DINSTEIN, Yoram. The Principle of Distinction and Cyber War in International Armed Conflicts. **Journal of Conflict and Security Law**, Volume 17, Issue 2, Summer 2012, Pages 261-277. Disponível em: https://academic.oup.com/jcsl/article/17/2/261/852776 Acesso em: 02 maio 2021.

21 No original: *"A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate".* In: SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017.

em conformidade com o Direito Internacional Humanitário e, em consequência disso, alguns deles, em especial os utilizados para espionagem e coleta de dados de inteligência, não se qualificam como ataques segundo a acepção do Direito Internacional dos Conflitos Armados.

Ainda nesse sentido, argumenta Jansen (2013) que o princípio da proporcionalidade só será aplicado quando a operação cibernética for caracterizada como um ataque dentro do escopo do DICA. Nesses casos, as operações deverão observar, em especial, o dano e os efeitos indiretos que poderão advir do ataque. Saxon (2016), com base em ponto de vista semelhante, entende que os danos causados por efeitos indiretos advindos das operações cibernéticas são de maior relevância quando se analisa esse princípio pelo prisma das ações realizadas no ciberespaço.

Droege (2012) afirma que tão somente as operações cibernéticas classificadas como ataques pela óptica do Direito Internacional dos Conflitos Armados estão sujeitas aos princípios de distinção, proporcionalidade e precaução.

Por sua vez, Lin (2012) exemplifica da seguinte maneira:

> Se, por exemplo, uma usina de energia é o alvo de um ataque cibernético, uma avaliação deve ser feita para verificar se o dano à população civil causado pela interrupção do serviço elétrico não é desproporcional à vantagem militar que pode resultar do ataque à usina.[22] (tradução nossa)

Como já afirmado no princípio anterior, o Manual Tallinn 2.0, em sua Regra 72, entende que o princípio da proporcionalidade, no âmago das operações cibernéticas, foi recepcionado pelo Direito Internacional dos Conflitos Armados.

4.3.4 PRINCÍPIO DA LIMITAÇÃO

O presente princípio estabelece que os meios e métodos empregados nos conflitos armados não são ilimitados. Devem, isto sim, ser observados os demais princípios antes de qualquer operação militar. Por seu turno, Cinelli (2016) esclarece que o art. 22 do Regulamento da IV Convenção de Haia (1907) afirmava que as

22 No original: *"If, for example, a power plant is the target of a cyber attack, an assessment must be made as to whether the harm to the civilian population caused by disruption of electrical service is not disproportionate to the military advantage that might ensue from attacking the plant."* In: LIN, Herbert. Cyber conflict and international humanitarian law. **International Review of the Red Cross**, v. 94, n. 886, 2012. Disponível em: https://international-review.icrc.org/articles/cyber-conflict-and-international-humanitarian-law. Acesso em: 2 maio 2021.

partes envolvidas na guerra não gozavam de direito ilimitado na escolha dos meios para derrotar a parte adversa, entendimento posteriormente ratificado pelo Protocolo Adicional I (1977), em seu art. 35: “em qualquer conflito armado, o direito de as partes no conflito escolherem os meios e métodos não é ilimitado”[23].

Cinelli (2016) ainda subdivide o princípio da limitação em (i) *ratione loci*, (ii) *ratione personae* e (iii) *ratione conditionis*:

(i) *ratione loci*: é proibido o ataque contra alvos considerados ilícitos, ou seja, aqueles cujos efeitos na população civil irão certamente superar os objetivos militares pretendidos. São exemplos desse tipo de alvo as construções dedicadas a abrigar obras de arte, os monumentos históricos, os locais de cultos religiosos e demais lugares considerados patrimônios culturais;

(ii) *ratione personae*: os ataques devem ser direcionados a alvos e objetivos militares, ou seja, as hostilidades devem ser voltadas às forças militares das partes envolvidas no conflito, conforme dispõe o art. 51 (1 e 2) do Protocolo Adicional I: “os civis e a população civil gozam de proteção geral contra os perigos resultantes de operações militares [...] São proibidos atos ou ameaças de violência com o objetivo principal de espalhar o terror no meio da população civil.”;

(iii) *ratione conditionis*: os meios e métodos empregados devem estar condicionados à missão militar, de modo a não ultrapassar os limites toleráveis e razoáveis de sofrimento. Essa condicionante guarda íntimo relacionamento com o princípio da proporcionalidade.

O princípio da limitação possui escopo pulverizado dentro das normas do Direito Internacional dos Conflitos Armados, todavia a Regra 94 do Manual Tallinn melhor representa esse princípio quando positiva em seu *caput* que: “A população civil como tal, bem como os civis individualmente, não devem ser objeto de ataque cibernético[24]”. (tradução nossa)

---

23 Cf. Convenções de Genebra. Comitê Internacional da Cruz Vermelha. Disponível em: https://www.icrc.org/pt/publication/os-protocolos-adicionais-convencoes-de-genebra-de-12-de-agosto-de-1949. Acesso em: 1º ago 2021.

24 No original: *“The civilian population as such, as well as individual civilians, shall not be the object of cyber attack”.* In: SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law Applicable to cyber operations**. New York: Cambridge University Press, 2017.

4.3.5 PRINCÍPIO DA DISTINÇÃO

Esse princípio encarna todo o corpo normativo do Direito Internacional dos Conflitos Armados destinado à proteção humana e seus bens, como muito bem ilustra Cinelli (2016), afirmando que tal princípio se baseia na definição do objetivo militar e impõe que as ações militares se pautem por essa determinação. Concomitantemente, com a adequada distinção entre civis e militares, estabelecem-se as dicotomias civis *versus* militares e bens civis *versus* objetivos militares.

Nesse diapasão, Dinstein (2012) apresenta o entendimento emanado pela Corte Internacional de Justiça, em sua Opinião Consultiva sobre Armas Nucleares, de 1996:

> Os princípios fundamentais contidos nos textos que constituem a estrutura do direito humanitário são os seguintes. O primeiro visa à proteção da população civil e dos bens civis e estabelece a distinção entre combatentes e não combatentes; os Estados nunca devem fazer de civis o objeto de ataque e, consequentemente, nunca devem usar armas que são incapazes de distinguir entre alvos civis e militares.[25] (tradução nossa)

O autor ainda conclui ser esse o conceituado princípio da distinção, aquele que se situa na origem do Direito Internacional dos Conflitos Armados, sendo parte integrante e inseparável do Direito Internacional Consuetudinário moderno. Está positivado no art. 48 do Protocolo Adicional I (1977) às Convenções de Genebra de 1949 e é denominado “regra básica”. Sua redação segue abaixo:

> As Partes do conflito devem, em todos os momentos, distinguir entre a população civil e os combatentes e entre os objetos civis e objetivos militares e, portanto, devem dirigir suas operações apenas contra objetivos militares.[26] (tradução nossa)

---

25 No original: *“The cardinal principles contained in the texts constituting the fabric of humanitarian law are the following. The first is aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants; States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets”.* In: DINSTEIN, Yoram. The Principle of Distinction and Cyber War in International Armed Conflicts. **Journal of Conflict and Security Law**, Volume 17, Issue 2, Summer 2012, Pages 261-277. Disponível em: https://academic.oup.com/jcsl/article/17/2/261/852776 Acesso em: 02 maio 2021.

26 No original: *“[…] the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives”.* In: DINSTEIN, Yoram. The Principle of Distinction and Cyber War in International Armed Conflicts. **Journal of Conflict and Security Law**, Volume 17, Issue 2, Summer 2012, Pages 261-277. Disponível em: https://academic.oup.com/jcsl/article/17/2/261/852776 Acesso em: 02 maio 2021.

Em seu relacionamento com as operações cibernéticas, o princípio da distinção ganha voz em Saxon (2010), que esclarece que, em conformidade com o Direito Internacional Humanitário, as normas de seleção de alvos, bem como os princípios da distinção e da proporcionalidade, devem ser obedecidas quando as partes lançam ataques cibernéticos, logo a violação de alguma dessas regras ensejaria um crime de guerra, positivado no Estatuto de Roma do Tribunal Penal Internacional (TPI).

Tal qual já estabelecido anteriormente, a aplicação do Direito Internacional dos Conflitos Armados às operações cibernéticas é limitada às ações que constituem um ataque sob a óptica do DICA. Segundo Droege (2012 apud Schmitt, 2011), operações cibernéticas psicológicas não estariam sujeitas ao princípio da distinção; para o autor, um bom exemplo de arma cibernética que respeitou o princípio da distinção foi o vírus Stuxnet, cuja ação se restringiu às usinas de enriquecimento de urânio no Irã. Mesmo esse vírus, todavia, apresentou efeitos indiretos indesejáveis. A questão, à qual não se pode fugir, é saber como controlar tais armas numa rede tão interligada como a internet, na qual há pouquíssima separação do que sejam redes exclusivamente militares e redes civis.

4.4 Síntese Conclusiva

Este trabalho partiu do questionamento acerca do caráter das operações de ataque cibernético à luz do Direito Internacional dos Conflitos Armados. Era preciso, de saída, saber se tais operações, que se dão em um espaço virtual, infringem os princípios do DICA. Essa questão nos conduz a outra: poderiam operações cibernéticas em tempos de paz ser consideradas atos de guerra cibernética? Em caso positivo, constituiriam infração ao DICA? Para responder a essas indagações, foi necessário, além da análise de certos conceitos, fazer o seguinte percurso: (i) definir a guerra cibernética enquanto guerra, (ii) identificar nos mecanismos normativos do DICA possíveis aplicações à guerra cibernética e, finalmente, (iii) contrastar as possibilidades de guerra cibernética com os princípios do DICA.

A esta altura, é-nos possível afirmar que as ações cibernéticas são, em certa medida, análogas aos conflitos armados, donde serem os fundamentos do Direito Internacional dos Conflitos Armados perfeitamente aplicáveis a elas. Em outras

palavras, uma vez caracterizadas as ações cibernéticas no espectro do conflito armado, tais ataques, operacionalizados no ciberespaço, deverão respeitar em toda sua amplitude, os princípios da humanidade, da necessidade militar, da proporcionalidade, da limitação e da distinção.

O uso do ciberespaço para fins militares é um campo que merece ser amplamente explorado. A atuação nessa área do conhecimento humano é muito recente, privando-nos, assim, de exemplos concretos para melhor compreensão do problema. Entretanto, de modo algum os princípios do DICA se afastam em razão da inovação tecnológica ou do ineditismo no emprego de meios e métodos de realizar ataques. Deve ser reforçado que o Protocolo Adicional I (1977), em seu art. 36, estabelece:

> Armas novas
> Durante o estudo, preparação aquisição ou adoção de uma nova arma, de novos meios ou de um novo método de guerra, a Alta Parte Contratante tem a obrigação de determinar se o seu emprego seria proibido, em algumas ou em todas as circunstâncias, pelas disposições do presente Protocolo ou por qualquer outra regra do direito internacional aplicável a essa Alta Parte Contratante.

Para melhor determinar a aplicabilidade dos princípios do Direito Internacional dos Conflitos Armados à guerra cibernética, buscamos nos seus mecanismos normativos alguns conceitos particularmente pertinentes a essa nova modalidade de conflito: (i) ataque, (ii) soberania, (iii) campo de batalha e (iv) responsabilidade internacional dos Estados.

Com base no Manual Tallinn 2.0, que nos serviu de referência neste trabalho, pudemos estabelecer um paralelo entre as operações cibernéticas e os conceitos estudados. Claro está que só uma operação cibernética classificada como ataque estará sujeita ao Direito Internacional dos Conflitos Armados. O simples trânsito de dados em áreas proibidas, por exemplo, não constitui por si só uma ilicitude.

No que se refere aos demais conceitos, resta claro que as ações realizadas no ciberespaço podem constituir ilegalidade, uma vez que descumpram os preceitos, por exemplo, de soberania e campo de batalha, ensejando responsabilidade do Estado diante de qualquer violação ao ordenamento jurídico internacional.

Para atingir os objetivos deste trabalho, nosso passo inicial foi definir a guerra cibernética enquanto guerra e, em seguida, proceder à classificação das operações

cibernéticas, pois, como bem conceituou Schmitt (2012), o regime jurídico aplicável é determinado em razão da natureza do conflito.

Foi demonstrado que as operações cibernéticas podem ser classificadas como conflito armado internacional e conflito armado não internacional, do que depende estarem submetidas ao regime do Direito Internacional Humanitário. Entretanto, alguns pressupostos devem ser considerados. Como bem apresentado pelo Comitê Executivo da International Law Association, o conflito armado não pode ser confundido com ações esporádicas, atos isolados, incidentes, distúrbios e tensões internas, banditismo etc. As ações precisam ser revestidas de um mínimo de intensidade e organização.

Em outras palavras, as ações cibernéticas, por si só, não constituem conflito armado e, assim, não estão automaticamente sujeitas à aplicação do DICA. Tais operações devem ter caráter militar, ou seja, devem constituir um ataque à luz dos preceitos do Direito Internacional Humanitário para que estejam sob o regime deste.

Nossa análise conduziu-nos, portanto, ao entendimento de que operações cibernéticas *em tempos de paz* não podem ser consideradas atos de guerra cibernética e, portanto, não constituem infração ao DICA.

Uma operação cibernética precisaria ocorrer em circunstância de conflito armado (internacional ou não internacional) para ser caracterizada como ataque, como operação militar, à luz do DICA, e para estar sob o manto protetor deste. Uma operação cibernética que se inicie no momento de paz, entretanto, pode constituir um ataque suficiente para desencadear uma situação de conflito armado e suas consequências.

Logo, ainda que, nessa hipótese, não houvesse infração ao Direito Internacional dos Conflitos Armados, seria possível aplicar as regras do Direito Internacional, do Direito Internacional dos Direitos Humanos ou ainda, conforme o caso, os regramentos internos, como a responsabilidade dos Estados diante das operações cibernéticas por estes realizadas, sofrendo o escrutínio das obrigações legais internacionais, recepcionadas pelo ordenamento jurídico interno.

A questão-chave deste trabalho, no entanto, era saber em que medida as operações realizadas no ciberespaço, *no contexto de guerra cibernética,* podem constituir uma infração ao DICA.

Desde que as operações realizadas no ciberespaço estejam no espectro dos conflitos armados e possam ser classificadas como ataques sob a óptica do Direito Internacional Humanitário, o conjunto normativo de regras do DICA atuará irrestritamente nestas ações e deverão ser respeitados todos os princípios, tais como a humanidade, a necessidade militar, a limitação, a proporcionalidade e a distinção. Deverão, ainda, ser observados os institutos da soberania e do campo de batalha, bem como deverá o Estado estar ciente de todas as suas responsabilidades perante a comunidade internacional.

5 CONCLUSÃO

Esta pesquisa partiu da necessidade de consolidar adequado tratamento jurídico a um fenômeno novo, a chamada guerra cibernética. Estaria o Direito Internacional dos Conflitos Armados apto a arbitrar esse tipo de conflito? O primeiro passo para avançar nessa discussão era buscar a conceituação de guerra no decorrer da história. Em seguida, era preciso examinar os mecanismos normativos do DICA a fim de verificar sua aplicabilidade à nova realidade e, finalmente, contrastar as possibilidades de guerra cibernética com os seus princípios.

No âmbito dessa discussão, formulamos a hipótese de que certas operações realizadas no espaço virtual em tempos de paz pudessem ser tomadas como atos de guerra cibernética, uma vez que eventuais violações de sigilo de dados, ainda que não perpetradas com claros objetivos bélicos, podem pôr em risco a segurança nacional.

Para caracterizar as espécies de operações realizadas no ciberespaço enquanto guerra à luz do Direito Internacional dos Conflitos Armados, foram revisitados autores clássicos e contemporâneos. Dessa forma, pudemos avançar na compreensão do fenômeno da guerra cibernética e sua subsunção ao regime jurídico do DICA, restando clara a sua classificação em conflitos armados internacionais e conflitos armados não internacionais, a depender da situação. Há que se destacar a preciosa contribuição do Comitê Executivo da International Law Association na definição de alguns pressupostos capitais, tais como “organização” e “intensidade” nas operações realizadas no contexto do conflito armado não internacional.

Uma vez definida a classificação das operações cibernéticas submetidas ao regime jurídico do Direito Internacional Humanitário, foi-nos possível identificar mecanismos normativos. Os institutos selecionados, a saber: (i) ataque, (ii) soberania, (iii) campo de batalha e (iv) responsabilidade internacional dos Estados, ao ratificarem a sintonia de tais conceitos com a guerra cibernética, permitiram o prosseguimento na pesquisa. Cabe aqui repisar o conceito de ataque, que, sob a égide do DICA, será aplicado às ações virtuais, como determinante para estabelecer o regime jurídico que governará as ações cibernéticas realizadas.

Compreendidos os exames anteriores, a pesquisa avançou para contrastar os princípios do Direito Internacional dos Conflitos Armados com a guerra cibernética. Sendo constatada a existência de um conflito armado no âmago das ciberoperações, os princípios da humanidade, necessidade militar, proporcionalidade, limitação e distinção deverão ser plenamente respeitados em todos os momentos das hostilidades. De modo algum se podem afastar os princípios do DICA em face do avanço científico dos armamentos bélicos ou do ineditismo no emprego de meios e métodos nas operações militares.

Destarte resta claro o atingimento do objetivo principal do trabalho, qual seja: *determinar em que medida as operações realizadas no ciberespaço, no contexto de guerra cibernética, podem constituir uma infração ao DICA*. Contanto que sejam caracterizadas como ataques à luz dos preceitos do Direito Internacional dos Conflitos Armados, as ações cibernéticas serão perfeitamente reguladas sob o regime jurídico do Direito Internacional Humanitário. A preliminar classificação das hostilidades é determinante para estabelecer as normas legais aplicáveis ao caso concreto.

Dessa forma, a hipótese aventada não se confirmou, uma vez que, ainda que possam representar ameaça à segurança nacional, as violações ocorridas no ciberespaço em tempo de paz não se caracterizam como ataque, pelo menos sob a égide do Direito Internacional dos Conflitos Armados, o que afasta a possibilidade de aplicação desse regime jurídico a situações dessa natureza.

Esta pesquisa, embora ilumine uma discussão de grande relevância, não traz soluções definitivas para o tratamento jurídico das operações realizadas no ciberespaço. O tema é pouco estudado no ordenamento jurídico nacional, motivo pelo qual nos socorremos, sobretudo, de contribuições doutrinárias estrangeiras.

A definição de conflito armado não internacional (em situações concretas, como terrorismo e eventos análogos), no contexto das guerras de quarta geração, constitui verdadeiro desafio ao operador jurídico-militar. O tema merece, portanto, ser mais explorado, principalmente no âmbito acadêmico das Forças Armadas.

REFERÊNCIAS

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

BRASIL. Ministério da Defesa. Comando da Aeronáutica. **Manual de trabalhos acadêmicos da UNIFA.** Rio de Janeiro, 2021.

BRASIL. Ministério da Defesa. MD35-G-01: **Glossário das Forças Armadas**. 2016. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em 16 dez. 2020.

CINELLI, Carlos Frederico. **Direito Internacional Humanitário**: ética e legitimidade na aplicação da força em conflitos armados. Curitiba: Jaruá, 2011.

CLAUSEWITZ, Carl Von. **Da Guerra**. Tradução do inglês para o português CMG (RRm) Luiz Carlos Nascimento e Silva do Valle, 1832.

CICV. Comitê Internacional da Cruz Vermelha. **Convenções de Genebra**. Disponível em: https://www.icrc.org/pt/publication/os-protocolos-adicionais-convencoes-de-genebra-de-12-de-agosto-de-1949. Acesso em: 1º ago 2021.

CRAWFORD, Emily e Pert, Alison. **International Humanitarian Law**. 2. ed. Cambridge: University Press, 2020.

DINSTEIN, Yoram. The principle of distinction and cyber war in international armed conflicts. **Journal of Conflict and Security Law**, v.17, n. 2, 2012. pp. 261-277. Disponível em: https://academic.oup.com/jcsl/article/17/2/261/852776" https://academic.oup.com/jcsl/article/17/2/261/852776. Acesso em: 2 mai. 2021.

DIONÍSIO, Cátia S. Guerreiro. **A responsabilidade internacional dos Estados e operações cibernéticas**. Dissertação (mestrado em Direito), Universidade de Lisboa. Lisboa, 2018. Disponível em:https://repositorio.ul.pt/bitstream/10451/37376/1/ulfd136516_tese.pdf. Acesso em: 11 out. 2020.

DROEGE, Cordula. Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. **International Review of the Red Cross**, v. 94, n. 886, 2012. Disponível em: https://international-review.icrc.org/sites/default/files/irrc-886-droege.pdf" https://international-review.icrc.org/sites/default/files/irrc-886-droege.pdf. Acesso em: 2 mai. 2021.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 6. ed. São Paulo: Atlas, 2017.

INTERNATIONAL LAW ASSSOCIATION. **Final report on the meaning of armed conflict in International Law (ILA 2010)**. Disponível em: http://www.rulac.org/assets/downloads/ILA_report_armed_conflict_2010.pdf"

http://www.rulac.org/assets/downloads/ILA_report_armed_conflict_2010.pdf. Acesso em: 4 jul. 2021.

INTERNATIONAL STRATEGY FOR CYBERSPACE. **Prosperity, security, and openness in a networked world**. Maio, 2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf" https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Acesso em: 2 mai. 2021.

JAAKKOLA, E. Designing conceptual articles: four approaches. **AMS Rev**. 10, 18–26 (2020). Disponível em: https://doi.org/10.1007/s13162-020-00161-0 Acesso em: 23 abr. 2021.

JENSEN, Eric Talbot. Cyber attacks: proportionality and precautions in attack. **International Law Studies.** n. 198, v. 89, 2013. Disponível em: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils" https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils. Acesso em: 2 mai. 2021.

LIN, Herbert. Cyber conflict and international humanitarian law. **International Review of the Red Cross**, v. 94, n. 886, 2012. Disponível em: https://international-review.icrc.org/articles/cyber-conflict-and-international-humanitarian-law. Acesso em: 2 mai. 2021.

SAXON, Dan. Violations of international humanitarian law by non-state actors during cyberwarfare: challenges for investigations and prosecutions. **Journal of Conflict and Security Law**, v. 21, n. 3, 2016. pp. 555–574. Disponível em: https://academic.oup.com/jcsl/article-abstract/21/3/555/2567000?redirectedFrom=fulltext. Acesso em: 2 mai. 2021.

SCHMITT N., Michael. Classification of cyber conflict**. Journal of Conflict and Security Law**, v.17, n. 2, 2012. pp.245–260. Disponível em: https://doi.org/10.1093/jcsl/krs018" https://doi.org/10.1093/jcsl/krs018. Acesso em: 2 mai. 2021.

SCHMITT N., Michael. **Tallinn manual on the International Law applicable to cyber warfare**, New York: Cambridge University Press, 2013.

SCHMITT N., Michael. **Tallinn manual 2.0 on the International Law applicable to cyber operations**. New York: Cambridge University Press, 2017.

RØISLIEN, Hanne Eggen. Thoughts on autonomous weapon systems and meaningful human control of cyber. **Open Democracy**, n.7, nov. 2014. Disponível em: https://www.opendemocracy.net/en/thoughts-on-autonomous-weapons-systems-and-meaningful-human-control-of-cyber/. Acesso em: 2 mai. 2021.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 7. ed. São Paulo: Atlas, 2007.