Operações cibernéticas em conflitos armados: o Direito Internacional Humanitário legitimaria a militarização do ciberespaço?[1]

Isabel Soares da Costa
Chefe da Divisão de Assuntos Humanitários e Migrações
Ministério das Relações Exteriores
ORCID: https://orcid.org/0000-0002-0473-4787
e-mail: isabel.costa@itamaraty.gov.br

Carlos Márcio Bicalho Cozendey
Secretário de Assuntos Multilaterais Políticos
Ministério das Relações Exteriores
e-mail: carlos.cozendey@itamaraty.gov.br

Larissa Schneider Calza
Chefe da Divisão de Defesa e Segurança Cibernética
Ministério das Relações Exteriores
e-mail: larissa.calza@itamaraty.gov.br

Revisores: Cláudia Márcia Ramalho Moreira Luz (e-mail: claudia.luz@mpm.mp.br)
Cláudia Aguiar Britto (ORCID: https://orcid.org/0000-0002-4229-7952;
CV Lattes: http://lattes.cnpq.br/7455964413594325)
e-mail: claudiaaguiarbritto@gmail.com

[1]As opiniões expressas neste artigo são de responsabilidade de seus autores e não representam necessariamente a posição do Ministério das Relações Exteriores do Brasil.

Data de recebimento: 30/09/2024
Data de aceitação: 30/10/2024
Data da publicação: 25/11/2024

RESUMO: O uso de operações cibernéticas em conflitos armados é uma realidade contemporânea. As consequências do uso de tecnologias de informação e comunicação (TICs) com fins militares têm preocupado a comunidade internacional e motivaram a inclusão do tema na agenda das Nações Unidas. Embora a maioria dos Estados considere que o Direito Internacional Humanitário (DIH) se aplica ao ciberespaço, o tema desperta controvérsias em contexto geopolítico de polarização. Este artigo apresenta a posição de diferentes Estados sobre a aplicação do DIH no ciberespaço nas negociações do Grupo de Trabalho Aberto (OEWG) da ONU e discute o argumento de que a aplicação do DIH às atividades dos Estados no ciberespaço equivaleria a legitimar a militarização desse domínio. Conclui-se pela necessidade de esforços conjuntos para promover uma agenda para a paz no ciberespaço, o que pode incluir debate a respeito da necessidade de novas normas para fortalecer a proteção dos civis e da infraestrutura civil.

PALAVRAS-CHAVE: conflitos armados; Direito Internacional Humanitário; ciberespaço; militarização; Nações Unidas.

ENGLISH

TITLE: Does International Humanitarian Law Legitimize the Militarization of Cyberspace?

ABSTRACT: The use of cyber operations in armed conflicts is a contemporary reality. The consequences of the use of information and communication technologies (ICTs) for military purposes have concerned the international community and motivated the inclusion of the topic on the United Nations agenda. Although most states consider that International Humanitarian Law (IHL) applies to cyberspace, the topic raises controversies in a polarized geopolitical context. This article presents the position of different states on the application of IHL in cyberspace and discusses the

argument that the application of IHL to state activities in cyberspace would legitimize the militarization of this environment.

KEYWORDS: armed conflicts; International Humanitarian Law; cyberspace; militarization; United Nations.

SUMÁRIO

1 INTRODUÇÃO

O uso de operações cibernéticas em conflitos armados é uma realidade. A doutrina militar tem descrito o ciberespaço como "o quinto campo de batalha"[2], com base no reconhecimento de que ataques cibernéticos podem constituir ameaças vitais aos interesses e à segurança de um Estado e que, em determinadas circunstâncias, seriam comparáveis a um ato de guerra.

No aniversário dos 75 anos das Convenções de Genebra, a presidente do Comitê Internacional da Cruz Vermelha defendeu a importância de que os Estados garantam que o uso de novas tecnologias de guerra, como as operações cibernéticas e a inteligência artificial, adiram estritamente ao DIH (CICV, 2024). Esse foi um dos quatro temas levantados na ocasião, o que demonstra sua centralidade como parte dos desafios contemporâneos do direito dos conflitos armados.

[2] Juntamente com terra, mar, ar e espaço.

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

O relatório "Desafios do Direito Internacional Humanitário (DIH)" de 2024 reconhece que a regulamentação em um ambiente de guerra tecnologicamente avançado faz parte das questões cruciais para a proteção de civis na contemporaneidade[3].

As TICs são frequentemente usadas para causar danos ou perda de funcionalidade em infraestruturas civis críticas, como reservatórios e sistemas de distribuição de água, usinas de eletricidade, redes de transmissão de energia, ou serviços médicos (CICV, 2024). Sua disciplina, portanto, está relacionada ao tema da proteção de civis durante conflitos armados.

As consequências do uso de tecnologias de informação e comunicação (TICs) para fins militares têm preocupado a comunidade internacional e motivaram a inclusão do tema na agenda das Nações Unidas, na forma de um grupo de trabalho aberto vinculado à Primeira Comissão da Assembleia Geral, responsável por temas relacionados ao desarmamento e à segurança internacional.

Embora a maioria dos Estados considere que o Direito Internacional Humanitário (DIH) se aplica ao ciberespaço, o tema continua a despertar controvérsias em contexto geopolítico de polarização. Discussões a respeito de como as normas da guerra devem ser interpretadas em casos de operações cibernéticas conduzidas durante conflitos armados estão entre as mais sensíveis do debate a respeito da aplicação do direito internacional ao ciberespaço.

O Comitê Internacional da Cruz Vermelha (CICV) calcula, no total, 120 conflitos armados em andamento em todo o mundo no ano de 2024

[3] *Cf.:* https://t.co/zjMHTyAJWy. Acesso em: 12 set. 2024.

(CICV, 2024). Embora poucos Estados tenham reconhecido publicamente recurso a meios cibernéticos em operações militares, o Comitê estima que mais de 100 desenvolveram ou estejam desenvolvendo capacidades militares cibernéticas, em diferentes regiões, inclusive os 5 membros permanentes do Conselho de Segurança (CICV, 2024).

No âmbito multilateral, é possível concluir que a avaliação do Comitê é compartilhada pelos Estados:

> [...] vários Estados estão desenvolvendo capacidades de tecnologias de informação e comunicação (TICs) para fins militares. Eles também lembraram que o uso de TICs em futuros conflitos entre Estados está se tornando mais provável e **notaram que as TICs já foram usadas em conflitos em diferentes regiões. O aumento contínuo de incidentes envolvendo o uso malicioso de TICs por atores estatais e não estatais, incluindo terroristas e grupos criminosos, é uma tendência perturbadora**. Alguns atores não estatais demonstraram capacidades de TIC anteriormente disponíveis apenas para Estados (AGNU, A/75/816, 2021.Grifo nosso. Tradução nossa)[4].

Essa realidade levou ao reconhecimento de que também no ciberespaço se aplica o Direito Internacional[5] e, em contextos de conflitos armados, o Direito Internacional Humanitário (DIH).

Em relação ao direito internacional, a linguagem consensuada foi a de que "o direito internacional, em particular a Carta das Nações Unidas, é aplicável e essencial para manter a paz, a segurança e a estabilidade no uso

[4] "States recalled that a number of States are developing ICT capabilities for military purposes.8 They also recalled that the use of ICTs in future conflicts between States is becoming more likely, and noted that ICTs have already been used in conflicts in different regions. The continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States." (A/75/816 (2021), anexo I, para. 16

[5] Resoluções da Assembleia Geral das Nações Unidas A/68/98 (2013), A/70/174 (2015), A/70/174 (2015), A/76/135 (2021, para 71(f)) e A/78/265(2023).

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

das tecnologias de informação e comunicação (TICs) pelos Estados (AGNU, A/75/816, 2021).

Questões relacionadas à manutenção da paz e da segurança internacionais, portanto, estão no centro dessas discussões, mais do que polêmicas jurídicas a respeito do direito aplicável em cada operação individualmente considerada.

Em relação ao DIH, por sua vez:

> O Grupo observou que o direito internacional humanitário se aplica apenas em situações de conflito armado. Ele relembra os princípios legais internacionais estabelecidos, incluindo, quando aplicável, os princípios de humanidade, necessidade, proporcionalidade e distinção que foram mencionados no relatório de 2015. O Grupo reconheceu a necessidade de mais estudos sobre como e quando esses princípios se aplicam ao uso das TICs pelos Estados e **ressaltou que relembrar esses princípios de forma nenhuma legitima ou encoraja o conflito**." (AGNU, A/76/135, 2021. Grifo nosso. Tradução nossa).[6]

Essa relação entre o DIH e a possível legitimação da guerra surgiu em reiteradas ocasiões desde a proscrição do uso ou ameaça do uso da força como meio de resolver disputas pelo Artigo 2(4) da Carta das Nações Unidas (*jus contra bellum*)[7].

O argumento de que o DIH seria instrumento para "legitimação" da guerra, no entanto, não foi levantado apenas nos últimos 20 anos, quando

[6] The Group noted that international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognised the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles byno means legitimizes or encourages conflict.

[7] Art. 2(4) da Carta da Nações Unidas.

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0,
Qualis B4, DOI: 10.5281/zenodo.14203542

foram iniciados os debates sobre a aplicação do DIH no ciberespaço. Ao contrário, tem sido apresentado em diferentes ocasiões.

Quando da aprovação do Protocolo Adicional I às Convenções de Genebra, na década de 1970, por exemplo, foi necessário incluir em seu preâmbulo que "nenhuma disposição do presente Protocolo nem das Convenções de Genebra de 12 de agosto de 1949 **pode ser interpretada no sentido de legitimar ou autorizar qualquer ato de agressão ou qualquer outro uso da força incompatível com a Carta das Nações Unidas**".

O DIH toma a guerra como um fato, e não se ocupa com aspectos relacionados ao *jus ad bellum*; logo, o argumento de que a aplicação do DIH às atividades dos Estados no ciberespaço equivaleria a legitimar a militarização desse ambiente não deve prosperar.

O objetivo deste artigo é oferecer uma introdução descritiva dos aspectos mais relevantes dos debates multilaterais a respeito da aplicação das normas de DIH no contexto cibernético, por considerar que os desafios relacionados à compreensão e interpretação do direito da guerra em sua aplicação ao ciberespaço não tem somente natureza jurídica. Não incluirá, portanto, interpretações a respeito das normas aplicáveis ao ciberespaço (*lege lata*), nem da eventual existência de lacunas normativas. Tampouco será realizado exercício de deontologia, das normas como "deveriam ser".

O artigo argumenta que reconhecer a aplicabilidade das normas do DIH no ciberespaço não encoraja sua militarização, mas impõe limites ao uso de operações cibernéticas durante conflitos armados, de acordo com os propósitos e objetivos do *jus in bellum*.

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

Embora o uso de ferramentas cibernéticas por atores não estatais seja uma realidade preocupante, este trabalho enfocará apenas no uso das tecnologias de informação e comunicação (TICs) por Estados.

Este artigo é composto por cinco seções. Após introdução a respeito do contexto e da relação entre as operações cibernéticas e o DIH, será analisado o argumento a respeito da militarização do ciberespaço.

Serão comentadas as negociações multilaterais relevantes para a aplicação do jus in bello no ciberespaço, em visão geral das discussões multilaterais sobre operações cibernéticas durante conflitos armados, com foco nos argumentos sobre a aplicabilidade do DIH a essas operações e a relação entre o DIH e a Carta da ONU.

Em seguida, serão tecidas breves considerações a respeito das posições dos principais atores envolvidos, assim como a posição brasileira. Por fim, serão explicitados os principais desafios para o futuro em relação aos esforços conjuntos necessários ao objetivo de promover a paz no ciberespaço, o que pode incluir debate a respeito da necessidade de novas normas para fortalecer a proteção dos civis e da infraestrutura civil na atualidade.

Para tanto, foi realizada análise documental das negociações multilaterais no âmbito das Nações Unidas, incluindo os relatórios dos Grupos de Peritos Governamentais (GGE) e do Grupo de Trabalho Aberto (OEWG), bem como das posições nacionais submetidas pelos Estados. Examinou-se também a literatura especializada.

Limitação importante da pesquisa é a prevalência de informações classificadas ou não divulgadas publicamente pelos Estados nesse tema, o

que leva a viés devido à maior disponibilidade de informações de certos países ou regiões. Ainda assim, foi possível realizar análise abrangente e sistemática do estado atual das discussões sobre a aplicação do DIH no ciberespaço.

2 O QUE É MILITARIZAÇÃO DO CIBERESPAÇO

2.1 Escopo

A militarização do ciberespaço, para os fins deste artigo, refere-se ao desenvolvimento e utilização de capacidades militares no domínio cibernético, ou seja, o uso de operações cibernéticas direcionadas a objetivos militares específicos em contextos de conflitos armados, o que é possível por meio do desenvolvimento de capacidades cibernéticas ofensivas e defensivas por parte de Estados ou atores não governamentais.

A título de exemplo, os Estados Unidos, o Reino Unido e a Austrália reconheceram publicamente a utilização de operações cibernéticas contra o grupo Estado Islâmico. Há relatos, na doutrina especializada, de que operações cibernéticas foram realizadas em outros países envolvidos em conflitos armados, como a Geórgia em 2008, a Ucrânia desde 2015 e a Arábia Saudita em 2017, embora os autores desses ataques cibernéticos permaneçam desconhecidos e a atribuição de responsabilidade seja contestada (Gisel, 2020).

É importante, no entanto, esclarecer que a maior parte das operações cibernéticas não tem relação direta com conflitos armados e que os chamados "ataques cibernéticos" não são sinônimos de "ataque" como entendido pelo

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

DIH, nos termos do Protocolo Adicional I, artigo 49(1), ou seja, atos de violência contra um adversário, seja de ataque, seja de defesa.

A imensa maioria do que se chama de "ataques cibernéticos" envolve danos econômicos, espionagem, roubo de identidade, danos à reputação ou outras situações sujeitas a legislações domésticas. Operações cibernéticas relevantes para o DIH, portanto, são pequeno subconjunto das ações ou intervenções maliciosas no ciberespaço.

Do ponto de vista político, ressalte-se que a ausência de conflito armado não necessariamente configura situação "pacífica". Operações que não atingem o limiar de "ataque" foram chamadas de "acts of unpeace" na tipologia de Lucas Kello, para quem, muitas vezes, "o conflito cibernético ocorre no espectro entre os polos de guerra e paz" e "os métodos não-violentos de 'não-paz' podem ser fontes mais potentes de poder e influência nacional do que a violência aberta da guerra Clausewitziana" (Kello, 2022).

Observa-se o uso cada vez mais difundido de operações cibernéticas como alternativa ou complemento às operações militares cinéticas, não necessariamente atraindo a aplicação do DIH.

Por outro lado, uma operação cibernética pode, em tese, por si só, ser de tal gravidade, ter efeito tão significativo e duradouro, que poderia ser qualificada como ataque que constitui o início de um conflito armado, o que requer hostilidades sistemáticas, ou seja, envolvendo uso de força armada de certa extensão, duração e intensidade (Fleck, 2021, p. 48).

Essa possibilidade foi reconhecida pelo Brasil em sua posição nacional, como se verá a seguir, de forma que um ciberataque pode equivaler ao uso proibido da força sob o Artigo 2(4) da Carta da ONU, embora a

questão de quando um ciberataque poderia constituir “uso da força” ou equivaler a um ataque armado não tenha sido explicitado.

A posição do CICV é bastante clara: “o direito internacional humanitário não incentiva a militarização nem legitima o conflito em qualquer domínio” e não deve ser “interpretado como legitimando ou autorizando qualquer ato de agressão ou qualquer outro uso da força incompatível com a Carta das Nações Unidas” (CICV, 2019).

2.2 Contexto histórico

A criação da Organização das Nações Unidas (ONU) em 1945 e a adoção das Convenções de Genebra de 1949 pertencem ao mesmo momento histórico: o pós-Segunda Guerra Mundial.

As Convenções de Genebra, instrumentos ratificados por 196 países, normas universalmente reconhecidas, portanto, inauguraram o DIH contemporâneo. As tragédias que o mundo experimentou durante a Segunda Guerra Mundial foram o pano de fundo para a adoção de novas proteções para prisioneiros de guerra e para os feridos e doentes, bem como de formulação de uma nova convenção para a proteção de civis em tempos de guerra.

Naquele contexto, argumentava-se que seria desnecessário e “derrotista” que o DIH fosse debatido nas Nações Unidas, tendo em conta a obrigação prevista na Carta de São Francisco de que os Estados devem se abster, em suas relações internacionais, de recorrer à ameaça ou ao uso da força contra a integridade territorial ou a independência política de qualquer

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

Estado, ou de qualquer outra forma incompatível com os propósitos das Nações Unidas (Artigos 2(4) e 51).

Em que pese esse período inicial de reticência, nos últimos 75 anos, a ONU contribuiu para consolidar o direito internacional humanitário, em reconhecimento de que o DIH estabelece limites que devem ser respeitados na infeliz e indesejável situação de um conflito armado, independentemente de a Carta da ONU ter sido violada (Oberleitner, 2022). Assim, a distinção entre 'guerra justa' (*bellum justum*) e 'guerra injusta' (*bellum injustum*) é irrelevante para a incidência do DIH.

O Conselho de Segurança, principalmente por meio de sua agenda de Proteção de Civis, mas também os órgãos de direitos humanos da ONU tornaram-se ferramentas importantes no monitoramento ao respeito ao direito internacional humanitário e na investigação de suas violações (Benedetti, 2023). Não há dúvidas, por exemplo, de que o DIH se aplica às operações de paz da ONU, com base no direito internacional humanitário consuetudinário.

2.3 O DIH como legitimação da guerra?

No contexto das discussões sobre a aplicabilidade do DIH às operações cibernéticas durante conflitos armados, alguns Estados expressaram oposição à militarização do ciberespaço e demonstraram preocupação com uma possível "corrida armamentista cibernética". Expressaram também preocupações quanto à legitimação do uso de operações cibernéticas para fins militares e advogaram, em decorrência, por prudência na discussão da aplicabilidade do DIH (Gisel, 2020).

Qualquer recurso à força pelos Estados, seja de natureza cibernética ou cinética, é regulado pela Carta das Nações Unidas e pelo direito internacional. Sendo assim, qualquer disputa entre estados deve ser resolvida por meios pacíficos, tanto no ciberespaço, como em todos os outros domínios, nos termos do Art. 33.

O DIH toma a existência de um conflito armado como um fato da realidade, e não deveria, portanto, ser interpretado como um aval para o uso da violência, mas sim como um conjunto de normas que limitam e regulam as atividades cibernéticas também durante conflitos armados, restringindo a escolha dos beligerantes sobre os meios e métodos de guerra, independentemente de o uso da força ser ou não lícito.

Em vez de legitimar operações cibernéticas, ou qualquer outra operação militar durante um conflito armado, o *jus in bello* estabelece limites adicionais àqueles encontrados na Carta da ONU.

Afirmar que o DIH se aplica às operações cibernéticas durante um conflito armado não é incentivo para militarizar o ciberespaço e não deve, de forma alguma, ser entendido como uma legitimação da guerra cibernética, assim como a aplicação do DIH a conflitos armados não representa incentivo ao uso da força (AGNU, A/76/136, 2021)[8].

Ao contrário, o DIH impõe restrições à militarização do ciberespaço ao limitar os meios e métodos de guerra, por exemplo, o "desenvolvimento de capacidades cibernéticas que se qualificassem como armas e fossem, por

[8] Compêndio oficial de contribuições nacionais voluntárias sobre o tema de como o direito internacional se aplica ao uso de tecnologias de informação e comunicação pelos Estados, submetido por peritos governamentais participantes do Grupo de Peritos Governamentais sobre o Avanço do Comportamento Responsável dos Estados no Ciberespaço no Contexto da Segurança Internacional, estabelecido nos termos da resolução 73/266 da Assembleia Geral.

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

natureza, indiscriminadas ou causassem ferimentos supérfluos ou sofrimento desnecessário" (Gisel, 2020).

Cabe ressaltar, ademais, a decisão paradigmática da Corte Internacional de Justiça (CIJ) na Opinião Consultiva sobre o Uso das Armas Nucleares que reconhece que o DIH se aplica a todos os meios e métodos de guerra: passados, presentes e futuros (ICJ, 1996, p. 259).

3 NEGOCIAÇÕES MULTILATERAIS

A comunidade internacional está cada vez mais interessada em institucionalizar aspectos civis e militares da segurança cibernética, em diversos foros multilaterais.

Os desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional têm sido discutidos pela Assembleia Geral da ONU desde 1998 (Resolução 53/70, de 4 de janeiro de 1999), quando a Rússia apresentou seu projeto de resolução à Primeira Comissão da Assembleia Geral das Nações Unidas (AGNU).

Desde então, a Assembleia Geral da ONU adotou várias resoluções sobre o assunto. Uma das principais evoluções desse período foi o estabelecimento de seis sucessivos Grupos de Peritos Governamentais (GGE) sobre Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional em 2004, 2009, 2012, 2014, 2016 e 2019.

Os peritos governamentais que participaram do primeiro GGE da ONU em 2004, contudo, não conseguiram chegar a um consenso e nenhum

relatório foi adotado. Os três GGEs subsequentes elaboraram relatórios consensuais, inclusive sob presidência brasileira, que estabelecem normas voluntárias de comportamento responsável dos Estados nos usos das TICs. Em 2010 (UN Doc A/65/201), 2013 (UN Doc A/68/98), 2015 (UN Doc A/70/174) e 2021 (UN Doc A/76/135) foram adotados relatórios de consenso que foram reconhecidos pela Assembleia Geral da ONU. O relatório do terceiro GGE da ONU, de 2013, é um marco porque afirmou a aplicabilidade do direito internacional, especialmente a Carta da ONU, ao ciberespaço, o que foi posteriormente reafirmado no relatório de 2015.

Pela resolução 70/237 da Assembleia Geral, os Estados-Membros concordaram por consenso em ser guiados no uso das TICs pelo relatório de 2015 do GGE que elencou 11 regras (voluntárias) de comportamento responsável dos Estados no uso das TICs, consolidando, assim, uma estrutura inicial para o tema.

Ressalte-se que os especialistas participantes do GGE 2016-2017 não conseguiram chegar a consenso e, portanto, não adotaram relatório, por desentendimentos relacionados ao direito internacional.

China, Cuba e Rússia foram contrárias ao parágrafo 34 da minuta de relatório, que tratava do uso de contramedidas em casos de atos ilícitos internacionais, legitima defesa nos termos do Artigo 51 da Carta da ONU e direito internacional humanitário (Delerue, 2020).

O ministério das Relações Exteriores da Rússia publicou explicação de sua posição, rejeitando a aplicação do DIH ao ciberespaço (Federação Russa, 2020):

> **Há ênfase excessiva em certos ramos do direito internacional, incluindo o direito internacional**

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

> **humanitário** (DIH), direito internacional penal, bem como o direito internacional dos direitos humanos. **Consideramos potencialmente perigosas as tentativas de impor o princípio da aplicabilidade plena e automática do DIH ao ambiente das TICs em tempos de paz**. Essa afirmação em si é ilógica e contraditória, pois o DIH é aplicado apenas no contexto de um conflito armado, enquanto **atualmente as TICs não se enquadram na definição de uma arma**.[9]

A China também teria rejeitado a linguagem proposta, segundo relatos, embora não tenha feito declarações públicas a respeito do tema nessa ocasião.

Cuba, por sua vez, defendeu que "devem existir instrumentos para promover a paz, não para promover a guerra, o uso da força, o intervencionismo, a desestabilização, o unilateralismo ou ações terroristas" e que "não se deve converter o ciberespaço em um teatro de operações militares e legitimar, nesse contexto, ações de força punitiva unilateral, incluindo a aplicação de sanções e até mesmo ações militares por Estados que alegam ser vítimas de usos ilícitos das TICs." Argumentou, por fim, em relação "à suposta aplicabilidade no contexto das TIC dos princípios do Direito Internacional Humanitário", que "não podemos aceitar tal afirmação, pois isso legitimaria um cenário de guerra e ações militares no contexto das TIC" (Cuba, 2017).

É importante ressaltar, nesse contexto, que Rússia e Cuba defendem a necessidade de um novo tratado para regular a aplicação do Direito

[9] "Overwhelming emphasis is placed on certain branches of international law including international humanitarian law (IHL), international criminal law, as well as international human rights law. We regard as potentially dangerous the attempts to impose the principle of full and automatic applicability of IHL to the ICT environment in peacetime. This statement itself is illogical and contradictory, because IHL is applied only in the context of a military conflict while currently the ICTs do not fit the definition of a weapon".

Internacional ao ciberespaço, não estando sua posição relacionada à rejeição da incidência do Direito Internacional nesse meio.

O relatório do último GGE (AGNU, A/76/135, 2021) foi o primeiro documento a mencionar explicitamente o DIH, ao reconhecer que se aplica apenas em situações de conflito armado e ressalvar que esse reconhecimento não legitima ou encoraja o conflito.

O primeiro Grupo de Trabalho Aberto (OEWG, na sigla em inglês) sobre desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional, por sua vez, foi estabelecido em 2018 como grupo aberto a todos os Estados-membros da ONU, permitindo ampla participação e diversidade de perspectivas, e se reuniu entre 2019 e 2021. Mandato[10] para um segundo OEWG foi dado para o período 2021-2025 pela resolução A/RES/75/240.

No relatório final adotado pelo primeiro grupo em 2021, não há menções ao direito internacional humanitário (OEWG, 2021). O representante australiano, em sua intervenção de explicação de posição, resumiu o estado das negociações àquela altura:

> A Austrália saúda o fato de o Grupo de Trabalho Aberto ter adicionado aos acordos anteriores a confirmação de que meios pacíficos [de soluções de controvérsias] se aplicam ao ciberespaço. **Lamentamos que um pequeno número de delegações tenha continuado a resistir ao reconhecimento específico no relatório de que o direito internacional humanitário (DIH) se aplica às atividades cibernéticas em conflitos armados.**
> **A Austrália entende que essas delegações não se opõem à aplicação do DIH em si, mas sim à inclusão de tal**

[10] Seu mandato é continuar construindo entendimentos comuns em seis pilares: (i) ameaças existentes e potenciais; (ii) normas de comportamento responsável; (iii) direito internacional; (iv) medidas de construção da confiança; (v) construção de capacidades; e (vi) diálogo regular institucional (definição de espaço permanente de debate do tema).

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

> **referência no relatório, com o argumento de que tal referência incentivaria a militarização do ciberespaço. Nesse sentido, a Austrália recorda a posição tomada pelo CICV de que o reconhecimento da aplicação do DIH não encoraja a militarização, nem legitima o recurso ao conflito em qualquer domínio**. Notamos também o reconhecimento no relatório de que "o uso das TICs em futuros conflitos entre estados está se tornando mais provável" [na seção de "ameaças"]. Embora a Austrália lamente sua ausência no Relatório Substantivo, saudamos as referências ao DIH no Resumo do Presidente. (ONU, 2021. Grifo nosso. Tradução nossa, acervo dos autores).

O resumo do presidente do primeiro OEWG, o embaixador Jürg Lauber, da Suíça, é também bastante elucidativo para compreensão do quadro parlamentar dessas negociações multilaterais, ao registrar posições que atraíram apoio substancial, mas que não lograram o necessário consenso para serem incorporadas ao relatório final:

> 12. Recordou-se que o direito internacional é base para a estabilidade e previsibilidade nas relações entre Estados. Em particular, o direito internacional humanitário reduz riscos e potenciais danos tanto para civis e objetos civis quanto para combatentes no contexto de um conflito armado. Ao mesmo tempo, **os Estados enfatizaram que o direito internacional humanitário não incentiva a militarização nem legitima o recurso ao conflito em qualquer domínio**.
> (…)
> 18. Embora se tenha recordado que o direito internacional, e em particular a Carta das Nações Unidas, se aplica ao uso das TICs, foi destacado que **certas questões sobre como o direito internacional se aplica ao uso das TICs ainda não foram totalmente esclarecidas**. Alguns Estados propuseram que tais questões incluam, entre outras, o tipo de atividade relacionada às TICs que pode ser interpretada por outros Estados como uma ameaça ou uso da força (Art. 2(4) da Carta) ou que possa dar a um Estado motivo para invocar seu direito inerente de autodefesa (Art. 51 da Carta). Elas também incluem questões relevantes sobre como os princípios do direito internacional humanitário, tais como os princípios de humanidade, necessidade, proporcionalidade, distinção e precaução, se aplicam às operações de TICs.

> Nesse sentido, alguns Estados observaram que as discussões sobre a aplicabilidade do direito internacional humanitário ao uso das TICs pelos Estados precisam ser abordadas com prudência. Os Estados notaram que é necessário um estudo mais aprofundado sobre esses tópicos importantes em discussões futuras." (ONU, 2021. Grifo nosso).

O último relatório de progresso anual do segundo OEWG, presidido pelo Embaixador Burhan Gafoor, de Singapura, adotado em julho de 2024, demonstra que as delegações permanecem divididas quanto à aplicabilidade do direito internacional sobre as TICs e quanto às normas de comportamento responsável, à luz das tensões geopolíticas e da intensa polarização que é observada desde o início do conflito entre Rússia e Ucrânia. Foi possível, contudo, acordo a respeito dos elementos fundamentais do mecanismo que sucederá o OEWG após 2025: (i) que será um único mecanismo permanente, de liderança estatal, sob os auspícios das Nações Unidas, reportando-se à Primeira Comissão da Assembleia Geral; (ii) que terá como objetivo continuar a promover um ambiente de TIC aberto, seguro, estável, acessível, pacífico e interoperável; (iii) que tomará como base de seu trabalho o marco de comportamento responsável do Estado no uso de TICs acordado em relatórios anteriores do OEWG e GGE; e (iv) que será um processo aberto, inclusivo, transparente, sustentável e flexível, capaz de evoluir de acordo com as necessidades dos Estados e com os desenvolvimentos no ambiente das TICs.

É importante ressaltar que a posição cubana foi modulada desde 2017. Na posição nacional publicada em 28 de junho de 2024, o país reconheceu que o DIH se aplica ao ciberespaço em situações de conflitos armados:

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

> 16. O Direito Internacional Humanitário (DIH) só se aplica em situações de conflito. A aplicabilidade do DIH não está limitada ao ciberespaço, nem a qualquer outro âmbito físico ou abstrato. Da mesma forma, os objetivos que não são considerados legítimos nem em tempo de guerra são objetivos que se protegem contra todo tipo de ataques ou ações, sejam cibernéticas ou não.
>
> 17. Para a República de Cuba, todos os Estados têm a obrigação de cumprir e fazer cumprir o DIH, embora lamentavelmente um Estado tenha objetado refletir este consenso sobre essa norma consuetudinária na XXXIII Conferência Internacional da Cruz e do Crescente Vermelho. O anterior não exclui a necessidade de desenvolver normas internacionais primárias para este tipo de situações em concreto, da mesma forma que em matéria de desarmamento se estabelecem novos instrumentos jurídicos com o objetivo de fortalecer e complementar o DIH. (Cuba, 2024).

Apesar da posição de alguns poucos países, portanto, há amplo reconhecimento de que as operações cibernéticas durante conflitos armados são reguladas pelo DIH – assim como qualquer arma, meio ou método de guerra utilizado por um beligerante em um conflito.

Ainda que superado este primeiro impasse, as discussões têm encontrado dificuldades em chegar a um consenso sobre *como* o DIH se aplica às operações cibernéticas e em avançar no debate de como suas regras devem ser interpretadas.

Há divergências, ademais, a respeito da necessidade de novo tratado ou convenção específica para tratar das operações cibernéticas durante conflitos armados. Outros pontos de desacordo são se os dados civis mereceriam a mesma proteção que os objetos civis em conflitos armados, bem como os requisitos específicos para atribuir responsabilidade por um ataque a um determinado Estado e as medidas que este Estado poderia tomar em resposta ao incidente.

3.1 Posições nacionais: quadro parlamentar

Dos 32 Estados a apresentar posições nacionais (AGNU, A/76/136, 2021), 28 foram favoráveis à aplicação do DIH no espaço cibernético em situações de conflito armado[11]. China, Rússia, Irã e Cazaquistão foram os únicos países a apresentar posições à Assembleia Geral das Nações Unidas sem mencionar DIH.

Como visto, China, Rússia, Venezuela e Irã vêm questionando a aplicação do DIH no ciberespaço com o argumento de que fazê-lo significaria "militarizar ainda mais o ciberespaço (Akande, 2022. p. 6-7; Delerue, 2020. p. 15-17)."

A União Africana, que reúne 55 países, único grupo regional que apresentou posição comum, também reconheceu a aplicação do DIH em situações de conflitos armados no uso das TICs.

A Comissão Jurídica Interamericana da Organização dos Estados Americanos (OEA), por sua vez, aprovou relatórios e resoluções reconhecendo a aplicação do DIH no ciberespaço[12]. A Assembleia Geral da OEA, apesar de não ter aprovado formalmente uma posição comum, também reconheceu que:

> Direito internacional, incluindo a Carta das Nações Unidas em sua totalidade, a Carta da Organização dos Estados

[11] Na região latino-americana e caribenha, apenas Brasil, Costa Rica e Cuba apresentaram posições nacionais. Equador, Peru, México e Chile, em seus discursos no Debate Aberto do Conselho de Segurança sobre Cibersegurança, em 29/6/2021, reconheceram a aplicabilidade do DIH no ciberespaço (S/2021/540).

[12] Resolução CJI/RES. 260 (XCVII-O/20) e Relatórios CJI/doc.615/20, relator Duncan B. Hollis; CJI/doc. 648/21 (2021) e CJI/doc. 671/22 (2022), relatora Mariana Salazar Albornoz.

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

> Americanos, o Direito humanitário internacional, o Direito internacional dos direitos humanos, o dever de não intervenção, a igualdade soberana dos Estados e o Direito de responsabilidade do Estado, é aplicável ao uso das tecnologias da informação e das comunicações (TICs) por parte dos Estados e daqueles que são internacionalmente responsáveis." (CJI/RES. 260).

A União Europeia (UE) e seus Estados-Membros defendem que a estabilidade no ciberespaço só pode ser fundamentada no direito internacional existente, que inclui a Carta das Nações Unidas em sua totalidade, o direito internacional humanitário (DIH) e o direito internacional dos direitos humanos[13].

Apesar das controvérsias, vê-se que há concordância significativa sobre a relevância e a aplicabilidade do DIH no contexto das TICs entre os Estados que se pronunciaram a respeito do tema. É preciso reconhecer, no entanto, que muitos estados ainda não se pronunciaram claramente a respeito de como seria a aplicação das normas do DIH. Há, portanto, risco de deixar a poucos Estados e a atores não estatais o monopólio da produção ou interpretação do regime jurídico aplicável a operações cibernéticas, inclusive em situações de conflitos armados.

4 A POSIÇÃO BRASILEIRA

A posição do Brasil sobre a aplicação do Direito Internacional Humanitário (DIH) ao ciberespaço foi informada em compêndio oficial da Assembleia Geral de posições nacionais submetidas pelos peritos

[13] Discurso no Debate Aberto do Conselho de Segurança sobre Cibersegurança, em 29/6/2021.

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0,
Qualis B4, DOI: 10.5281/zenodo.14203542

participantes do sexto e último GGE (A/76/136), após processo de consultas no Ministério das Relações Exteriores.

O Brasil reconhece que o direito internacional existente é aplicável ao ciberespaço e que, em situações de conflito armado, isso inclui as normas e os princípios pertinentes do DIH, inclusive os princípios da humanidade, necessidade, proporcionalidade e distinção.

A posição brasileira é de que a aplicação do DIH no ciberespaço não deve ser vista como uma legitimação da militarização desse ambiente, mas sim como uma forma de garantir a proteção dos direitos humanos e a manutenção da paz e segurança internacionais.

Tendo em vista o objetivo da manutenção da paz, é necessário cautela ao estabelecer a equivalência entre o uso da força armada e operações cibernéticas, embora essa possibilidade seja reconhecida.

O Brasil foi o único, entre os países que apresentaram posição nacional à ONU, a citar a cláusula Martens, que é uma disposição do DIH que garante proteção aos civis e combatentes mesmo quando não há uma regra específica aplicável.

5 CONCLUSÃO

Este artigo procurou apresentar as principais questões a respeito da aplicabilidade do Direito Internacional Humanitário (DIH) ao ciberespaço nas discussões multilaterais em andamento.

Identificou-se que o argumento da militarização do ciberespaço é utilizado por uma minoria de Estados e que persistem divergências sobre a

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

aplicação e interpretação das normas do DIH (*lege lata*), bem como sobre a necessidade de novas normas (*lege ferenda*).

Embora haja amplo apoio à ideia de que o DIH se aplica às operações cibernéticas durante conflitos, é necessário continuar discutindo como suas regras devem ser interpretadas tendo em conta as particularidades do ciberespaço. Isso inclui considerar se novas regras seriam necessárias para fortalecer a proteção dos civis e da infraestrutura civil.

Concluiu-se que reconhecer a aplicabilidade do DIH às operações cibernéticas não legitima a militarização do ciberespaço, mas impõe limites ao uso da força e protege civis em situações de conflito.

O CICV tem defendido, à luz do desenvolvimento de capacidades de TIC para fins militares e seu potencial impacto humanitário, que as discussões sobre como o direito internacional humanitário limita as operações cibernéticas durante conflitos armados precisam continuar.

Conclui-se pela necessidade de esforços conjuntos para promover uma agenda para a paz no ciberespaço, o que pode incluir debate a respeito da necessidade de novas normas para fortalecer a proteção dos civis e da infraestrutura civil.

A cooperação internacional, nesse contexto, será central para assegurar que as TICs sejam utilizadas de maneira responsável e ética, minimizando os impactos humanitários durante os conflitos armados. A conscientização sobre esses impactos, ademais, pode ajudar a moldar uma cultura de responsabilidade e respeito pelos direitos humanos no ciberespaço.

Acordar claramente em processos multilaterais transparentes e inclusivos quanto às normas aplicáveis à conduta no ciberespaço em

contextos de conflitos armados, pode ser considerado também como importante medida de construção de confiança e redução de tensões.

As Nações Unidas, na visão brasileira, devem continuar a desempenhar papel central nesses debates. É consensual, nos debates no âmbito do OEWG, a necessidade de criação de um mecanismo permanente para tratar desses temas no âmbito das Nações Unidas, ainda que haja, por ora, divergências com relação ao formato e às modalidades que esse futuro mecanismo deverá ter. Espera-se, ao longo do último ano do mandato do OEWG atual, lograr a convergência necessária entre as posições para o estabelecimento do mecanismo.

Para o Brasil, há pelo menos três áreas para discussão futura: a definição de ciberataque para os fins do artigo 49 do AP I; a questão da natureza de dados como objeto civil, o que implicaria proteção sob o DIH; e quando um civil atuando no ciberespaço pode ser considerado como participando diretamente das hostilidades.

Alguns desafios importantes se apresentam a este respeito em decorrência da própria natureza das operações, como a dificuldade em determinar a autoria dos ataques. O aprofundamento das discussões provavelmente identificará outras questões específicas que necessitem discussão para a melhor compreensão da forma e alcance em que o DIH deve ser aplicado.

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0,
Qualis B4, DOI: 10.5281/zenodo.14203542

REFERÊNCIAS

AKANDE, Dapo; COCO, Antonio; SOUZA DIAS, Talita de. Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies. *International Law Studies*, v. 99, p. 4-36, 2022.

ASSEMBLEIA GERAL DA ONU. *A/75/816* (2021, anexo I, para. 7). "International law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment".

ASSEMBLEIA GERAL DA ONU. *A/76/135* (2021), reafirmado em A/78/265 (2023).

ASSEMBLEIA GERAL DA ONU. *A/76/136* (2021).

ASSEMBLEIA GERAL DA ONU. *Carta das Nações Unidas*. 1945. Art. 2(4).

BENEDETTI, Juliana Cardoso. The Role Of The United Nations Security Council In Relation To International Humanitarian Law: An Assessment Of Recent Practice. *In*: *Cadernos de política exterior*, Ano IX, Número 13, 2023.

CICV. *Cyber threats impacting the safety and dignity of civilians in conflict*. International Committee of the Red Cross. 05/03/2024. Disponível em: https://www.icrc.org/en/un-oewg-cyber-threats-7th-meeting-statement. Acesso em: 28 ago. 2024.

CICV. *Discurso da presidente do Comitê Internacional da Cruz Vermelha* (CICV), Mirjana Spoljaric, no Conselho de Segurança das Nações Unidas, em 21 de maio de 2024. Disponivel em: https://press.un.org/en/2024/sc15702.doc.htm. Acesso em: 20 set 2024.

CICV. *Discurso proferido em 4 de março de 2024*. Disponível em: https://www.icrc.org/en/un-oewg-cyber-threats-7th-meeting-statement. Acesso em: 28 agosto 2024.

CICV. *Geneva Conventions 75th anniversary*: Foundational treaties save lives and dignity, but massive humanitarian suffering shows the world must recommit. 22/08/2024. Disponível em: https://www2-prd.icrc.org/en/news-release/geneva-conventions-75th-anniversary-foundational-treaties-save-lives-and-dignity. Acesso em: 10 set. 2024.

CUBA. *Documento de posición de la República de Cuba sobre la aplicación del Derecho Internacional a las Tecnologías de la Información y Comunicación en el ciberespacio*. La Habana, 28 jun. 2024. Disponível em: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_(2021)/Documento_de_posici%C3%B3n_de_Cuba._Aplicaci%C3%B3n_del_Derecho_Internacional_a_las_TIC_en_el_ciberespacio..pdf. Acesso em: 27 set. 2024.

CUBA. *71 UNGA*: Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (Representaciones Diplomáticas de Cuba en El Exterior, 23 June 2017). Disponível em: misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-gov ernmental-experts-developments-field-information. Acesso em: 20 set. 2024.

DELERUE, François. Does International Law Matter in Cyberspace? *In*: *Cyber Operations and International Law*. Cambridge Studies in International and Comparative Law. Cambridge: Cambridge University Press, 2020. p. 1-50, p. 191–378.

DEVANNY, J.; GOLDONI, L. R. F.; MEDEIROS, B. P. The rise of cyber power in Brazil. *Revista Brasileira de Política Internacional*, v. 65, n. 1, p. e013, 2022.

FEDERAÇÃO RUSSA. *Commentary on the Initial "Pre-Draft" of the Final Report of the United Nations Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. 2020. Acesso em: 19/09/2024. Disponível em: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-owegzero-draft-report-eng.pdf.

FLECK, D. (ED.). *The handbook of international humanitarian law*. Fourth edition ed. Oxford, United Kingdom: Oxford University Press, 2021, p 48.

GISSEL, Laurent; RODENHÄUSER, Tilman; DÖRMANN, Knut. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, v. 102, n. 913, p. 287-334, 2020. DOI: 10.1017/S1816383120000387.

HUANG, Zhixiong; MAČÁK, Kubo. Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches. Chinese *Journal of International Law*, v. 16, n. 2, p. 271-310, jun. 2017.

INTERNATIONAL COURT OF JUSTICE. *Legality of the threat or use of nuclear weapons*. Advisory Opinion. July 8, 1996.

ICRC. *Comentários do CICV à minuta de relatório do OEWG*, novembro de 2019. Disponível em: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf. Acesso em: 11 set. 2024.

KELLO, L. *Striking Back*: The End of Peace in Cyberspace - And How to Restore It. [s.l.] Yale University Press, 2022.

MELZER, N. *Direito Internacional Humanitário*: Uma introdução abrangente. [s.l.] CICV, 2023.

OBERLEITNER, G. *The United Nations and International Humanitarian Law*: The Past 75 Years. Max Planck Yearbook of United Nations Law Online, v. 25, n. 1, p. 381–415, 23 Dez. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *Chair's summary*: open-ended working group on developments in the field of information and telecommunications in the context of international security. A/AC.290/2021/CRP.3*. Nova Iorque: ONU, 2021. Disponível em: https://www.un.org/disarmament/open-ended-working-group/. Acesso em: 27 set. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *Compendium of statements in explanation of position on the final report: open-ended working group on developments in the field of information and telecommunications in the context of international security*._ A/AC.290/2021/INF/2. Nova Iorque: ONU, 2021. Disponível em: https://www.un.org/disarmament/open-ended-working-group/. Acesso em: 27 set. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *Final substantive report: open-ended working group on developments in the field of information and telecommunications in the context of international security*._ A/AC.290/2021/CRP.2. Nova Iorque: ONU, 2021. Disponível em: https://www.un.org/disarmament/open-ended-working-group/. Acesso em: 27 set. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *Letter from OEWG Chair*, 2024. Disponível em: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_11_July_2024.pdf. Acesso em: 27 set. 2024.

POMSON, Ori. Methodology of Identifying Customary International Law Applicable to Cyber Activities. *Leiden Journal of International Law*, v. 36, n. 4, p. 1023-1047, 2023.

SCHMITT, Michael (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013, 300 pp.

UNITED NATIONS. *Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies*. Disponível em:

https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021. Acesso em: 10 set. 2024.

ANEXO

POSIÇÃO BRASILEIRA (Resolução A/76/136)

"O direito internacional humanitário (DIH) está bem equipado para responder muitas das questões associadas às novas tecnologias, incluindo as TICs. Não há dúvida de que o DIH se aplica ao uso das TICs pelos Estados durante um conflito armado. O fato de uma arma específica ter sido inventada após o desenvolvimento do direito humanitário não a isenta de regulação. Segundo o Parecer Consultivo da CIJ sobre a Legalidade da Ameaça ou Uso de Armas Nucleares, excluir as operações cibernéticas do âmbito de aplicação do DIH seria incompatível com o caráter intrinsecamente humanitário dos princípios jurídicos em questão, que permeiam o direito dos conflitos armados e se aplicam a todas as formas de guerra e a todos os tipos de armas, as do passado, as do presente e as do futuro."

O DIH aplica-se a situações que configuram conflito armado, independentemente de sua classificação como tal pelas partes. Para o DIH, não importa se o conflito armado é lícito ou não, pois seu objetivo é minimizar o sofrimento humano e proporcionar um nível mínimo de proteção aos civis em qualquer cenário de hostilidades.

Portanto, o reconhecimento de que o direito internacional humanitário se aplica ao ciberespaço não endossa de nenhuma forma a sua militarização ou legitima a guerra cibernética, mas apenas garante um nível mínimo de proteção caso surja um conflito armado.

Há duas instâncias em que o DIH pode se aplicar às atividades cibernéticas. Primeiro, se elas forem realizadas como parte de um conflito armado em andamento, contribuindo para operações convencionais conduzidas pelas partes. Segundo, se as próprias atividades cibernéticas ultrapassarem o limiar de violência para serem caracterizadas como um conflito armado.

De particular importância, o relatório do GGE de 2015 observou os princípios estabelecidos, incluindo, quando aplicável, os princípios de humanidade, necessidade, proporcionalidade e distinção.

Para o Brasil, o princípio do DIH de precaução também se aplica ao uso das TICs pelos Estados, ou seja, as partes devem "tomar todas as precauções possíveis na escolha dos meios e métodos de ataque com vistas a evitar, e em qualquer caso minimizar, a perda incidental de vidas civis, lesões a civis e danos a bens civis".

Além disso, de acordo com o Protocolo Adicional I (AP I), os Estados têm a obrigação, "no estudo, desenvolvimento, aquisição ou adoção de uma nova arma, meio ou método de guerra," de "determinar se seu emprego seria, em algumas ou todas as circunstâncias, proibido". Esta norma, embora seja menos estrita do que alguns Estados desejavam durante as negociações do AP I, já abrange alguns elementos de precaução. Deve orientar o desenvolvimento, aquisição e adoção de capacidades cibernéticas.

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0, Qualis B4, DOI: 10.5281/zenodo.14203542

Ao fazer a avaliação de necessidade, distinção, proporcionalidade e precaução, as partes devem levar em consideração as particularidades do ciberespaço, como a interconectividade entre redes militares e civis. O princípio da distinção determina que os ataques cibernéticos devem ter como alvo objetivos militares e não devem ser indiscriminados. Em caso de dúvida se uma infraestrutura cibernética normalmente dedicada a fins civis está sendo usada para contribuir de forma efetiva para a ação militar, presume-se que não esteja sendo usada para tal fim.

Apesar de reconhecer que o DIH se aplica ao ciberespaço, há questões que merecem uma reflexão mais aprofundada, tais como a definição de ciberataque para os fins do artigo 49 do AP I; a consideração de dados civis como um objeto civil que implica proteção sob o DIH; e quando um civil atuando no ciberespaço pode ser considerado como participando diretamente das hostilidades.

Em todo caso, onde o DIH é omisso ou ambíguo, a "cláusula Martens" permanece aplicável, garantindo que, nos casos não cobertos pelas regras existentes, "civis e combatentes permaneçam sob a proteção e autoridade dos princípios do direito internacional derivados do costume estabelecido, dos princípios de humanidade e dos ditames da consciência pública".

Revista do Ministério Público Militar, a. 51, n. 44, Brasília, nov. 2024, pp. 75-106, CC BY 4.0,
Qualis B4, DOI: 10.5281/zenodo.14203542