ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
DIVISÃO DE ENSINO
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2025

WEBERT LEANDRO BARRETO DA SILVA, Cap Sju

Direito Internacional dos Conflitos Armados: segurança jurídica para as operações cibernéticas do COMAER

Rio de Janeiro
2025

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
DIVISÃO DE ENSINO
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2025

WEBERT LEANDRO BARRETO DA SILVA, Cap Sju

Direito Internacional dos Conflitos Armados: segurança jurídica para as operações cibernéticas do COMAER

Trabalho de conclusão de curso apresentado à Escola de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-Graduação *Lato Sensu* em Liderança com Ênfase em Gestão no COMAER.
Linha de Pesquisa: Guerra Cibernética
Orientadora: Jaqueline de Azevedo Bruno, TC Int

Rio de Janeiro
2025

WEBERT LEANDRO BARRETO DA SILVA, Cap Sju

Direito Internacional dos Conflitos Armados: segurança jurídica para as operações cibernéticas do COMAER

Trabalho de conclusão de curso apresentado ao Curso de Aperfeiçoamento de Oficiais da Escola de Aperfeiçoamento de Oficiais da Aeronáutica.

Aprovado por:

_____

Presidente, Jaqueline de Azevedo Bruno, TC Int - IEFA

_____

Danilo Bichir, Maj Inf - EAOAR

Rio de Janeiro

2025

RESUMO

Considerar a internet como um novo domínio de guerra passou a fazer parte dos estudos militares, de modo que os dispositivos vinculados a ela podem ser considerados potenciais objetivos militares. Nesse cenário, para evitar abusos e violações humanitárias e respeitar as Convenções de Genebra e seus Protocolos Adicionais, o Comando da Aeronáutica deve respeitar as normas do Direito Internacional dos Conflitos Armados, pois fornece uma base jurídica suficiente para regular e limitar as operações cibernéticas da Força. Esse Direito possui um caráter intrinsecamente humanitário ao ponto que os seus princípios e regras 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. Embora não existam tratados específicos para a guerra cibernética, normas como as Convenções de Genebra e seus Protocolos Adicionais se aplicam a essas operações que ocorrem em contexto de conflito armado. Para garantir a conformidade jurídica das operações cibernéticas, o Comando da Aeronáutica deve investir em capacitação e treinamento, como cursos e simulações. Além disso, a discussão sobre o DICA e as operações cibernéticas estimula a pesquisa interdisciplinar em áreas como direito internacional e estudos estratégicos, aprofundando a compreensão dos desafios e oportunidades.

Palavras-chave: Direito Internacional dos Conflitos Armados; operações cibernéticas; segurança jurídica.

1 INTRODUÇÃO

Para explorar as vulnerabilidades do inimigo, o emprego de novas estratégias, táticas ou métodos não previstos pelo oponente é uma característica essencial para qualquer guerra, inclusive as travadas por meio de operações cibernéticas. Nesse cenário, a internet passou a ser considerada um domínio de guerra nos estudos militares, com seus dispositivos vistos como potenciais objetivos militares.

A operação cibernética, para os fins deste trabalho, refere-se ao desenvolvimento e utilização de capacidades militares no domínio cibernético, em conflitos armados, direcionada a objetivos militares específicos (Costa; Cozendey; Calza, 2024), podendo alterar, interromper, enganar, degradar ou destruir sistemas ou redes de computadores usados por um adversário (Lin, 2012; The judge advocate general of the Air Force, 2020). Nesse contexto, o Comando da Aeronáutica (COMAER) criou o Centro de Defesa Cibernética da Aeronáutica (CDCAER) para gerenciar, executar e controlar todas as atividades relacionadas à defesa cibernética no âmbito da Força (Brasil, 2024).

Ocorre que a ausência da aplicação do Direito Internacional dos Conflitos Armados (DICA) nas operações cibernéticas do COMAER resultaria em um aumento de danos aos civis, devido à falta de restrições na condução das operações, e em um maior risco de escalada de conflitos, impulsionado pela incerteza e desconfiança. Além disso, haveria a erosão da proteção de bens essenciais, como hospitais; a impunidade se fortaleceria, decorrente da dificuldade em responsabilizar por violações; e as operações seriam deslegitimadas perante a comunidade internacional, comprometendo a posição do Estado brasileiro.

Assim, o DICA foi elaborado de tal maneira que se aplica a todas as formas de conflito e armas, incluindo as futuras. No entanto, a ausência de normas internacionais e nacionais específicas para operações cibernéticas pode levar a um tratamento jurídico inadequado e prejudicar a atuação do COMAER em conflitos. Dessa forma, este trabalho defende que o Direito Internacional dos Conflitos Armados fornece uma segurança jurídica suficiente para regular e limitar as operações cibernéticas do Comando da Aeronáutica.

Para subsidiar esta tese, observa-se que as regras do DICA protegem a humanidade, conforme reconhecido pelo Tribunal Internacional de Justiça em 1996 ao afirmar que sua aplicação se estende a todas as formas de guerra e armas, incluindo operações cibernéticas. Adicionalmente, as Convenções de Genebra, seus Protocolos Adicionais e os Princípios do DICA, embora não mencionem expressamente a guerra cibernética, aplicam-se a qualquer meio ou método de guerra, incluindo os ataques cibernéticos.

2 DESENVOLVIMENTO

A capacidade de projetar força militar via Internet estimulou as Forças Armadas a estabelecerem Unidades, dentro de suas estruturas, responsáveis por operações de rede de computadores defensivas e ofensivas. O CDCAER foi instituído pelo Comando da Aeronáutica com o propósito de gerenciar, executar e supervisionar todas as ações concernentes à defesa cibernética na Força.

Sob estas circunstâncias, este trabalho propõe-se a examinar dois aspectos centrais relacionados à interação entre o DICA e as operações cibernéticas. Primeiramente, será analisada a afirmação do Direito Internacional dos Conflitos Armados como um marco normativo aplicável a esse novo domínio de atuação, considerando o posicionamento essencialmente humanitário adotado pelo Tribunal Internacional de Justiça. Em seguida, será analisada a compatibilidade dos princípios fundamentais do DICA com as especificidades dos conflitos cibernéticos.

2.1 O DICA E SUA AFIRMAÇÃO DIANTE DAS OPERAÇÕES CIBERNÉTICAS

Em julho de 1996, o Tribunal Internacional de Justiça ao ser consultado sobre a licitude da ameaça ou emprego de armas nucleares entendeu que as características únicas das armas nucleares e, em particular, sua capacidade destrutiva, sua capacidade de causar sofrimento humano incalculável e sua capacidade de causar danos às gerações futuras possuem aplicabilidade no DICA.

Consciente de que a existência e o desenvolvimento contínuos de armas nucleares representam sérios riscos à humanidade e de que os Estados têm a obrigação, sob a Carta das Nações Unidas, de se abster da ameaça ou uso da força contra a integridade territorial ou independência política de qualquer Estado, o Tribunal apontou que o respeito da pessoa humana deve ser observado por todos os Estados, tenham ou não ratificado as convenções que as contêm, vez que constitui princípio intransponível do direito internacional (Tribunal Internacional de Justiça, 1996). Nessa linha, as regras do DICA são tão fundamentais para aquele respeito fundamental que as Convenções de Genebra têm desfrutado de uma ampla adesão por ser um imperativo humanitário, como ensina o professor Resek (2018).

A despeito de existir uma diferença qualitativa e quantitativa entre armas nucleares e todas as armas convencionais, o posicionamento do Tribunal caminhou no sentido de que o DICA possui um caráter intrinsecamente humanitário ao ponto que os seus princípios e regras

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 (Tribunal Internacional de Justiça, 1996), o que inclui as operações cibernéticas.

Considerando a definição de Operações Cibernéticas anotada no início deste ensaio, tem-se que a dinâmica dessas operações é negar ao inimigo o uso de uma determinada tecnologia, acessá-la para usar suas informações ou assumir o controle sobre o que é gerenciado pela tecnologia (Hughes; Colarik, 2017).

Nesse contexto, esse novo tipo de guerra com características e modo de combater diferentes, conforme escreveu Cinelli (2016, p. 270), "[...] ao contrário do que possa parecer, não somente ratifica, mas na verdade fortalece a convicção de que é preciso observar as normas do DICA para se obter legitimidade no exercício da violência."

Ademais, tendo em vista que a grande maioria das normas do direito internacional foi desenvolvida muito antes da invenção dos computadores, tem-se que a maioria das questões legais relacionadas a operações cibernéticas depende de normas contidas na Carta das Nações Unidas adotada em 1945, nas Convenções de Genebra de 1949 e seus Protocolos Adicionais. No entanto, nos ensinamentos de Delerue (2020), essas normas não se aplicam apenas às formas de atividades do Estado existentes no momento de sua adoção ou codificação, mas às atividades do Estado em geral. Por essas razões, parece inquestionável que o direito internacional se aplica às atividades cibernéticas.

E, nesse cenário, Schmitt (2019) argumentou que os propósitos do DICA são tais que visam proteger aqueles que não participam diretamente nas hostilidades e suas propriedades; a proteção em si é enquadrada em termos de ferimentos ou morte ou, no caso de propriedade, danos ou destruição. Assim, deve-se raciocinar que o conflito armado ocorre quando um grupo toma medidas que ferem, matam, danificam ou destroem, características alcançadas pelas operações cibernéticas.

Portanto, a aplicação do Direito Internacional dos Conflitos Armados estabelece uma segurança jurídica suficiente às operações cibernéticas do COMAER, uma vez que é aplicável tanto a novas armas quanto a métodos de guerra, independentemente de sua execução específica.

2.2 A APLICABILIDADE DOS PRINCÍPIOS DO DICA NAS OPERAÇÕES CIBERNÉTICAS

Embora não existam tratados específicos para a guerra cibernética, normas como as Convenções de Genebra de 1949 e seus Protocolos Adicionais de 1977, promulgados no Brasil, respectivamente, por meio do Decreto nº 42.121, de 21 de agosto de 1957 (Brasil, 1957), e do

Decreto nº 849, de 25 de junho de 1993 (Brasil, 1993), se aplicam às operações cibernéticas que ocorrem em contexto de conflito armado.

Essas operações usam computadores para interromper, negar, degradar ou destruir informações residentes em computadores e redes de computadores, ou os próprios computadores e redes. A título exemplificativo, um ataque cibernético que destruísse sistemas de computadores inimigos não poderia ser direcionado contra infraestrutura ostensivamente civil, como sistemas de computadores pertencentes a bancos, hospitais ou escolas. Isso porque são objetivos militares os combatentes, incluído os participantes de um levantamento em massa, e os civis que participem diretamente das hostilidades, conforme preconizado nos arts. 48, 51 e 52 do Protocolo Adicional I (Brasil, 1993).

As quatro Convenções de Genebra (Brasil, 1957) protegem aqueles que não participam diretamente do conflito e garantem a dignidade humana durante as operações (Princípio da Humanidade). No contexto das operações cibernéticas, a Primeira Convenção protege os feridos e doentes em conflitos terrestres e as operações cibernéticas contra hospitais militares ou sistemas médicos violariam essa proteção; a Segunda Convenção protege feridos, doentes e náufragos em conflitos navais e um ataque cibernético que comprometa sistemas de comunicação de navios-hospitais também violaria essa norma; a Terceira Convenção regula o tratamento de prisioneiros de guerra e os Sistemas cibernéticos que armazenam dados de prisioneiros não podem ser alvo de ataques que coloquem em risco sua integridade; e a Quarta Convenção protege civis e bens essenciais, de modo que as operações cibernéticas contra infraestruturas civis (como redes elétricas e abastecimento de água) podem violar essa proteção.

Nesse cenário, tais operações devem estar de acordo com os princípios da distinção e da proporcionalidade (Cinelli, 2016). É sobre esse primeiro que se assenta toda a estrutura normativa do DICA destinada à proteção das pessoas e dos bens. Identifica-se a necessária distinção entre civil e combatente e entre bem civil e objetivo militar. Na proporcionalidade, por sua vez, é observado o menor dano colateral possível, isto é, a ação não deve causar vítimas nem danos excessivos em relação à vantagem militar concreta e direta (Princípio da Necessidade Militar), conforme se vê no art. 51, §5º, “b”, e no art. 57 do Protocolo Adicional I (Brasil, 1993). Cita-se, por exemplo, a conveniência de se avaliar os efeitos potenciais de um ataque cibernético em computadores que não são objetivos militares, como computadores civis que não têm importância militar, mas que podem estar conectados em rede a computadores que são objetivos militares legítimos.

Desse modo, mesmo que não se espere que operações cibernéticas que constituem ataques resultem em perda excessiva de vidas, ferimentos ou danos incidentais (com isso a

operação seria proibida pelo princípio da proporcionalidade), a parte em conflito, no entanto, seria obrigada a tomar precauções viáveis para limitar tal perda de vidas, ferimentos e danos na condução dessas operações cibernéticas (United States of America, 2015).

É por isso que operações cibernéticas contra infraestruturas essenciais para a sobrevivência humana e contra sistemas que controlam usinas nucleares ou barragens são proibidas, conforme os arts. 54 e 56 do Protocolo Adicional I (Brasil, 1993).

As operações cibernéticas podem ser caracterizadas como medidas potenciais para reduzir o risco de danos supérfluos, sofrimento desnecessário e agressão ao meio ambiente (Princípio da Limitação). Em alguns casos, essas operações que resultam em efeitos não cinéticos ou reversíveis podem oferecer opções que ajudam a minimizar danos desnecessários a civis. Nesse sentido, as capacidades cibernéticas podem, em algumas circunstâncias, ser preferíveis, como uma questão de política, às armas cinéticas porque seus efeitos podem ser reversíveis e podem ter o potencial de atingir objetivos militares sem qualquer efeito cinético destrutivo (United States of America, 2015).

O Direito Internacional dos Conflitos Armados não proíbe os Estados de usar pessoal civil para dar suporte às suas operações cibernéticas, incluindo ações de suporte que podem constituir participação direta nas hostilidades. Com isso, pessoas que não são membros das Forças Armadas, mas que estão autorizadas a acompanhá-las, têm direito ao status de prisioneiro de guerra (Brasil, 1957). Esta categoria inclui, por exemplo, pessoal civil com habilidades especiais na operação de equipamentos militares que dão suporte e participam de operações militares, assim como especialistas cibernéticos civis contrários ao Estado. Dessa maneira, esses civis passam a ser objetivos militares legítimos.

Como se vê, as normas das Convenções de Genebra (Brasil, 1957) e seus Protocolos Adicionais (Brasil, 1993) impõem limites claros às operações cibernéticas, garantindo que essas operações sigam os princípios da distinção, proporcionalidade e necessidade militar e, de igual modo, não afetem hospitais, escolas ou sistemas de abastecimento de água. Ademais, a despeito de não mencionar explicitamente a operação cibernética, os princípios do DICA garantem a proteção de civis, infraestrutura crítica e combatentes, limitando o uso indiscriminado da tecnologia na guerra.

Dessa forma, o Direito Internacional dos Conflitos Armados fornece uma segurança jurídica suficiente para regular e limitar as operações cibernéticas do Comando da Aeronáutica.

3 CONCLUSÃO

As operações cibernéticas do COMAER não dispõem de uma norma jurídica específica para respaldar a legalidade durante um conflito armado, o que acarretaria a necessidade de seguir o Direito Internacional dos Conflitos Armados como norma aplicável.

Demonstrou-se neste ensaio que as normas do DICA são essenciais para a salvaguarda da dignidade da pessoa humana e para a observância de princípios elementares de humanidade. Essa compreensão foi reafirmada pelo Tribunal Internacional de Justiça, em seu parecer consultivo de 8 de julho de 1996, ao tratar da legalidade da ameaça ou do uso de armas nucleares. Na ocasião, a Corte ressaltou que qualquer interpretação em sentido contrário seria incompatível com o caráter intrinsecamente humanitário do DICA, destacando que suas normas se aplicam a todas as formas de conflito armado e a todos os tipos de armamento (passados, presentes e futuros), incluídas as operações cibernéticas.

Foi demonstrado, também, que embora o cenário da operações cibernéticas ainda não possua tratados internacionais especificamente dedicados à sua regulamentação, é reconhecido que as normas estabelecidas pelas Convenções de Genebra de 1949, juntamente com seus Protocolos Adicionais de 1977, que visam proteger vítimas de conflitos armados e regular a conduta das hostilidades, são consideradas aplicáveis a essas operações que venham a ocorrer dentro do contexto mais amplo de um conflito armado tradicional, demandando uma análise cuidadosa de como seus princípios fundamentais podem ser interpretados e aplicados no domínio cibernético, dada a sua natureza peculiar.

Assim, tendo em vista as implicações humanitárias provocadas por essas operações, o Direito Internacional dos Conflitos Armados, em sua configuração atual, oferece um conjunto de princípios e regras jurídicas suficientemente abrangente para a regulação e a imposição de limites às operações cibernéticas conduzidas em contexto de conflito armado pelo COMAER.

Por fim, ressalta-se que a aplicação do DICA às operações cibernéticas exige que o Comando da Aeronáutica invista no desenvolvimento de capacidades específicas e no treinamento de pessoal para garantir a conformidade com os princípios jurídicos. Isso pode incluir a criação de cursos, simulações e exercícios que abordem os aspectos legais das operações cibernéticas. Além disso, a discussão sobre o DICA e as operações cibernéticas pode estimular a pesquisa acadêmica e o desenvolvimento de novos estudos nas áreas de direito internacional, ciência da computação, relações internacionais e estudos estratégicos. Essa interdisciplinaridade é fundamental para aprofundar a compreensão dos desafios e oportunidades nesse campo.

REFERÊNCIAS

BRASIL. Decreto nº 849, de 25 de junho de 1993. Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armado. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 1993. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0849.htm. Acesso em: 30 mar. 2025.

BRASIL. Decreto nº 42.121, de 21 de agosto de 1957. Promulga as Convenções concluídas em Genebra, a 12 de agosto de 1949, destinadas a proteger as vítimas da guerra. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 1957. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1950-1969/d42121.htm. Acesso em: 30 mar. 2025.

BRASIL. Portaria GABAER/GC3 nº 1.465, de 27 de junho de 2024. Cria e ativa o Centro de Defesa Cibernética da Aeronáutica (CDCAER). **Diário Oficial da União**: seção 1, Brasília, DF, n. 123, p. 37, 28 jun. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gabaer/gc3-n-1.465-de-27-de-junho-de-2024-568654790. Acesso em: 4 maio 2025.

CINELLI, Carlos Frederico. **Direito Internacional Humanitário**: Ética e Legitimidade na aplicação da força em conflitos armados, 2. ed. Curitiba: Juruá, 2016.

COSTA, Isabel Soares da; COZENDEY, Carlos Márcio Bicalho; CALZA, Larissa Schneider. Operações cibernéticas em conflitos armados: o Direito Internacional Humanitário legitimaria a militarização do ciberespaço? **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.

DELERUE, François. **Cyber Operations and International Law**. Cambridge: Cambridge University Press, 2020.

HUGHES, Daniel; COLARIK, Andrew. The Hierarchy of Cyber War Definitions. *In*. Pacific-Asia Workshop on Intelligence and Security Informatics. **Proceedings** [...]. Jeju Island: PAISI, 2017, p. 15-33.

LIN, Herbert. Cyber conflict and international humanitarian law. **International Review of the Red Cross**. v. 94, n. 886, p. 515-531, 2012.

RESEK, José Francisco. **Direito Internacional Público**: curso elementar. 17 ed. São Paulo: Saraiva, 2018.

SCHMITT, Michael. Wired warfare 3.0: Protecting the civilian population during cyber operations. **International Review of the Red Cross**, Cambridge, n. 101 (1), p. 333–355, 2019. DOI:10.1017/S1816383119000018.

THE JUDGE ADVOCATE GENERAL OF THE AIR FORCE. **The law of air, space, and cyber operations**.[s. l.],Fourth Edition, 2020.

TRIBUNAL INTERNACIONAL DE JUSTIÇA. Legality of the Threat or Use of Nuclear Weapons. **Advisory Opinion**. Haia, 1996.

UNITED STATES OF AMERICA. Department of Defense. **Law of War Manual**, 2015. [2023] Disponível em: https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF. Acesso em: 30 mar. 2025.