ESCOLA DE GUERRA NAVAL

CC MARCELO NASCIMENTO RIBEIRO DA SILVA

A SELEÇÃO DE ALVOS E O DICA:
aplicabilidade no ciberespaço.

Rio de Janeiro
2016

CC MARCELO NASCIMENTORIBEIRO DA SILVA

A SELEÇÃO DE ALVOS E O DICA:
aplicabilidade no ciberespaço.

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

Orientador: CF André Marcus Blower

Rio de Janeiro
Escola de Guerra Naval
2016

AGRADECIMENTOS

Primeiramente, e acima de tudo, a Deus, agradeço pela minha existência, minha família, meu trabalho e a saúde de que disponho para seguir minha caminhada.

À minha esposa Elma, pelo seu sacrifício diário para conciliar seus diversos afazeres com a educação e o cuidar dos nossos filhos, pela sua paciência ao entender as minhas ausências, neste ano acadêmico.

À minha filha Isabela e ao meu filho João Marcelo, que iluminam de maneira especial os meus pensamentos e fazem-me cada vez mais buscar o crescimento intelectual e profissional.

Ao meu orientador, CF André Marcus Blower, pela sua cordialidade, paciência, ensinamentos e orientações que nortearam a confecção deste trabalho, sempre de maneira disposta e precisa.

À EGN, em especial a todos aqueles responsáveis pela organização e condução do C-EMOS, pelas experiências e orientações transmitidas, mas, sobretudo, por ter-me proporcionado esta oportunidade de crescer profissionalmente.

E, por fim, aos amigos da turma Almirante Ary Parreiras e Oficias integrantes da turma C-EMOS 2016, bem como a todos que direta ou indiretamente contribuíram na confecção deste trabalho.

RESUMO

As singularidades que caracterizam o ambiente cibernético, ou ciberespaço, inicialmente, colocam em dúvida a capacidade regulamentadora e limitadora do Direito Internacional dos Conflitos Armados (DICA), bem como de seus princípios, com relação a uma possível guerra cibernética. Além disso, tais singularidades têm levado à reflexão sobre o potencial calamitoso de um conflito com ações conduzidas a partir do ciberespaço, onde as mesmas podem ter como objetivos uma grande diversidade de alvos, sendo alguns de considerável risco para os bens e populações civis. Dessa forma, o presente trabalho foi desenvolvido com o objetivo de tratar a possibilidade de aplicação das fontes tradicionais do DICA e de seus princípios fundamentais, no processo de seleção de alvos, a partir deste novo domínio, o chamado domínio do ciberespaço. Para tal, o método utilizado foi o de pesquisa bibliográfica e documental, por meio da busca e leitura de fontes especializadas no assunto e de artigos científicos sobre o tema em questão. Por fim, a pesquisa realizada indicou resultados com conclusões positivas sobre a aplicabilidade do DICA e de seus princípios na seleção de alvos, no domínio do ciberespaço, sem, entretanto, descartar a possibilidade de uma revisão e atualização das normas reguladoras internacionais dos conflitos armados, com vista a um melhor enquadramento para os avanços tecnológicos observados nos meios e métodos de se fazer a guerra.

Palavras-chave: Seleção de Alvos. Direito Internacional dos Conflitos Armados. Ciberespaço. Guerra Cibernética.

SUMÁRIO

1 INTRODUÇÃO

Desde o início de sua criação, por meio da celebração da 1ª Convenção de Genebra (1864), ocasião em que foram elaboradas as primeiras normas e condutas em relação ao tratamento de combatentes, não combatentes e vítimas da guerra, as fontes tradicionais do Direito Internacional dos Conflitos Armados (DICA) vem sofrendo diversas adaptações.

As adaptações sofridas são decorrentes da evolução do processo de condução das hostilidades entre os Estados e, de forma mais específica, dos conflitos armados entre os mesmos. Como exemplo, tem-se as convenções subsequentes realizadas, como a Declaração de São Petersburgo (1868)[1], as Convenções e Declarações de Haia[2], em 1899 e 1907, a Convenções de Genebra de 1949 e os seus Protocolos Adicionais de 1977, que, atualmente, compõem as fontes tradicionais do DICA.

Nesse contexto, em função do surgimento de novas tecnologias, em conjunto com a era da informação[3] e o advento da *Internet*, responsável pelo nascimento e, posteriormente, pelo aumento das relações interestatais em rede, a guerra no ambiente cibernético desponta como um novo desafio para a aplicação do DICA em um conflito que se utilize desse novo domínio.

Cabe ressaltar, entretanto, que, apesar de toda evolução e modificações observadas, ou que ainda venham a ocorrer, o DICA buscará manter seu objetivo principal, que é a preservação da pessoa humana e dos bens civis.

---

[1] A Declaração de São Petersburgo foi o primeiro instrumento internacional criado com a finalidade de regular os métodos e meios de combate, tendo sido considerado o primeiro documento consolidador de alguns direitos consuetudinários existentes, proibindo ataques a não-combatentes, bem como a utilização de armamentos que elevasse o sofrimento de feridos.

[2] As Convenções e Declarações de Haia fazem referência à 1ª Conferência Internacional de Paz, assinada em 29 de julho de 1899 e à 2ª Conferência Internacional de Paz, assinada em 18 de outubro de 1907 (CICV, 2001)

[3] A informação, em si mesma, é *epimaterial*. É sempre transportada por um meio material, mas não é idêntica ao transportador. Um dos pilares do progresso no processamento de informação é a tecnologia que permite uma alta taxa entre unidade de informação e quantidade de matéria necessária para transportá-la. Existe um enorme avanço nesse campo, baseado em profundo conhecimento das ciências físicas sobre a estrutura da matéria (SENDOV, 1994).

Dessa forma, o presente trabalho tem como propósito verificar a aplicabilidade do DICA no processo de seleção de alvos no ambiente cibernético.

A importância de se responder a tal questionamento se dá em função das particularidades que caracterizam o domínio do ciberespaço. Vale destacar que essas particularidades, da mesma forma que podem trazer diversos benefícios para a humanidade, por meio do progresso tecnológico, acabam fomentando, também, novas capacidades militares nos campos de batalha. Tal fato, consequentemente, gera diversas dúvidas e diferentes interpretações com relação às normas que regulam o uso da força.

Neste trabalho, emprega-se o método de pesquisa bibliográfica e documental, baseado na leitura de fontes especializadas no assunto e consulta a artigos científicos.

Adicionalmente, destaca-se que o propósito do mesmo foi de explorar e conhecer os principais conceitos e singularidades do ambiente e da guerra cibernética. Ao mesmo tempo, busca-se verificar a origem e os conceitos dos princípios e das fontes tradicionais do DICA, bem como se os mesmos são aplicáveis no ciberespaço, em especial, por ocasião do processo de seleção de alvos durante uma ação de guerra cibernética.

Buscando alcançar o objetivo proposto, este estudo foi organizado em 3 capítulos, além da presente Introdução e de uma Conclusão.

No segundo capítulo, realiza-se uma breve contextualização histórica dos Tratados e Convenções Internacionais, que se consolidaram como fontes tradicionais do DICA. Foram estudados, ainda, quatro dos seus cinco princípios fundamentais e a importância dos mesmos para a seleção de alvos – quais sejam: humanidade, necessidade militar, proporcionalidade e distinção.

No terceiro capítulo, são explorados e analisados os principais conceitos, possibilidades e particularidades do ciberespaço e das ações conduzidas nesse ambiente. São, também, identificados alguns dos atores inseridos no contexto do ambiente cibernético, os

alvos existentes no mesmo e as possíveis consequências de ataques cibernéticos sobre esses alvos. Com relação a tais atores, é importante salientar que, apesar da diversidade dos mesmos, este trabalho terá como foco apenas as ações cibernéticas conduzidas pelos atores estatais.

No quarto capítulo, são verificadas algumas das referências acerca de documentos e legislações internacionais que atualmente vem sendo estudadas e utilizadas como forma de melhor orientar e regulamentar os conflitos que utilizam o domínio do ciberespaço como meio de se fazer a guerra.

Dentro desse contexto, será analisada a aplicação do DICA, seus princípios fundamentais e a importância e influência dos mesmos na seleção de alvos, por ocasião de um ataque cibernético. Além disso, é verificada a possibilidade de enquadramento dos conceitos de *Jus ad Bellum* (Direito à Guerra) e de *Jus in Bello* (Direito da Guerra) à guerra conduzida no ciberespaço.

Na conclusão, buscar-se-á responder ao questionamento sobre a aplicabilidade do arcabouço jurídico do DICA à luz de um conflito onde sejam observadas ações de guerra cibernética, em particular, no processo de seleção de alvos e, complementarmente, a sugestão vislumbrada para a eliminação das possíveis lacunas jurídicas existentes.

2 DICA: FONTES E PRINCÍPIOS FUNDAMENTAIS

Neste capítulo, busca-se apresentar uma breve contextualização histórica do DICA, também conhecido como Direito Internacional Humanitário, das suas fontes, dos seus princípios fundamentais e da importância dos mesmos para a seleção de alvos.

Esta primeira abordagem é importante para entender como se deu a evolução de tal campo do Direito Internacional.

2.1 O DICA e suas Fontes

Segundo Hugo Grotius (1583-1645)[4], que, em 1625, já afirmava a importância do Direito para o Sistema Internacional (SI), não existe associação de homens que possa ser mantida sem Lei, da mesma forma que a associação responsável pela união da raça humana, ou de muitos Estados, tem a necessidade de uma regulação (GROTIUS, 2004).

Saber da existência de uma lei, entretanto, não significa dizer que seja fácil forjar um arcabouço legislativo, principalmente quando se trata de um ambiente complexo como é o SI. Esse, portanto, é o grande desafio do Direito Internacional, qual seja, de compreender o funcionamento do SI e, a partir de então, organizar e regular as relações existentes dentro do mesmo, que se encontra em constante mutação.

Ainda dentro do contexto das relações existentes no SI, os conflitos, violentos ou não, e constantemente inseridos nas mesmas, foram os responsáveis por moldar, política e economicamente, a configuração mundial no passar do tempo.

Em especial, a forma contundente com que tais conflitos foram travados, com consequências consideráveis, como destruição de bens, quantidade numerosa de mortos e feridos, bem como de refugiados, além da dor desnecessária causada a diversas nações,

[4] Nascido em Delft, nos Países Baixos, em 1583, Hugo Grotius foi durante muito tempo considerado como o pai do Direito Internacional Público. Aos 11 anos, matriculou-se na recém fundada universidade de Leiden, onde estudou Direito e Línguas Clássicas. Hugo Grotius morreu em Rostock, na Alemanha, em 1645.

representa, continuamente, fator de preocupação e de comoção da humanidade.

Historicamente, as regras que regem o emprego da força pelos Estados envolvidos em conflitos, são relativamente recentes. Ainda que tenham havido tentativas anteriores de se mitigar o uso da violência nos conflitos, as críticas e teorias mais significativas sobre as guerras e suas consequências surgiram de forma mais significativa na Idade Moderna[5], com pensadores como Hugo Grotius e Immanuel Kant (1724-1804)[6].

No entanto, tais críticas e teorias, bem como os limites impostos ao recurso das armas, não eram tão consistentes. Mesmo que já se falasse em Direito Internacional, as normas estabelecidas pelo mesmo somente eram cumpridas por aqueles Estados que haviam concordado em aceitá-las, seja por meio da assinatura de um tratado, ou por meio de um padrão de comportamento assumido de forma consensual.

Não obstante, pode-se dizer que, mesmo que se tenha a data de 1864 como o marco do nascimento do DICA, quando foi celebrada a 1ª Convenção de Genebra, as preocupações e algumas regras sobre métodos e meios de condução das hostilidades entre os Estados tem antecedentes remotos.

Naquela ocasião, já havia o pensamento de que, ainda que inevitável, a guerra não deveria ocasionar sofrimentos, ou destruições, desnecessários que não aqueles indispensáveis para seu objetivo político. Isso pode ser também comprovado por meio da doutrina de Jacques Rousseau (1712-1778), que trouxe, junto com ela, uma alteração nas ações dos Estados que passaram a enxergar os conflitos como uma relação entre eles, nas quais o homem era encarado como um soldado que defendia seu Estado.

Dessa forma, fica evidenciada, antes mesmo da existência formal de normas

---

[5] Entende-se como Idade Moderna o recorte temporal compreendido entre o final do Século XV e o final do Século XIX.

[6] Filósofo, nascido de uma modesta família de artesãos, Immanuel Kant foi o autor, dentre outras obras, da reconhecida *A Paz Perpétua* (1795), na qual demonstra sua fé em uma paz perpétua, construída graças a razão ter mais força que o poder. Segundo ele, a guerra é só o melancólico meio para afirmar o direito de um Estado pela força.

jurídicas responsáveis por legislar a condução de conflitos, a preocupação com a proteção da população civil.

Foi a partir da criação do Comitê Internacional da Cruz Vermelha (CICV), em 1863, que se promoveu a já citada 1ª Convenção de Genebra (1864), ocasião em que surgiu o primeiro arcabouço de condutas e normas voltado ao tratamento de combatentes, não combatentes e vítimas da guerra. Em sequência à Convenção de Genebra, são criadas a Declaração de São Petersburgo (1868) e as Convenções e Declarações de Haia, em 1899 e 1907.

Dando sequência ao seu processo de evolução, tais convenções progrediram consideravelmente após a Primeira Guerra Mundial (1914-1918), com a realização das Convenções de Genebra de 1929, muito em função dos traumas deixados pelos danos excessivos observados durante tal conflito. Entretanto, o DICA foi finalmente amadurecido e consolidado após o advento da Segunda Guerra Mundial (1939-1945), com as Convenções de Genebra de 1949 e os seus Protocolos Adicionais de 1977, confirmando a preocupação com a necessidade de proteção às vítimas de conflitos armados, sejam eles internacionais ou não (DEYRA, 2001).

Foram justamente as Convenções de Haia e de Genebra, juntamente com seus Protocolos, que se consolidaram como as fontes convencionais e principais vertentes do DICA, definido por Swinarski, da seguinte forma:

> Conjunto de normas internacionais, de origem convencional ou consuetudinária, especificamente destinado a ser aplicado nos conflitos armados, internacionais ou não-internacionais. E que limita, por razões humanitárias, o direito das Partes em conflito de escolher livremente os métodos e os meios utilizados na guerra, ou que protege as pessoas e os bens afetados, ou que possam ser afetados pelo conflito (1993, p. 9).

O conceito acima também foi o mesmo adotado pelo Ministério da Defesa brasileiro, que ainda resumiu o DICA como um conjunto de normas que tem como objetivo proteger os indivíduos e bens durante os conflitos armadas, bem como estabelecer regras

comportamentais para os Estados envolvidos nos conflitos, no que se refere aos métodos e meios de combate utilizados pelo Direito, por ocasião da condução das hostilidades (BRASIL, 2011).

Ainda com relação à definição de Swinarski (1993), quando se faz menção à "origem convencional ou consuetudinária" do DICA, o mesmo se remete às suas fontes, que sendo convencionais fazem referência aos tratados, ou seja, documentos escritos ou contratuais adotados por mais de um Estado.

Já as fontes consuetudinárias constituem um arcabouço informal de normas ou leis, resultante da conjugação de práticas de Estados, ou seja, que seus governantes dizem e fazem, sendo obrigatórias para os mesmos que, por sua vez, contribuem para o desenvolvimento e evolução de tais normas (BYERS, 2007).

Dessa forma, independentemente de sua origem convencional ou consuetudinária, o DICA é considerado uma norma de *jus cogens*, ou seja, de caráter imperativo e com precedência sobre normas conflitantes ou sobre qualquer tratado que seja firmado de forma a violá-lo.

Em face ao exposto, observa-se que, ainda que sujeito a desenvolvimento, discussões e transformações, o DICA pretende, acima de tudo, proteger a vida humana, os indivíduos, independentemente do tipo de conflito travado, e o faz, principalmente, por meio do estabelecimento de limites na condução das hostilidades. Para tal, foram estabelecidos alguns princípios fundamentais que o regulam e que serão estudados a seguir.

2.2 Os quatro princípios fundamentais do DICA

Neste subitem serão descritos, de maneira sucinta, quatro dos cinco princípios do DICA, quais sejam, a humanidade, a necessidade militar, a proporcionalidade e a distinção, os quais possuem maior peso específico no processo de seleção de alvos.

a) Princípio da humanidade

O Princípio da humanidade busca preservar e manter a dignidade da pessoa humana, evitar o seu sofrimento, seja combatente ou não, bem como garantir os seus direitos e protegê-la dos abusos inerentes aos conflitos. Segundo Mello (1997), tal princípio se fundamenta unicamente no ser humano e leva em consideração que o indivíduo não faz parte da guerra, mas sim as coletividades estatais.

O CICV concebe este princípio, como uma importante ferramenta para a consecução do objetivo de evitar ou minimizar o sofrimento, o caos e as barbáries, o que pode ser alcançado respeitando-se a pessoa humana, independente de sua nacionalidade, raça, classe política ou social, religião, seja em tempos de guerra ou de paz (KRIEGER, 2009).

Adicionalmente, pode-se dizer que o princípio da humanidade imprime limites às consequências da guerra e minimiza suas calamidades, tendo em vista que impede ações desumanas durante a condução das hostilidades, priorizando-se a observância do DICA. Com isso, proíbe-se a utilização de métodos e armas que aumentam desnecessariamente o sofrimento daqueles que se encontram fora de combate.

b) Princípio da necessidade militar

A definição básica do princípio da necessidade militar é de que o mesmo tem como função limitar o uso da força, durante os conflitos armados, àquele estritamente necessário para o cumprimento dos objetivos militares, independentemente do nível de decisão considerado.

Para Mello (1997), não se pode recorrer a este princípio caso os danos causados à população e aos bens civis excedam a vantagem militar concreta e esperada. Considera-se ainda o da necessidade militar subordinada ao princípio da proporcionalidade, que será visto mais adiante, o qual restringe seu emprego de forma injustificada.

A origem e definição deste princípio já se encontrava presente no Século XIX, antes mesmo da existência das atuais normas do DICA. O Código de Lieber, de 1863, durante a Guerra de Secessão (1861-1865), ratifica isso ao citar a importância de se tomar medidas que possibilitassem alcançar os objetivos da guerra, entretanto que as mesmas fossem lícitas e de acordo com as normas e costumes da guerra (ICRC, 2005).

Atualmente, o princípio da necessidade militar pode ser caracterizado como uma ferramenta que limita os ataques estritamente aos objetivos militares. Vale dizer, aqueles ataques que devido à sua natureza, utilização, localização ou destino representem uma contribuição para a ação militar, sendo sua destruição, neutralização ou captura uma vantagem militar precisa (CICV, 1998).

Logo, o uso da força em caso de necessidade militar deve ter relação com a vantagem militar pretendida, não justificando condutas desumanas e atividades proibidas pelo DICA (BRASIL, 2011). Muitas são as controvérsias e questionamentos em face deste princípio, basicamente em função da dificuldade, principalmente nos conflitos mais recentes, de se definir um objetivo como sendo militar.

Não são raros os casos de conflitos atuais, onde uma das partes se vale de locais como escolas, hospitais ou outros, onde haja grande concentração de civis, para esconder ou alojar depósitos e paióis de armas e munição.

Dessa forma, um Comandante, baseado nesse princípio, poderá reduzir, modificar ou flexibilizar, em casos excepcionais, as normas estabelecidas no DICA, sendo, portanto, fundamental uma clara definição de seus objetivos militares, observando e obedecendo as normas previstas no mesmo, para a realização e continuidade das operações.

c) Princípio da proporcionalidade

A proporcionalidade se observa à medida que buscamos utilizar os meios

adequados, a fim de se atingir um determinado objetivo militar com um índice mínimo de destruição, baixas e danos às pessoas e aos bens envolvidos, durante os conflitos armados. Como uma definição simples, podemos dizer que se trata da relação entre o uso da força e o grau de baixas, destruição e efeitos colaterais causados por ocasião de ataque aos objetivos.

Dentro desse contexto, o Protocolo I Adicional às Convenções de Genebra de 1949, em seu artigo 57, aborda o princípio da proporcionalidade como a forma de abrir mão de realizar um ataque, do qual se possa esperar que venha a causar acidentalmente perdas de vidas humanas e ferimentos em não combatentes (CICV, 1998).

Devem ser considerados, ainda, os possíveis danos aos bens de caráter civil, bem como uma combinação das perdas e danos, considerados excessivos com relação à vantagem militar concreta e direta esperada (*Ibidem*).

Adicionalmente, cabe ressaltar que o princípio da proporcionalidade deve ser observado também para aqueles ataques possíveis de se causar danos desnecessários e prolongados ao meio ambiente, ainda que tenham como propósito obter alguma vantagem militar.

Conclui-se que, em função do princípio da proporcionalidade, os Estados partícipes de um conflito devem ser criteriosos e rigorosos ao medir os danos que podem ser causados por ocasião de um ataque a alvos militares, ou civis com fins militares, tentando sempre poupar as vidas humanas não envolvidas nas hostilidades e, do mesmo modo, evitar a destruição de bens civis e ambientais de forma indiscriminada.

d) Princípio da distinção

Este princípio institui que os Estados beligerantes envidem esforços para fazer a distinção entre combatentes e não combatentes, entre os bens de caráter civil e alvos militares, buscando realizar seus ataques e suas campanhas apenas contra objetivos militares. Os bens

de caráter civil e os não combatentes não devem ser alvos de ataques ou represálias (BRASIL, 2011).

De acordo com o Protocolo Adicional I, às Convenções de Genebras, em seu Art.48 fica bem clara a obrigatoriedade das partes beligerantes, em relação à proteção das vítimas dos conflitos armados:

> Com vista a assegurar o respeito e a proteção da população civil e dos bens de caráter civil, as Partes em conflito devem sempre fazer a distinção entre população civil e combatentes, assim como entre bens de caráter civil e objetivos militares, devendo, portanto, dirigir suas operações unicamente contra objetivos militares (CICV, 1998, p. 39).

Portanto, o princípio da distinção impõe que seja feita, pelas partes envolvidas em um conflito, a distinção dos combatentes e não combatentes, entre os bens civis e os objetivos militares.

Por este princípio, é imperativo que os ataques não sejam realizados de forma indiscriminada, ou seja, são proibidos todos os ataques que não são, ou não podem ser direcionados a um objetivo militar específico, bem como aqueles cujos danos não podem ser limitados, conforme exigido pelo DICA.

São ainda vedadas as investidas contra objetivos militares ou combatentes, que venham a vitimar civis incidentalmente ou causar estragos considerados excessivos, com relação à vantagem militar concreta e direta pretendida.

Em face ao exposto, pode-se observar que, de um modo geral, os princípios, além de relativos, necessitam de uma cuidadosa interpretação em todos os níveis de decisão. Os ataques e ações militares, que não sejam justificados e que não estejam fundamentados nos referidos princípios, podem conduzir, futuramente, a questionamentos no Tribunal Penal Internacional[7], principalmente, se houver dúvidas sobre a vantagem militar requerida.

Após descrever estes quatro princípios fundamentais do DICA, seguir-se-á adiante

[7] Organização Internacional Permanente criada por um tratado (Estatuto de Roma de 1998) para processar e julgar alguns crimes internacionais. O TPI tem como pilares o Princípio da Complementaridade e a Cooperação Internacional.

expondo a importância dos mesmos para a seleção de alvos.

2.3 A Importância dos princípios fundamentais do DICA para a seleção de alvos

Com vistas a contribuir para a solidez de um planejamento no qual se fará necessário o emprego de uma força militar, é fundamental que se tenha atenção quanto aos dados de inteligência que irão subsidiar uma precisa e correta seleção de alvos, bem como dos meios e métodos a serem empregados.

Devem ser consideradas particularidades quanto à localização dos alvos, além da necessária e devida vantagem militar que se busca obter, sem deixar de lado as informações sobre possíveis danos colaterais, efeitos e desdobramentos consequentes desse emprego, levando-se sempre em consideração os princípios e as normas que constituem o arcabouço legislativo do DICA.

Ainda que se revista de grande dificuldade e subjetividade realizar uma análise sobre a vantagem militar buscada e os possíveis efeitos colaterais que podem ser causados, é imprescindível que exista a constante preocupação, das partes envolvidas em um conflito, em se cumprir os princípios fundamentais do DICA. Em outras palavras, à parte das dificuldades interpretativas inerentes aos seus princípios, o respeito às normas do DICA, deve, em quaisquer circunstâncias, ser sempre o objetivo maior a ser atingido por ocasião de um conflito armado, levando-se sempre em consideração seu propósito maior de proteção aos combatentes e não-combatentes envolvidos.

Ao analisar os conflitos mais recentes, pode-se observar que a preocupação com os efeitos colaterais causados pelos mesmos e sua capacidade de atingir tanto a população, quanto os bens civis, tem aumentado de maneira relevante.

Atualmente, não há dúvidas do quão prejudiciais seriam, para o desenrolar de um conflito, as imagens de não combatentes ou bens de caráter civil sendo atingidos ou destruídos

por ocasião de uma operação militar. Portanto, a fim de mitigar tais efeitos negativos e de buscar o apoio da população e sociedade civil em relação às ações conduzidas durante um conflito, faz-se necessário realizar uma precisa análise física e uma criteriosa seleção dos alvos. Para tal, deve-se buscar obter informações suficientes sobre suas vulnerabilidades, o que subsidiará a decisão sobre quais os meios e métodos deverão ser utilizados, bem como a quantidade e a forma de serem empregados (BRASIL, 2011).

Considerando, portanto, como referência os quatro princípios do DICA estudados, a seleção de alvos, no caso de um conflito armado, deve ser fundamentada nos seguintes aspectos: a dignidade da pessoa humana, por meio do princípio da "humanidade", a fim de evitar o seu sofrimento desnecessário, seja combatente ou não; uma indubitável "necessidade militar" que os alvos selecionados devem possuir, ou seja, é imperativo que os mesmos apresentem uma vantagem militar concreta; as ações militares conduzidas sobre tais alvos devem ser "proporcionais", é desejável que não sejam observados danos colaterais excessivos aos civis ou aos bens de caráter civil; e a "distinção" entre os combatentes e os não combatentes, a fim de proteger a população civil.

Em função do exposto, observa-se que a principal contribuição de tais princípios não se restringe apenas ao objetivo de destruir os alvos selecionados, se não, a fim de serem definidos os meios e métodos a serem empregados, para se atingir estes alvos. Dessa forma, objetiva-se, principalmente, limitar os efeitos e danos colaterais que podem ser gerados para as populações e bens civis dos Estados beligerantes.

2.4 Conclusões parciais

Neste capítulo, realizamos a pesquisa sobre a evolução histórica do DICA, seus princípios e a importância dos mesmos para a seleção de alvos durante a condução de uma

campanha militar, bem como os reflexos gerados por ocasião da captura, destruição ou neutralização dos mesmos.

Ainda que existam meios e métodos utilizados em conflitos livres de proibições ou restrições impostas pelo DICA, os princípios estudados devem ser sempre observados, tendo em vista que, em qualquer ataque realizado, haverá sempre a possibilidade de ocorrerem perdas pessoais e materiais indesejáveis. Tais perdas, segundo as normas e entendimentos relacionados ao DICA, devem, sempre que possível, ser evitados, tendo em vista serem considerados supérfluos ou desnecessários.

Por fim, é importante repisar que todas as regras do DICA visam regular a conduta de hostilidades aplicáveis durante os conflitos armados e que, pelo seu caráter cogente, as mesmas revestem-se de uma singularidade importante: estabelece-se um conflito permanente entre o corpo de tratados e convenções internacionais (fontes do DICA) *versus* a conduta *tipificável* do Estado – e/ou de suas Forças Armadas – que se escuda em sua soberania, para deixar de observar as normas internacionais.

No capítulo seguinte, será feita uma abordagem sobre alguns conceitos, antecedentes históricos e origem do espaço cibernético. Além disso, serão analisadas algumas características do ciberespaço, suas possibilidades como um novo ambiente de conflitos interestatais e a ausência de limites territoriais e fronteiras nesse ambiente, o que algumas vezes pode representar uma ameaça à soberania dos Estados.

3 CONCEITOS E CARACTERÍSTICAS DO CIBERESPAÇO E DA GUERRA CIBERNÉTICA

É senso comum que a informação tem sido um item indispensável nas atividades das pessoas, ainda que, nos primórdios do desenvolvimento humano, não houvesse consciência de sua importância, tampouco, da necessidade de sua proteção (CARVALHO, 2011).

Adicionalmente, o advento da *internet* proporcionou conectividade em tempo real e abrangência mundial. Com isso, o volume de informações, cada vez mais acessíveis a todos, apresentou um aumento nunca antes observado. Em contrapartida, também cresceram as preocupações com os dados trafegados em rede, em função de sua extrema vulnerabilidade, combinado com as intenções diversas por parte dos variados atores existentes no cenário internacional (*Ibidem*).

É nesse contexto que um número cada vez maior de computadores e seus sistemas de interconexão e de apoio à decisão surgem como ferramenta fundamental, compondo o ambiente cibernético, dentro do qual o acesso a tais informações torna-se o objetivo principal (SILVA, 2014).

Nesse sentido, busca-se, neste capítulo, entender conceitos, características e possibilidades do ambiente cibernético. Ademais, quais atores estão inseridos no mesmo e como ocorrem as relações entre eles dentro de um ambiente ausente de fronteiras, mais especificamente, entre os atores estatais.

3.1 Antecedentes históricos e conceitos gerais do ambiente cibernético

A palavra cibernética tem sua origem na palavra grega *kubernetes*, que significa piloto ou, ainda, condutor, controlador, governador, ou aquele que tem o leme ou o timão,

podendo também, segundo Platão[8] (427 a.C. - 347 a.C.), ser relacionado à arte de governar (WIENER, 1973). Em 1948, o termo cibernética foi utilizado por Norbert Wiener (1973) abrangendo o conjunto formado pelos princípios de controle e de comunicação em uma máquina ou em um animal.

Dessa forma, possibilitou-se a criação de um ambiente intelectual em que o funcionamento e o controle de computadores, sistemas de comunicação e controle, comandos eletromagnéticos, transmissões eletrônicas nas máquinas de calcular e nos autômatos modernos pudessem ser desenvolvidos. Nesse contexto, Silva[9] definiu cibernética da seguinte forma:

> Uso de sistemas de comunicação e, consequentemente, de seus componentes, que são vitais para a troca de informações entre esses componentes, dentro de um mesmo sistema, e também entre o sistema e o ambiente (2014, p. 195).

Ainda que se tenha chegado a essa definição, o termo cibernética engloba outras proposições que vão além do singelo controle de sistemas computacionais, de comunicação e de informação via *internet* (OLIVEIRA, 2011). Ainda na opinião desse autor, que prefere não definir tal termo, seria um tanto quanto prematura a apresentação de conceitos, principalmente por se tratar de uma área tão dinâmica. Para ele, é preferível falar em entendimento acerca de um ambiente ou espaço cibernético, onde ocorre a interação entre pessoas, empresas e instituições públicas e privadas, nacionais e internacionais, que fazem uso de recursos atuais de Tecnologia da Informação e das Comunicações.

Nessa mesma linha, Mandarino Junior (2011) também escolheu por não conceituar cibernética, mas sim o espaço cibernético, ou ciberespaço, como sendo a totalidade de pessoas, empresas, equipamentos e as conexões entre os mesmos, bem como o conjunto dos sistemas de informações e de conhecimentos que trafegam entre tais atores.

---

[8] Importante filósofo grego nascido Atenas, provavelmente em 427 a.C e morreu em 347 a.C. É considerado um dos principais pensadores gregos, tendo em vista sua profunda influência na filosofia ocidental.

[9] Júlio Cezar Barreto Leite da Silva é Doutor em Ciências Navais pela Escola de Guerra Naval (EGN) e Mestre em Ciências da Computação e Informática, na área de Inteligência Artificial, pelo Instituto Militar de Engenharia (IME).

Para Gibson[10], o termo ciberespaço se aproxima bastante do conceito atribuído por Mandarino Junior, tendo em vista que designou o mesmo como um sistema interligado de computadores, roteadores, chaves e pessoas, que estava em constante transformação (1991 citado por SILVA, 2014).

Adicionalmente aos termos mencionados, surgem outros, também ligados à cibernética, que necessitam ser conhecidos, quais sejam, Operações Cibernéticas, Ataques Cibernéticos e Guerra Cibernética. Tais termos, mais voltados para a questão de segurança, envolvendo diretamente o instrumento militar, têm feito com que um número cada vez maior de computadores passasse a compor o espaço cibernético militar, que tem como objetivo maior a obtenção de informações (SILVA, 2014).

Inseridos nesse contexto, encontram-se também os sistemas de comando, controle, comunicações e informações, interconectados pelos seus diversos equipamentos, além dos sistemas que dão apoio à decisão,

No caso do termo Guerra Cibernética, na opinião de Silva (2014), não há, ainda, um senso comum para se definir tal termo. Entretanto, para ele, é possível conceituá-lo como um conflito estabelecido entre dois ou mais Estados dentro do ciberespaço, levando-se em consideração que ciberespaço, ou espaço cibernético, seria o ambiente operacional onde serão desencadeadas as interações entre os variados atores.

De uma forma mais completa, seriam as diversas ações ofensivas, defensivas e ou exploratórias, realizadas buscando-se negar o uso deste espaço pelo inimigo, bem como assegurar que o sigilo das informações contidas em computadores, redes e sistemas de comunicação serão usados em proveito próprio, juntamente com sua segurança, confiança, integridade e rapidez, seja na área militar ou na civil (*Ibidem*).

Já os ataques cibernéticos, podem ser enquadrados como as demais ações

[10] GIBSON, William. *Neuromancer*. 4. ed. São Paulo: Editora Aleph, 1991.

desencadeadas por outros atores, que não sejam os Estados, capazes de causar danos às informações.

Em face ao exposto, pode-se considerar que o espaço cibernético, nos dias de hoje, se reveste de grande importância durante um conflito, tendo em vista o destaque que os computadores ganharam dentro de um cenário militar, bem como as redes por onde trafegam grande quantidade de decisões, ordens e informações.

Ainda mais importante do que essas redes, são os acessos as mesmas e, consequentemente, às informações que por elas circulam. A utilização de tais informações em proveito próprio, constitui-se num importante objetivo dentro de uma guerra cibernética.

A seguir aborda-se como os Estados têm desenvolvido o chamado *Cyber Power* (do português, Poder Cibernético), sua relação com o domínio do ciberespaço e os atores que interagem no ambiente cibernético.

3.2 Cyber Power, o domínio do ciberespaço e os atores cibernéticos

Uma das características que define o ambiente das relações internacionais é o Equilíbrio de Poder que se estabelece entre os Estados e determina uma certa hierarquia entre os mesmos. Em termos teóricos, o Século XX teve na busca pelo poder um dos pilares principais do realismo clássico das relações internacionais (PECEQUILO, 2012).

No século atual, a disputa pelo poder, por parte dos Estados, segue no cerne das relações internacionais, entretanto, com o advento da cibernética e a nova realidade das relações no âmbito do ciberespaço, a tendência atual é de desenvolvimento de um novo tipo de poder, qual seja, o *Cyber Power*.

Ao longo dos últimos anos, os Estados se tornaram cada vez mais sabedores de que o poder cibernético lhes traz vantagens na busca da dominação da informação, não apenas no espaço cibernético, mas também em outros ambientes. Em função disso, o importante para

esses Estados, que almejam mais poder no cenário internacional, é otimizar o uso de seu poder cibernético, desenvolvendo-o em conjunto com seu *Hard Power*[11] e seu *Soft Power*[12] (BARROS, 2015).

A história mundial tem mostrado que o desenvolvimento de novas tecnologias leva à reflexão sobre as consequências que as mesmas trazem para as relações internacionais.

Assim ocorreu, por exemplo, quando o homem se lançou ao mar e estabeleceu o domínio dos mares, que levou à discussão sobre o poder naval. Da mesma forma, o domínio aéreo trouxe reflexões acerca do poder aéreo e, mais recentemente, o mesmo foi observado com o domínio espacial (NYE JUNIOR, 2011, tradução nossa). Com isso, conclui-se que a busca pelo desenvolvimento de um poder cibernético, por parte de alguns Estados, é reflexo da recente descoberta da importância do domínio do ciberespaço, definido, hoje, como o quinto domínio da guerra, após a terra, a água, o ar e o espaço.

É importante ressaltar que uma das características que diferencia este quinto domínio dos demais, despertando a curiosidade e motivando a pesquisa científica, é que o mesmo foi criado pelo próprio homem, ou seja, o domínio do ciberespaço não é um domínio natural. Tal fato faz dele um ambiente de mudanças rápidas e constantes, podendo cada vez mais alterar as relações de poder entre os Estados (BARROS, 2015).

Adicionalmente, pode-se destacar que, por não possuir limites reais, aliado às dificuldades de se estabelecerem fronteiras legais capazes de protegê-lo, este domínio pode tornar-se um ambiente de características complexas e hostis. Essas características do ciberespaço podem gerar uma instabilidade nas relações internacionais, tendo em vista as

---

[11] O *Hard Power* (do português, Poder Duro) é um conceito usado, principalmente, no realismo das relações internacionais e se refere a uma distinção quanto ao poder, relacionado à tipologia dos recursos de um Estado. Portanto, o Hard Power, ou poder duro, corresponde aos recursos de caráter tradicional de um Estado, quais sejam, suas dimensões territoriais, posicionamento geográfico, clima, demografia, capacidade industrial instalada, disponibilidade de matérias-primas e status militar (PECEQUILO, 2012).

[12] O *Soft Power* (do português, Poder Brando), usado em contraste com o termo *Hard Power*, corresponde ao poder de cooptação e refere-se às fontes de poder que advém da economia, ideologia, tecnologia e cultura, que correspondem à capacidade de adaptação, flexibilidade e convencimento de um determinado Estado sobre seus pares. Insere-se, portanto, nessa dimensão, a habilidade política de um Estado de disseminar seus valores, bem como de produzir modelos ideológicos de vida (Ibidem).

dificuldades de se controlar tudo o que ocorre em seu interior, facilitando, inclusive, a instauração de um conflito.

Outra preocupação, que se encontra inserida na realidade complexa do ciberespaço, diz respeito a grande diversidade de atores existentes nesse ambiente, os quais têm como característica comum o fato de estarem ligados a uma rede mundialmente conectada, qual seja, a *internet*.

Ainda que a grande parte dos atores estejam bem identificados, como, por exemplo, os Estados, as Corporações Industriais/Empresariais, o Setor Financeiro, o Setor de Serviços, Grupos de ativistas políticos/religiosos, *hackers*, criminosos digitais e pessoas comuns; os mesmos se multiplicam, em número e variedade, de acordo com o avanço das informações, comunicações e tecnologia. Outro fator, que também contribui para o aumento do número desses atores, é o acesso, cada vez maior, por parte da humanidade, às facilidades e aos meios e sistemas computacionais (SILVA, 2014).

É importante lembrar que, em função desta complexidade, o foco deste estudo estará voltado para as ações cibernéticas desencadeadas apenas pelos atores estatais – os próprios Estados e suas Forças Armadas. Além disso, cabe destacar que, para se falar de DICA, é preciso que seja observada a ocorrência de um conflito armado.

Inseridas nesse contexto, estarão as operações e os ataques conduzidos pelas partes beligerantes, recorrendo-se aos meios e métodos que utilizem o quinto domínio da guerra. Serão desconsideradas, portanto, as situações mais genéricas envolvendo a questão da segurança cibernética, como por exemplo os ataques realizados por *hackers*, criminosos digitais e demais atores cibernéticos.

Cabe ressaltar, ainda, que a realidade complexa do domínio do ciberespaço exige um grande investimento por parte dos Estados, visando desenvolver o seu poder cibernético. Entretanto, é preciso fundamentar tal investimento em dois aspectos principais: na utilização

da cibernética visando o aumento de sua influência no SI, inclusive como um incremento para o seu *Hard Power* e o seu *Soft Power*; e na criação de mecanismos de defesa de seu domínio cibernético, a fim de garantir a segurança das informações que trafegam pelo mesmo contra possíveis ações ou interferências externas.

Em sequência, estuda-se as especificidades que caracterizam o ambiente cibernético, em especial a inexistência de fronteiras desse ambiente e sua transversalidade pelos demais domínios.

3.3 A ausência de fronteiras e a transversalidade no domínio do ciberespaço

Atualmente os espaços e os domínios marítimo, terrestre e aéreo estatais são bem definidos e seus limites fronteiriços formalmente estabelecidos e, ainda que em alguns casos estejam sob litígio, são perfeitamente tangíveis e possíveis de serem medidos e identificados. O domínio espacial, apesar de não possuir fronteiras formais estabelecidas, não representa um problema para o SI, por ser considerado um ambiente internacionalizado, um *Global Common*[13].

No caso do domínio do ciberespaço, diferentemente dos demais domínios, as fronteiras são inexistentes. Conforme comentado anteriormente, por ser um domínio artificial, criado pelo homem, e que vive em constante mutação, o ambiente cibernético é um domínio ainda não conhecido completamente, sem uma clara definição, ausente de limites fronteiriços e ainda deficiente de uma normatização forte.

Essas características fazem com que o ciberespaço seja considerado como uma terra sem dono e, consequentemente, com grande potencialidade de se constituir em mais um tema para a disputa de poder no cenário internacional.

---

[13] *Global Common* (do português, Condomínio Global) pode ser entendido como espaços, áreas ou ambientes de recursos definidos como de uso comum e possíveis de serem explorados, para fins pacíficos, por qualquer Estado (BARROS, 2015).

Assim como o que ocorre nos espaços e ambientes recém descobertos e com uma regularização ainda não muito bem definida, pessoas de intenções duvidosas estão sempre buscando obter vantagens ilegais ou repugnáveis, por meio do uso do ciberespaço. Dessa forma, o espaço cibernético, por sua facilidade de acobertar pessoas e grupos, em função da distância e do anonimato, representa o palco propício para todos aqueles que buscam explorar alguma vantagem, por meio de informações e dados privilegiados (CANONGIA; MANDARINO JUNIOR, 2009).

Pode-se, em função dessa ausência de fronteiras, dizer que o ambiente cibernético, ou o domínio do ciberespaço, faz-se presente em toda e qualquer parte do globo, onde existam redes de computadores e equipamentos a elas conectados, ou controlados pelas mesmas. Isso faz desse novo domínio um ambiente, não apenas complexo, mas também vulnerável.

É nesse contexto que se insere a nova realidade das guerras assimétricas, onde atores com recursos limitados são capazes de causar grandes danos a um outro mais poderoso, bastando, para isso, um computador, ou outro equipamento, em qualquer local do mundo, inclusive bem próximo à vítima, conectado a uma rede de dados (CLARKE; KNAKE, 2015).

Vale dizer, são inúmeras as possibilidades de hostilidades que podem ser conduzidas utilizando o domínio do ciberespaço: desde um simples acesso a informações, até ataques para movimentar considerável quantia de valores, instruções para derramar petróleo, espalhar gás, explodir geradores, colidir aviões, neutralizar um sistema de radares, dentre outros (*Ibidem*).

Adicionalmente à ausência de fronteiras, o ambiente cibernético tem, como uma outra característica marcante, a transversalidade pelos demais domínios. Por meio de suas redes físicas ou não, o ciberespaço transpassa por todos os ambientes convencionais – terra, mar, ar e espaço – tendo nos mesmos suas raízes e ramificações (VENTRE, 2012, tradução nossa).

A transversalidade concebe, ainda, ao ciberespaço a capacidade de se propagar por tais domínios, já que em cada uma das dessas quatro dimensões, podemos encontrar *internet*, telecomunicações, infraestruturas de computação e informática, dados e tráfego de informações (*Ibidem*, tradução nossa).

Considera este autor, que a transversalidade permite que um ator, por meio do ciberespaço, projete seu poder, e seus efeitos, por todos os demais domínios. Contudo, seu uso indevido e descontrolado pode trazer reflexos sem precedentes, como por exemplo um ataque às infraestruturas estratégicas para um Estado, quais sejam, seu sistema energético (inclusive nuclear), sistemas de fornecimento de água, serviços de comunicações, sistema financeiro, dentre outros.

Conclui-se que o papel das normas reguladoras e, principalmente, da sua capacidade para limitar as relações e ações que ocorrem no ciberespaço, a fim de que o uso do mesmo esteja voltado, não para o prejuízo, mas sim, para o benefício da humanidade. É nesse contexto que o DICA ganha importância, principalmente devido à potencialidade dessas ações cibernéticas serem catastróficas, com danos consideráveis à humanidade, no caso de um conflito armado.

3.4 O ambiente cibernético e seus alvos

O domínio do ciberespaço e suas redes de dados nos fornecem vantagens e facilidades consideráveis, em contrapartida também implica em riscos, tendo em vista que dados privados, ou secretos, que se encontram armazenados, são alvos atrativos para os atores cibernéticos.

Se levar em consideração que atualmente são infinitos os sistemas e serviços que se encontram conectados e utilizando redes de computadores, as vulnerabilidades podem ficar ainda mais expostas e os problemas decorrentes podem ser ainda mais complexos.

O conjunto de alvos cibernéticos é amplo e variável, podendo incluir desde dados particulares existentes em redes sociais, passando por dados bancários, comerciais e financeiros, até chegar aos sistemas de defesa, sistemas de comunicações e outras infraestruturas críticas de um Estado.

Ainda que o principal objetivo das ações conduzidas no espaço cibernético seja o de obter informações e dados vitais, a sua transversalidade permite que os objetivos e alvos inseridos em uma guerra realizada no ciberespaço, da mesma forma que a realizada nos ambientes terrestre, marítimo, aéreo e espacial, também possam estar divididos nos níveis político, estratégico, operacional e tático, conforme discriminado a seguir (SILVA, 2014):

a) **alvos políticos**: além das próprias pessoas diretamente ligadas ao governo de um Estado, os alvos políticos seriam todos aqueles relacionados às informações sobre as políticas, ideologias, projetos e sistemas governamentais;

b) **alvos estratégicos**: todos os sistemas ligados à infraestrutura estatal de energia, ao sistema financeiro e à infraestrutura social (sistemas de transporte, abastecimento, dentre outros), que concorreriam para a redução do poder de defesa e resposta de um Estado;

c) **alvos operacionais**: sistemas de Comando, Controle e Comunicação Operacional, que contribuiriam para a redução do poder de coordenar e de apoiar às decisões e manobras de uma parcela das Forças Armadas de um Estado; e

d) **alvos táticos**: sistemas de comunicação, controle e monitoramento de uma Força Armada, ou de parcela de uma tropa, a fim de reduzir a capacidade logística e de defesa da mesma.

Adicionalmente, cabe ressaltar que quanto mais avançado e dependente em tecnologia é um Estado, maiores são suas vulnerabilidades e suscetibilidades às ações ofensivas por parte dos atores cibernéticos.

Em função das características de uma guerra cibernética, existe uma tendência para que os primeiros ataques e ações no domínio do ciberespaço ocorram sobre alvos de caráter civil. O objetivo seria afetar diretamente os serviços que um Estado presta à sua população, como sistemas de voos dos aeroportos, sistemas bancários e sistemas de abastecimento de água e de fornecimento de energia elétrica. Como exemplo, tem-se a interrupção das comunicações mundiais ocorrida na Geórgia, por ocasião da crise com a Rússia.

A inegável importância de tais sistemas para um Estado e sua sociedade, faz com que os impactos causados pelo emprego de armas cibernéticas, ainda que menores que aqueles causados pelo uso de armamento nuclear, em algumas situações, possam trazer grandes prejuízos e levar a um conflito de maiores proporções (CLARKE; KNANE, 2015).

Conclui-se, embora não sejam frequentes as ocorrências de mortes diretas, como consequência de ataques cibernéticos, que os mesmos têm reflexos consideráveis em serviços essenciais. Além disso, os ataques por meio do ciberespaço são capazes de produzir grandes prejuízos e impactos profundos à economia, à sociedade e, sobretudo, à defesa e segurança de um Estado.

3.5 Conclusões parciais

Neste capítulo, realizou-se a pesquisa sobre os antecedentes históricos do ambiente cibernético e sobre alguns conceitos gerais que se encontram inseridos no mesmo. Buscou-se relacionar o equilíbrio de poder, observado no século passado, com uma realidade atual de disputa por um novo poder, o *Cyber Power*, bem como a importância de se desenvolver este novo poder em conjunto com o *Hard* e o *Soft Power* de um Estado.

Identificou-se o ambiente cibernético como o quinto domínio da guerra e buscou-se destacar algumas de suas características marcantes, dentre elas a ausência de limites e

fronteiras legais, bem como a diversidade de atores que interagem neste domínio, que o torna um ambiente complexo e muitas vezes hostil. Dessa forma, observou-se que os Estados foram levados a desenvolver seu poder cibernético investindo não somente com vistas a aumentar sua capacidade tecnológica, mas também com o objetivo de criar mecanismos de defesa e de proteção de suas informações, dados e sistemas em geral.

Em função da ausência de fronteiras, verificou-se o importante o papel das normas reguladoras no sentido de coibir e limitar as ações de atores mal intencionados, tendo em vista que são inúmeras as possibilidades e variedades de ações, algumas hostis, que podem ser realizadas dentro do ciberespaço, incluindo danos em sistemas financeiros, infraestruturas estratégicas e bens civis.

Ainda sobre as características do domínio do ciberespaço, buscou-se ressaltar a sua transversalidade pelos domínios tradicionais (terra, mar, ar e espaço), que permite a um ator projetar seu poder sobre estes demais domínios. Buscou-se, também, identificar os alvos existentes no ambiente cibernético e algumas das possíveis consequências, para os Estados e suas sociedades, no caso de alguns desses alvos serem atingidos por ataques cibernéticos.

Portanto, considera-se que há a necessidade de normas jurídicas internacionais capazes de regular as atividades no ciberespaço, principalmente no caso de um conflito. O objetivo seria evitar os danos decorrentes de um ataque cibernético, com consequências indesejáveis às pessoas e bens protegidos pelo DICA.

É nesse contexto, que será avaliado, no próximo capítulo, se as legislações existentes atualmente atendem a um possível conflito travado no ciberespaço, bem como as possibilidades de se aplicar os princípios atuais do DICA na seleção de alvos, em uma guerra no ambiente cibernético.

4 APLICABILIDADE DO DICA NA SELEÇÃO DE ALVOS EM AÇÕES DE GUERRA CIBERNÉTICA

Neste capítulo, analisam-se documentos e legislações internacionais utilizados atualmente para orientar e regulamentar os conflitos armados e a aplicabilidade dos mesmos sobre as ações realizadas no domínio do ciberespaço, em particular, sobre a aplicação do DICA.

Ademais, busca-se verificar a aplicabilidade do DICA na seleção de alvos, por ocasião de um ataque cibernético, bem como as frequentes preocupações para que danos colaterais excessivos sejam mitigados e a população e bens civis protegidos.

4.1 As legislações internacionais reguladoras aplicadas no quinto domínio

No segundo capítulo, foi verificado que o DICA claramente prescreve a obrigação dos Estados de avaliar os meios e métodos a serem empregados no caso de um conflito armado. Considera-se esse o grande desafio do DICA, tendo em vista que a história mostra uma constante evolução dos meios e métodos de se fazer uma guerra, decorrentes do desenvolvimento tecnológico.

Por conseguinte, o conflito travado no domínio do ciberespaço, como método contemporâneo de se fazer a guerra, impõe desconfianças e questionamentos em relação às normas atualmente existentes, tendo em vista não haver regra particular, no ramo do DICA, para as ações desenvolvidas nesse domínio.

Uma aplicação eficaz das normas do DICA ao conflito cibernético é objeto de muita discussão por órgãos internacionais, juristas e autoridades militares, muito em função de pressões exercidas pelos Estados, que não estão dispostos a abrir mão de suas capacidades de guerra cibernética ou, até mesmo, de limitá-las (PAGANINI, 2012, tradução nossa).

Tal fato torna difícil a construção de um entendimento harmonioso sobre a sua normatização, tendo em vista que associar uma visão legal com os objetivos estatais é algo complexo, em virtude dos seus reflexos sobre o poder e sobre as relações dos poderes interestatais.

O Assessor Jurídico do Departamento de Estado dos Estados Unidos da América, Koh, entende que o domínio do ciberespaço não pode ser encarado como um ambiente isento de regras:

> O ciberespaço não é uma zona "livre do direito", onde qualquer um pode realizar atividades hostis, sem regras ou restrições. […] Esta não é a primeira vez que a tecnologia mudou e que o direito internacional tem sido solicitado a lidar com essas mudanças. Em particular, porque as ferramentas de conflito estão em constante evolução, um conjunto de leis relevante - o direito internacional humanitário, ou a lei de conflito armado - antecipa de forma positiva a inovação tecnológica, e prevê que as suas regras existentes serão aplicadas a tal inovação. Não há dúvidas, novas tecnologias levantam novas questões e, portanto, novas perguntas (2012, p. 3, tradução nossa).

Depreende-se, pelo exposto, que, independentemente dos diferentes entendimentos e visões acerca da aplicação do DICA à luz de um conflito no ciberespaço, bem como da ausência de legislações específicas para tal, pode-se considerar que os atos cometidos no domínio do ciberespaço também estão sujeitos às regulamentações internacionais para os conflitos armados.

A aplicação dos tratados que compõem o DICA deve ser realizada de forma que não sejam impostos impedimentos ou limites por ocasião da proteção aos bens civis e aos não combatentes, ainda que utilizando esse novo domínio e os meios e métodos disponíveis no mesmo.

As dificuldades inerentes à regulamentação de uma ofensiva cibernética são diversas. Dentre algumas, pode-se chamar atenção para a difícil tarefa de se identificar os responsáveis por um ataque no domínio do ciberespaço, tendo em vista que os mesmos podem ser oriundos de qualquer lugar do mundo. Dessa forma, custa-se atribuir a um Estado específico a responsabilidade por determinada agressão.

Outro grande desafio seria dimensionar a partir de que ponto um ataque cibernético pode ser considerado como um ato de agressão, ou de uso da força, e, por conseguinte, sujeitar o Estado agressor às normas do DICA (MELZER, 2011, tradução nossa).

Estes mesmos desafios e dificuldades foram visualizados por Koh (2012, tradução nossa), que declarou a importância de serem avaliados alguns fatores, a fim de verificar se determinado ataque cibernético pode ser enquadrado como uso da força. Tais fatores, segundo ele, seriam: o alvo e a sua localização, os efeitos do ataque, as intenções com tal ataque e o principal personagem do ataque (caso o mesmo seja identificado).

Diante disso, este autor considera que, se os danos materiais de um ataque cibernético puderem ser comparados aos efeitos físicos causados por um armamento cinético, o referido ataque pode ser encarado como um ato de agressão ou uso da força.

Objetivando auxiliar na classificação de um ataque cibernético como um ato de agressão e, em especial, visando contribuir para a resolução do problema da aplicabilidade do DICA, no caso de um conflito no ciberespaço, um Grupo Internacional de Peritos criou o Manual Tallinn[14], aplicado à Guerra Cibernética.

Dentre outras medidas, o referido manual propõe oito critérios, sobre os quais é possível enquadrar uma ação no domínio do ciberespaço como uso da força, quais sejam: gravidade, urgência, imediatismo, invasão, capacidade de medir os efeitos, caráter militar, envolvimento do Estado e legalidade presumida.

Confirmada a possibilidade de se realizar o enquadramento de um ataque cibernético como um ato de agressão, ou uso da força, o Estado vítima pode, na sequência, recorrer ao seu direito de legítima defesa.

A próxima seção tem como objetivo analisar o *jus ad bellum* e o *jus in bello*, juntamente com os princípios fundamentais do DICA, e as possibilidades de sua aplicação

[14] Disponível em: < https://ccdcoe.org/research.html >. Acesso em: 12 jul. 2016

para a seleção de alvos na guerra no quinto domínio.

4.2 *Jus ad Bellum*, *Jus in Bello* e a seleção de alvos no ambiente cibernético

Conforme foi visto na seção anterior, a criação do Manual Tallinn representa um esforço na busca de orientações e sugestões, para lidar com os principais questionamentos jurídicos relacionados à guerra cibernética e de uma melhor adequação e aplicabilidade do DICA a um conflito nesse domínio.

Dessa forma, pode-se observar que a ideia força do Manual Tallinn é a de confirmar que as normas jurídicas internacionais, atualmente em vigor, em especial aquelas que compõem o DICA, podem perfeitamente regular a guerra no quinto domínio. Dentre tais regras, estão as leis que dão o direito ao início de um ataque armado, o *jus ad bellum*, bem como, aquelas que regulam a conduta durante os conflitos armados, o *jus in bello*, (MÄLKSOO, 2013, tradução nossa).

A fim de melhor compreender a aplicação do *jus ad bellum* e do *jus in bello* no domínio do ciberespaço, será realizada uma exposição de seus conceitos separadamente. A intenção é relacioná-los com a seleção de alvos, à luz dos princípios fundamentais do DICA, dentro do contexto de um conflito armado, onde sejam observadas operações no ambiente cibernético.

a) Jus ad Bellum

Segundo Melzer (2011, tradução nossa), a principal fonte do *jus ad bellum* é a Carta da Organização das Nações Unidas (ONU), a qual estabelece as condições, a título de exceções, que justificam o uso da força por um Estado. Para este estudo, analisam-se as duas situações, quais sejam, de **autorização do Conselho de Segurança (CS) da ONU** ou de **legítima defesa individual ou coletiva** (grifo nosso).

Ao analisar-se a questão de autorização, pelo CS, do uso da força, a Carta da

ONU, em seu artigo 39, transmite ao CS a responsabilidade na determinação da existência de qualquer ameaça à paz. O CS pode, ainda, recomendar ou decidir sobre as medidas que serão tomadas em observância aos seus artigos 41 e 42, com a finalidade de manutenção ou restabelecimento da paz e da segurança internacionais (ONU, 2001).

Em função do exposto, no caso de autorização do uso da força, por parte do CS, como resposta a um ataque por meio do ciberespaço, as ações legais a serem executadas devem ser observadas e enquadradas nas situações previstas para tal e de acordo com orientações e determinações daquele Conselho.

Quanto ao direito da legítima defesa individual ou coletiva, em seu artigo 51, a Carta da ONU assegura a um Estado membro, no caso de um ataque armado contra ele próprio ou a outro membro, o direito de legítima defesa, enquanto o CS toma as medidas e providencias necessárias à manutenção da paz (ONU, 2001).

Ainda que o cerne para se considerar a legalidade do argumento de legítima defesa se concentre na ocorrência de um ataque armado, para Melzer (2011, tradução nossa), os ataques realizados no ambiente cibernético possuem a qualificação para serem enquadrados como tal.

Adicionalmente, cabe ressaltar que em caso de uso do direito à legítima defesa, deve-se ainda levar em consideração a observância aos princípios da necessidade militar e da proporcionalidade (CIJ, 1986).

Dentre os diversos questionamentos quanto ao uso da legítima defesa, um deles consiste na dúvida de como se recorrer a um ataque armado, utilizando forças e armamentos convencionais, como resposta a um ataque cibernético, sem, entretanto, ferir tais princípios.

Os Estados Unidos da América, em sua *International Strategy for Cyberspace*[15] (2011), declaram que, sempre que justificável, irão responder aos atos de agressão ocorridos

[15] Estratégia Internacional para o Ciberespaço (tradução nossa).

no ciberespaço igualmente como responderiam a qualquer outro tipo de ameaça àquele Estado (KOH, 2012, tradução nossa).

Em resumo, pode-se dizer que é possível aplicar o *jus ad bellum* em uma situação de ataque no ciberespaço, ainda que isso seja considerado um desafio às legislações atuais, tendo em vista que pode dar ensejo ao início de um conflito armado. Para tal, entretanto, é preciso que sejam fixados critérios transparentes para classificar ataques cibernéticos como uso da força e, a partir de então, definir quais devem ser enquadrados como ataques armados.

Conclui-se que, nesse caso, o Estado que sofrer um ataque poderá recorrer ao uso da força, seja ela convencional ou cibernética, lançando mão do *jus ad bellum*, por meio do seu direito de legítima defesa, desde que devidamente autorizado pelo CS da ONU, cumpridas as normas em vigor e observando os princípios da necessidade e proporcionalidade.

b) Jus in Bello

A natureza do *jus in bello* tem como procedência as fontes do DICA, compostas, principalmente, pelas quatro Convenções de Genebra (1949), juntamente com seus dois Protocolos Adicionais de 1977, o Direito de Haia (1907), bem como os demais tratados responsáveis por impor restrições e proibições quanto à utilização de determinados armamentos.

Seu propósito é regular o comportamento dos beligerantes, a partir do momento em que se inicia um conflito armado, a fim de garantir a proteção dos bens civis e das vítimas da guerra, juntamente com seus direitos fundamentais, seja qual for a parte a que pertençam (BRASIL, 2009).

O Protocolo Adicional I, às Convenções de Genebra, em seu artigo 35, determina restrições aos Estados envolvidos em um conflito armado para escolherem os meios e métodos a serem utilizados nas hostilidades (CICV, 1988).

Para o caso da existência de novos armamentos, o mesmo protocolo, em seu

artigo 36, determina que os Estados analisem a proibição, por parte do DICA, de sua utilização ou não, por ocasião do estudo, da preparação, desenvolvimento ou aquisição desses novos armamentos, meios e métodos de guerra (CICV, 1988).

Na opinião de Gisel (2013), independente do tipo de armamento, meios ou métodos utilizados nos conflitos armados, deve ser garantido que os Estados cumpram as normas internacionais em vigor. Espera-se, com isso, que a proteção estabelecida pelo DICA não seja descumprida ou colocada em segundo plano em função do avanço da tecnologia que, na situação em lide, encontra-se representado pelo advento da guerra no quinto domínio (GISEL, 2013).

Considera, este autor, que a opinião de Gisel é reforçada pelo DICA, tendo em vista que a Cláusula Martens[16], constante no relatório que antecedeu a Convenção de Haia (1899), na época decretou o seguinte:

> Enquanto se forma um Código mais completo das leis da guerra, as Altas Partes Contratantes julgam oportuno declarar que, nos casos não compreendidos pelas disposições regulamentárias por elas adotadas, as populações e os beligerantes permanecem sob a garantia e o regime dos princípios do Direito das Gentes preconizados pelos usos estabelecidos entre as nações civilizadas, pelas leis da humanidade e pelas exigências da consciência pública (CICV, 2001, p. 16).

Dessa forma, pode-se dizer que não existem aberturas jurídicas para o domínio do ciberespaço, já que o DICA, pela sua abrangência, é capaz de alcançar as novas tecnologias existentes, bem como aquelas que ainda se encontram em desenvolvimento (DROEGE, 2011).

Tal afirmativa ganha mais força quando se recorre ao artigo 1 do Protocolo Adicional I, às Convenções de Genebra, que estabelece a proteção dos civis e combatentes por parte dos princípios fundamentais do DICA, dos princípios humanitários e da consciência pública, ainda que em situações ou casos não previstos nestes dispositivos ou em qualquer outro (CICV, 1998). Essas situações ou casos, não previstos, podem ser perfeitamente entendidos como aquelas, ou aqueles, ocorridas nos conflitos conduzidos no quinto domínio.

[16] Esta cláusula foi baseada e teve o seu nome a partir de uma declaração lida pelo Professor Fyodor Fyodorovich Martens (1845-1909), delegado russo nas Conferências de Haia Paz, de 1899.

Em face ao exposto, conclui-se ser consensual o fato de que, independente dos meios e métodos de guerra utilizados, sejam os mesmos convencionais e regulados, ou não, a população civil e seus bens, bem como os combatentes, devem estar sempre assegurados pelos princípios fundamentais do DICA e pelo *jus in bello*.

Tais aspectos são importantes e imprescindíveis para o processo de seleção de alvos, por ocasião de um conflito, qualquer que seja o domínio. Sendo assim, considerando que os princípios do DICA já foram objetos de estudo no segundo capítulo deste trabalho, é preciso agora relacioná-los com a seleção de alvos, nos conflitos travados no ambiente cibernético.

Pelo princípio da humanidade, o objetivo maior é a busca pela preservação da pessoa humana e a garantia de seus direitos, a fim de que sejam evitadas arbitrariedades durante os conflitos armados. Tal princípio constitui a razão de ser do DICA, tendo em vista que as limitações impostas aos beligerantes, visando à proteção da população civil e de seus bens, são estabelecidas por razões humanitárias (BRASIL, 2009).

Em função disso, é fundamental a observância da humanidade também por ocasião dos conflitos ocorridos no domínio do ciberespaço, a fim de que não sejam conduzidos ataques indiscriminados e sem limites aos sistemas de computadores e redes que fazem parte de infraestruturas críticas – como usinas nucleares, por exemplo. Tais infraestruturas, se afetadas, podem trazer consequências calamitosas e desumanas para um Estado e sua população civil.

É, pois, necessário que seja dada a devida proteção aos civis e seus bens, buscando sempre a preservação da pessoa humana, conforme já citado, e evitando que sejam proporcionados sofrimentos desnecessários.

Essa diferenciação, existente entre população civil e combatentes, corresponde ao pilar do princípio da distinção. Dessa forma, por ocasião da seleção de alvos durante as ações

conduzidas no ambiente cibernético, tal princípio deve ser observado buscando-se que os ataques sejam dirigidos unicamente contra alvos militares (BRASIL, 2009). Ou seja, computadores, ou seus sistemas, que não fazem parte das infraestruturas militares, ou de apoio às mesmas, não podem ser objetivos de uma operação no quinto domínio.

Sistemas de computadores de estabelecimentos específicos para atendimentos dos civis, como redes de hospitais e de escolas, por exemplo, não devem ser alvos de ataques cibernéticos (DROEGE, 2011).

Dessa forma, este autor considera que o fato do domínio do ciberespaço ser um ambiente de elevada conexão entre as redes de instituições militares e civis preocupa o CICV, tendo em vista que isso representa uma dificuldade quando se deseja reduzir os reflexos, em um sistema civil, de um ataque cibernético a um alvo classificado como objetivo militar. Nesse caso, é importante que seja levando em consideração o princípio da necessidade militar.

Com base nesse princípio, Gisel (2013) destaca o cuidado que se deve ter ao executar um ataque cibernético contra os sistemas de computadores de um Estado. Tal cuidado é importante, em função do risco que um ataque cibernético pode representar para os serviços destinados ao atendimento da população civil, como redes de fornecimento de água potável, assistência médica, eletricidade e demais serviços básicos, que, inoperantes, afetariam diretamente os não combatentes.

De acordo com o princípio da necessidade militar, a adoção de medidas, que não estejam proibidas pelo DICA, são justificáveis, desde que sejam indispensáveis para contribuir com o atingimento dos objetivos militares e, consequentemente, com o cumprimento da missão atribuída.

Dentro desse contexto, Koh (2012, tradução nossa) chama a atenção para os danos colaterais que podem ser observados por ocasião do ataque a computadores não classificados como objetivos militares diretos, mas que estejam ligados às redes de uso comum, que dão

acesso aos mesmos. Nesse caso, a intensidade de tais ataques deve ser criteriosamente avaliada pelas partes beligerantes, conforme estabelecido pelo princípio da proporcionalidade, a fim de que seja utilizada na medida certa, para atingir os sistemas ligados às infraestruturas militares.

No entendimento deste autor, um bom exemplo para o caso em tela, diz respeito a um ataque a servidores e roteadores civis, que não seriam os alvos diretos da ação, mas que que podem servir para dar acesso a sistemas de computadores militares, tendo em vista que ambos estariam conectados à *internet*.

Pode-se, com base no que foi analisado nesta seção, concluir que é possível aplicar o *jus ad bellum* dentro do contexto de um conflito no ambiente do ciberespaço. No entanto, é desejável o estabelecimento de critérios bem definidos para classificar um ataque cibernético como uso da força, enquadrando-o como um ataque convencional e, a partir de então, permitir ao Estado vítima o direito de legítima defesa.

É importante ressaltar, porém, que a força a ser empregada, por ocasião do exercício do direito de legítima defesa, seja ela utilizando meios e métodos convencionais ou cibernéticos, deve ser devidamente normatizada, com vistas a cumprir, principalmente, os princípios do DICA.

Igual conclusão pode-se estabelecer com relação à aplicação do *jus in bello*, para a guerra no quinto domínio. Cabe ressaltar, mesmo que ainda não se falasse em ambiente cibernético na época de criação do arcabouço jurídico internacional, que tais normas já previam regras que contemplavam o surgimento de novas tecnologias, armas e métodos de se fazer a guerra.

Nesse caso, apesar do princípio da distinção ter uma grande importância, em função da possibilidade de utilização dos sistemas que compõem as estruturas cibernéticas igualmente por militares e civis, o princípio da humanidade ganha importância destacada por

ser um grande limitador para utilização dessas novas tecnologias.

Em contrapartida, esse princípio pode servir também como argumento e justificativa para o uso de meios e métodos que utilizam o ambiente cibernético para realizar um ataque a um outro Estado. O ataque, por meio do ciberespaço, seria realizado em detrimento ao uso de meios e armamentos convencionais, com potencial de causar danos colaterais catastróficos à população e bens civis.

A fim de ilustrar tal possibilidade, este autor apresenta o caso do ataque, por meio do vírus *Stuxnet*, ao sistema de controle das centrífugas de enriquecimento de urânio do Irã. Esse ataque obteve o êxito desejado, tendo em vista que conseguir retardar o programa nuclear daquele Estado, sem, entretanto, proporcionar consequências ou danos indesejáveis para a população civil iraniana.

Muito provavelmente, isso não teria sido possível de ser alcançado por meio de um ataque com armamento convencional, com mísseis, por exemplo. Ainda que o caso em lide não tenha ocorrido dentro do contexto de um conflito armado, o mesmo ajuda a exemplificar um novo meio de se fazer uma guerra, sem grandes reflexos para a humanidade.

4.3 Conclusões parciais

Pode-se concluir que o DICA, apesar de criado na época em que ainda não se vislumbrava o advento de uma guerra cibernética, estabelece regras importantes, que podem servir para balizar as decisões e condutas dos Estados, acerca de um conflito no domínio do ciberespaço, sendo, sim, capaz de impor os limites necessários para uma guerra nesse contexto.

Isso porque o DICA, apesar de não mencionar de forma específica as operações no ambiente cibernético, mostra-se amplo o suficiente para alcançar o desenvolvimento dos meios e métodos de se fazer a guerra, incluindo aqueles inseridos no cenário de um conflito

no quinto domínio. Além disso, ainda não há um campo de batalha exclusivamente virtual, completamente dissociado do mundo real, no qual ocorra unicamente uma guerra cibernética, para justificar a necessidade de se criar uma legislação completamente nova para regulá-la.

Não obstante, em complemento às normas internacionais vigentes para o conflito armado, o advento do Manual Tallinn surgiu, com suas orientações e sugestões, como uma demonstração do esforço internacional na busca de uma melhor interpretação e aplicação, por parte dos Estados, dos principais aspectos jurídicos relacionados à guerra cibernética.

Adicionalmente, foi verificado, ainda, ser possível aplicar os princípios fundamentais do DICA na seleção de alvos por ocasião de uma operação cibernética. Entretanto, é importante que os Estados tenham sempre a consciência sobre as possíveis consequências e danos colaterais de um ataque, por meio daquele domínio, para a população civil.

Em contrapartida, ao mesmo tempo que os ataques cibernéticos podem ser extremamente calamitosos e prejudiciais à população e bens civis, os mesmos podem também representar um meio alternativo, menos destrutivo, para se conduzir ataques sobre infraestruturas críticas de um Estado. Tal possibilidade já se torna mais difícil quando são utilizados armamentos convencionais, os quais, em sua grande maioria, geram consequências indesejáveis.

Em resumo, conclui-se que os ataques por meio do domínio do ciberespaço, podem ser um meio mais brando de ataque, quando comparado a um ataque cinético com armamento convencional. O caso do vírus *Stuxnet*, apesar de não ter ocorrido no contexto de um conflito armado, pode servir para exemplificar tal possibilidade.

De qualquer forma, ainda que se tenha verificada a aplicabilidade do DICA para um cenário de conflito no ciberespaço, bem como para o processo de seleção de alvos naquele domínio, isso não significa que seja totalmente desnecessário um aprimoramento das normas

internacionais que o compõem.

Isso porque, as novas tecnologias, os meios e os métodos de se fazer a guerra seguem evoluindo, da mesma forma que os seus potenciais de causar impactos negativos sobre a humanidade. Para tal, é fundamental uma participação mais efetiva e flexível dos Estados nas questões que envolvem o incremento do arcabouço jurídico internacional para as novas realidades e ameaças dentro do SI.

5 CONCLUSÃO

Com o processo de desenvolvimento dessa nova realidade que é o ciberespaço, o DICA vê-se desafiado pelas possibilidades impostas por este novo domínio e também pelas novas relações interestatais, advindas da era da informação. Diante dessa realidade, este trabalhou foi desenvolvido com o propósito de responder se há possibilidade de aplicação do DICA no processo de seleção de alvos no ambiente cibernético.

Para o atingimento deste objetivo, buscou-se compreender como se deu a criação e evolução do DICA, conhecer seus princípios e a importância dos mesmos no processo de seleção de alvos. Além disso, realizou-se uma abordagem sobre os antecedentes históricos, principais conceitos e algumas características do ciberespaço.

Realizou-se, posteriormente, uma análise se as normas internacionais vigentes, incluindo os seus princípios fundadores e as particularidades das demandas impostas atualmente, atendem ou não a um possível confronto travado no ciberespaço, principalmente, no que tange a seleção de alvos nesse domínio. Pôde-se, com isso, verificar a importância de cada um desses princípios para o processo de seleção de alvos, tendo como foco, sempre, a redução dos efeitos causados por um conflito armado.

Ademais, buscou-se estabelecer um paralelo entre o equilíbrio de poder que marcou o século passado com uma nova realidade de poder, qual seja, o *Cyber Power*, que, desenvolvido tanto para incrementar o *hard power*, quanto para, diplomaticamente, auxiliar o *soft power* de um Estado, pode levar a mudanças nas relações existentes, atualmente, no SI.

Dessa forma, foram apresentados os desafios trazidos a partir da identificação do ambiente cibernético como um quinto domínio da guerra, em função, principalmente, de algumas características desse novo domínio. Em particular, destacou-se a ausência de fronteiras e limites territoriais do ciberespaço, a diversidade de atores presentes no mesmo, bem como a sua transversalidade pelos demais domínios.

Em especial, o estudo considerou a elaboração do Manual Tallinn, formulado para auxiliar, com orientações e sugestões, no processo de enquadramento de um ataque cibernético como uso da força e de como os Estados podem exercer seu direito à legítima defesa.

Depreende-se, em que pese a existência de novos meios e métodos que possam ser utilizados em conflitos armados convencionais, ou propriamente no domínio do ciberespaço, que as normas e as regras do DICA devem ser sempre observadas, respeitadas e cumpridas.

Com isso, objetiva-se atender aos seus princípios, que visam evitar a ocorrência de perdas na população e nos bens civis, bem como outros danos colaterais que possam ser considerados desnecessários. Essa premissa é *sine qua non* dentro do contexto de um conflito, ainda que as fontes do DICA, de caráter cogente, abram lacunas para que os Estados, escorando-se em suas soberanias, deixem de observá-las.

Diante do exposto, conclui-se que o DICA estabelece regras e procedimentos que podem servir sim para limitar ações, meios e métodos de combate utilizados por um Estado, por ocasião de um conflito no ambiente cibernético. Isso ocorre em função da amplitude e abrangência do arcabouço jurídico que compõe o DICA, que o torna capaz de englobar, até mesmo, as formas de se fazer a guerra, que ainda se encontram em desenvolvimento, como é o caso da guerra no quinto domínio.

Acresce-se a isso o fato de não existir um cenário de batalha totalmente virtual, completamente dissociado do mundo real, onde possa ocorrer um conflito exclusivamente cibernético, que justificasse a necessidade de uma nova legislação para normatizá-lo. Os reflexos de um ataque cibernético acabam sempre recaindo sobre a realidade material.

Esta pesquisa concluiu, ainda, que as operações no ciberespaço podem também representar um meio mais brando e alternativo para se conduzir ataques sobre infraestruturas de um Estado, se comparadas aos ataques utilizando-se armamentos convencionais – cujo

exemplo foi o vírus *Stuxnet*, que, apesar de não ter ocorrido no contexto de um conflito armado, serve para ilustrar tal conclusão.

Por fim, este autor considerou que, mesmo sendo constatada a conveniência da aplicabilidade do DICA e de seus princípios no processo de seleção de alvos no ciberespaço, existe a necessidade de aprimorar as legislações hodiernas, visando um enquadramento mais específico das mesmas em relação à utilização de novas tecnologias dentro do contexto de um conflito na era da informação.

REFERÊNCIAS

BARROS, Renata Furtado de. *Guerra Cibernética: Os Novos Desafios do Direito Internacional*. 1 ed. Belo Horizonte: Ed. D'Plácido, 2015. 178 p.

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

BRASIL. Estado Maior da Armada. *EMA-135: Manual de Direito Internacional Aplicado às Operações Navais*. Brasília. 2009

BRASIL, Ministério da Defesa. *MD34-M-03: Manual de Emprego do Direito Internacioanl dos Conflitos Armados (DICA) nas Forças Armadas*. 1ª ed. Brasília. 2011.

CANONGIA, Claudia; MANDARINO JÚNIOR, Raphael. *Segurança cibernética: o desafio da nova Sociedade da Informação*. Parcerias Estratégicas - Revista do Centro de Gestão e Estudos Estratégicos do Ministério da Ciência e da Tecnologia, Brasília, v. 14, n. 29, 2009. pp. 21-46.

CARVALHO, Paulo Sergio Melo de. *O setor cibernético nas Forças Armadas Brasileiras*. In: BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de. (Org.). Desafios Estratégicos para a Segurança e Defesa Cibernética. 1 ed. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. pp. 13-36.

CLARKE, Richard A.; KNAKE, Robert K. *Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito*. Tradução de Bruno Salgado Magalhães, Davidson Rodrigo Boccardo, Rafael Soares Ferreira, Raphael Carlos Santos Machado e Ricardo Salvatore. 1. ed. Rio de Janeiro: Brasport, 2015. 241 p.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA – CICV. *Direito Internacional Relativo à Condução das Hostilidades: Compilação de Convenções de Haia e de alguns outros Instrumentos Jurídicos*. Genebra, 2001 (português).

COMITÊ INTERNACIONAL DA CRUZ VERMELHA – CICV. *Protocolos Adicionais às Convenções de Genebra de 12 de agosto de 1949*. Genebra, 1998 (português).

DEYRA, Michel. *Direito Internacional Humanitário*. Tradução de Catarina de Albuquerque e Raquel Tavares. Lisboa: Procuradoria-Geral da República, Gabinete de Documentação e Direito Comparado, 2001. 167 p. Título original: Droit International Humanitaire. Disponível em: <http://www.gddc.pt/direitos-humanos/DIHDeyra.pdf>. Acesso em: 08 jun. 2016.

DROEGE, Cordula. *No legal vacuum in cyber space. 18 ago. 2011. Entrevista concedida ao International Committe of the Red Cross (ICRC)*. Disponível em: <http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm>. Acesso em: 19 jul. 2016.

FRANÇA, Júnia Lessa; VASCONCELLOS, Ana Cristina de. *Manual de Normalização de Publicações Técnico-Científicas*. 8. ed. Belo Horizonte: UFMG, 2007. 255 p.

GISEL, Laurent. *O Direito de Guerra impõe limites aos ataques cibernéticos também*. Entrevista ao Comitê Internacional da Cruz Vermelha. 2013. Disponível em: <http://www.icrc.org/por/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm>. Acesso em: 18 jul. 2016.

GROTIUS, Hugo. *O Direito da Guerra e* da Paz (1625). Tradução de Ciro Mioranza. 2 ed. Florianópolis: Unijuí, 2004. 768 p.

INTERNATIONAL COMMITTEE OF THE RED CROSS – ICRC. *International Humanitarian Law* - Treaties & Documents: Instructions for the Government of Armies of the United States in the Field (Lieber Code). Geneva, 2005. Disponível em: <http://www.icrc.org/ihl.nsf/FULL/110?OpenDocument>. Acesso em: 21 jun. 2016.

INTERNATIONAL COURT OF JUSTICE – CIJ. *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States Of America)*. Mérito, 1986, §§ 191 e 195. Disponível em: <http://www.icj-cij.org/docket/ files/70/6503.pdf>. Acesso em: 18 jun. 2016.

KOH, Harold Hongju. *International Law in Cyberspace*. Harvard International Law Journal, 2012. Disponível em: <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858 &context=fss_papers>. Acesso em: 13 jul. 2016.

KRIEGER, César Amorim. *Direito Internacional Humanitário – Vol.10*. 4ª reimpressão. Curitiba: Juruá, 2009. 351 p.

MÄLKSOO Lauri. *The Tallinn Manual as an international event*, Diplomaatia, nº 120, Book Review, 2013. Disponível em: <http://www.diplomaatia.ee/en/article/the-tallinn-manual-as-an-international-event/>. Acesso em: 16 jul. 2016.

MANDARINO JUNIOR, Raphael. *Tendências globais em segurança e defesa cibernética*. In: BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de. (Org.). Desafios Estratégicos para a Segurança e Defesa Cibernética. 1 ed. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. p. 13-34.

MELLO, Celso Duvivier de Albuquerque. *Direitos Humanos e Conflitos Armados*. Rio de Janeiro: Renovar, 1997. 500 p.

MELZER, Nils. *Cyberwarfare and International Law*. United Nations Institute for Disarmament Research (UNIDIR), 2011. Disponível em: <http://unidir.org/files/ publications/pdfs/cyberwarfare-and-international-law-382.pdf>. Acesso em: 12 jul. 2016.

NYE JUNIOR, Joseph S. *The Future of Power*. 1 ed. New York: Public Affairs, 2011. 300 p.

OLIVEIRA, João Roberto de. *Sistema de Segurança e Defesa Cibernética Nacional: abordagem com foco nas atividades relacionadas à Defesa Nacional*. In: BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de. (Org.). Desafios Estratégicos para a Segurança e Defesa Cibernética. 1 ed. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. p. 105-128.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *Carta das Nações Unidas e Estatuto da Corte Internacional de Justiça*. Centro de Informação das Nações Unidas - UNIC Rio, 06 jul. 2001. Disponível em: <http://unicrio.org.br/img/CartadaONU_VersoInternet.pdf>. Acesso em: 16 jul. 2016

PAGANINI, Pierluigi. *The Rise of Cyber Weapons and Relative Impact on Cyberspace. Elmwood* Park: INFOSEC Institute, 2012. Disponível em: <http:// resources. infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/>. Acesso em: 12 jul. 2016.

PECEQUILO, Cristina Soreanu. *Política Internacional*. 2 ed. Brasília: Fundação Alexandre de Gusmão, 2012. 354 p.

SENDOV, Blagovest. *Entrando na era da informação*. Academia Búlgara de Ciências. Estudos avançados, v. 8, n. 20. São Paulo, 1994. Disponível em: <http://www.scielo.br/scielo. php?script=sci_arttext&pid=S0103-40141994000100008>. Acesso em: 04 ago. 2016.

SILVA, Júlio Cezar Barreto Leite da. *Guerra Cibernética: A guerra no quinto domínio, conceituação e princípios.* Revista da Escola de Guerra Naval. v.20, n. 1, 2014. p. 193-211.

SWINARSKI, Christophe. *Introdução ao Direito Internacional Humanitário*. Brasília: Comitê Internacional da Cruz Vermelha e Instituto Interamericano de Direitos Humanos, 1993. 74p.LINZ, WOLNEY. Direito Internacional Humanitário. Disponível em: <https://www.wlneylinz.com/watchv=lKysSpW5Ccg>. Acesso em: 15 jun.2016.

VENTRE, D. Daniel. *Ciberguerra*. In: XIX Curso Internacional de Defensa. (Org.). Seguridad global y potencias emergentes en un mundo multipolar. 1 ed. Espanha: Academia General Militar – Universidad de Zaragoza e Ministerio de Defensa, 2012. p. 31-46.

WIENER, Norbert. *Cibernética e Sociedade: o uso humano de seres humanos* (1954). Tradução de José Paulo Paes. 4. ed. São Paulo: Cultrix, 1973. 192 p.