O AMBIENTE CIBERNÉTICO E O DIREITO INTERNACIONAL DOS CONFLITOS ARMADOS: UMA PROPOSTA DE ADEQUAÇÃO DOUTRINÁRIA

Capitão Rafael Siqueira Marques

O autor agradece a orientação do Coronel Júlio César de Sales

O Capitão de Cavalaria Rafael Marques é Comandante de Esquadrão no 16º Regimento de Cavalaria Mecanizado (16º R C Mec). Foi declarado aspirante a oficial em 2007 pela Academia Militar das Agulhas Negras (AMAN). É Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) e Pós-graduado em Relações Internacionais pela Universidade de Brasília (UnB). Possui estágios nas áreas de Tecnologia da Informação e de Cibernética. Participou da Missão das Nações Unidas para a Estabilização no Haiti (*MINUSTAH*), em 2011 (rafael.cav@hotmail.com).

A forma como os conflitos armados vêm ocorrendo no mundo está em constante evolução. Nos últimos anos, as operações cibernéticas têm-se destacado pela potencialidade de se tornar uma das maiores vertentes de assimetria a ser inserida no rol das capacidades militares. Dentre as ferramentas passíveis de utilização em combate, as ações cibernéticas ganharam espaço na mídia em decorrência de sua potencialidade lesiva.

Em contrapartida, os Estados vêm priorizando o estabelecimento de normas e de procedimentos que visem a assegurar a legitimidade das ações militares realizadas nos conflitos modernos. Foi nesse contexto que, historicamente, surgiu o Direito Internacional dos Conflitos Armados (DICA) como um conjunto de normas destinadas a proteger certas pessoas e intalações que, direta ou indiretamente, encontram-se em áreas de conflito.

No amplo espectro dos conflitos, a inter-relação entre o DICA e o uso militar das operações de defesa cibernéticas tem justificado o desenvolvimento desse setor estratégico no Brasil. A contemporaneidade do tema e a escassez de manuais são fatores que evidenciam a necessidade de atualização da doutrina militar relacionada ao assunto.

O potencial danoso dos ataques cibernéticos, aliado à lacuna legislativa existente, dificulta a realização de operações de defesa cibernética, seja para resguardar o país de atacantes externos, seja para amparar as operações militares desencadeadas em resposta a ataques.

Nas publicações doutrinárias finalizadas no âmbito das Forças Armadas Brasileiras, tem sido cada vez mais frequente o estabelecimento de normas e de procedimentos visando obter o maior grau de legitimidade para o uso da força, favorecendo, em decorrência, melhores condições para a manutenção de uma narrativa dominante em um eventual conflito.

Nesse sentido, é possível verificar que a Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END) coadunam-se com os princípios constitucionais de respeito aos tratados internacionais dos quais o Brasil é signatário. No plano político-estratégico, esses dois importantes documentos inseriram o país no ambiente das demais nações, ressaltando a importância do desenvolvimento do setor cibernético internamente (BRASIL, 2012).

No Brasil, a militarização do tema cibernética vem se desenvolvendo de forma semelhante ao que ocorre em outros países. Neste ínterim, a END deixou clara a importância do tema ao incluí-lo dentre os setores considerados estratégicos e que demandam estudos aprofundados.

Esse documento elencou três setores estratégicos: o aeroespacial, o nuclear e o cibernético, ressaltando a necessidade

urgente de expansão desses setores e estabeleceu, para o Exército Brasileiro, responsabilidade pelo desenvolvimento do setor de defesa cibernética dentro do território nacional (BRASIL, 2012).

Tal direcionamento evidenciou a necessidade de realização de estudos com o intuito de estabelecer normas e procedimentos para adequar as capacidades de defesa do país ao cenário internacional. As possíveis inter-relações atuais, tais como a possibilidade de aplicação do Direito Internacional Humanitário (DIH) e do DICA aos conflitos assimétricos contemporâneos, são exemplos recentes da constante mutação que o ambiente operacional moderno vem sofrendo.

Os incrementos tecnológicos desenvolvidos no século XXI, especialmente os do campo da cibernética, acrescidos dos conceitos de guerra assimétrica e dos confrontos de quarta geração, são os pilares do que estudiosos denominaram de conflitos de quinta geração. Nesse contexto, a revolução tecnológica recentemente desenvolvida no mundo apresenta-se como uma das principais características dos conflitos de quinta geração, tendendo a ocasionar profundas modificações nas batalhas, empregando novas e modernas capacidades militares. Além disso, a inclusão do espaço cibernético como um possível teatro de operações, a utilização de biotecnologia e de nanotecnologia nos combates poderão acarretar mudanças significativas na forma como os conflitos armados acontecem.

Logo, parece bastante lógico supor que o potencial danoso de certos tipos de ataques cibernéticos poderá se sobrepor aos danos causados por um bombardeio convencional com fogos cinéticos, por exemplo. Dessa forma, um ataque cibernético realizado contra infraestruturas críticas de um país, como as de energia e de telecomunicações, por exemplo, poderá resultar em maiores danos para conquista de um objetivo militar do que um ataque com tropas regulares.

Historicamente, avanços tecnológicos aliados às constantes transformações do cenário mundial suscitam debates sobre os limites da guerra e da utilização da tecnologia como ferramenta de combate militar, já que os setores bélicos e tecnológicos se complementam de forma cíclica.

A ausência de respostas claras para os diversos questionamentos sobre esses limites da guerra pode ser exemplificada pelo seguinte cenário hipotético. Em uma região em litígio, na qual existe um conflito armado, há um indivíduo sentado em frente a um computador em sua residência. Esse indivíduo realiza a invasão a um sistema de segurança e sobrecarrega ou danifica toda uma rede de energia ou de comunicações da parte oponente. Tal indivíduo poderia ser considerado um combatente à luz do DICA? Seria justificável uma resposta militar, caso o atacante seja um ator estatal? Que limites existem para a restrição do dano possível de ser causado por esse tipo de ataque? E se as ações causarem prejuízos a instalações protegidas pelo Direito Internacional Humanitário como, por exemplo, hospitais?

O potencial danoso dos ataques cibernéticos, aliado à lacuna legislativa existente, dificulta a realização de operações de defesa cibernética, seja para resguardar o país de atacantes externos, seja para amparar as operações militares desencadeadas em resposta a ataques.

O emprego militar de determinadas tecnologias exemplificam as mudanças historicamente ocorridas na sociedade. O advento de elementos inseridos no rol das capacidades militares, como a pólvora, a automatização industrial de armamentos e o desenvolvimento de artefatos nucleares, ocasionou mudanças profundas nas doutrinas de combate e na forma de combater. Tais inserções motivaram grandes transformações, tanto nos campos de batalha quanto no próprio regime jurídico internacional, devido às suas potencialidades lesivas.

Atualmente, a doutrina militar vigente vem sendo adaptada à luz do DICA com a finalidade de legitimar as ações desenvolvidas, sobretudo no espaço onde os temas de cibernética e as normas de direito se relacionam. Essa adaptação tem possibilitado, em alguns países, a realização de operações armadas destinadas a coibir ações executadas em ambientes cibernéticos, como parte do teatro de operações dos conflitos assimétricos. Nesse contexto, faz-se necessário analisar a aplicabilidade do DICA sobre a doutrina de defesa cibernética praticada internamente, com o intuito de promover a adequação de procedimentos e/ou de manuais doutrinários, para manter a legitimidade das ações militares realizadas nesse tipo de ambiente.

Compreender o papel das ações cibernéticas e o da securitização desse setor no mundo é mais que um objetivo, trata-se de uma necessidade. A implementação doutrinária em curso, iniciada pela END, que impôs ao Exército a responsabilidade pelo desenvolvimento da defesa cibernética no Brasil, deve ser tratada com a devida importância demandada pelo setor.

Descrever as possibilidades do emprego da cibernética como ferramenta para a consecução de objetivos militares, assim como verificar o potencial danoso que essa ferramenta possui, é mais que uma obrigação e uma necessidade. Compreender os meandros do DICA em face dos conflitos assimétricos, enfatizando a proteção de infraestruturas críticas, a proteção de civis e as restrições à utilização de determinados armamentos, caracteriza-se como a principal demanda dos conflitos contemporâneos, pois, sem legitimidade, dificilmente haverá o controle da narrativa dominante em um conflito.

Nesse contexto, existe uma necessidade de atualização da doutrina militar vigente para legitimar o emprego de operações de defesa cibernética, adequando os aspectos peculiares dessas operações às possíveis correlações com os princípios do DICA. Essa adequação proporcionaria a melhor aplicação dos princípios desse ramo do direito às operações e, ainda, possibilitaria a evolução da doutrina militar vigente aplicada aos conflitos armados. Além disso, poderá contribuir na manutenção do alinhamento das publicações doutrinárias do país ao atual panorama internacional dos conflitos armados.

A SECURITIZAÇÃO DA CIBERNÉTICA E SEU POTENCIAL DANOSO

O amplo espectro dos conflitos contempla diversos fatores de assimetria. Atualmente, a possibilidade de emprego militar da cibernética é considerada uma da principais vertentes em curso no mundo. A prevalência de conflitos assimétricos, incrementados com recursos tecnológicos, e o emprego de capacidades militares no ambiente cibernético têm sido comuns em alguns conflitos contemporâneos.

Hammes (2007) apontou as ferramentas de tecnologia da informação como um dos principais vetores de modificação de ações no campo de batalha. Carr (2011) demonstrou ser factível o rápido processo de militarização do setor cibernético em diversos países. Nesse sentido, dentre as cinco formas de assimetria de conflito (tecnológica, doutrinária, normativa, de participantes e moral/ética), a assimetria tecnológica é uma das mais impactantes em termos de desequilíbrio de poder.

Os efeitos de certos tipos de ataques cibernéticos podem ser comparados aos de bombardeios estratégicos. Esses tipos de ataques podem possibilitar que países de pequena expressão no campo militar confrontem grandes potências mundiais, como se observa no caso em que a Coreia do Norte foi acusada de realizar ataques cibernéticos contra os Estados Unidos da América.

O processo de securitização da defesa cibernética no Brasil teve início no ano de 2012. A criação do Centro de Defesa Cibernética (CDCiber) foi o marco inicial para o desenvolvimento interno desse setor. Ao se comparar a data de expedição da política de defesa cibernética nacional com algumas normas doutrinárias internacionais sobre o assunto, é possível verificar que o desenvolvimento do setor cibernético no mundo é um processo bastante recente.

O Brasil, assim como a maioria dos outros países que estabeleceram suas estruturas de defesa cibernética, também o fez há poucos anos. Boa parte deles iniciou o planejamento de suas defesas cibernéticas após o ataque contra Estônia, empreendido pela Rússia, em 2007. Esse evento foi tão marcante que ficou conhecido como Primeira *Web* Guerra, caracterizando-se como um dos principais pontos de inflexão no desenvolvimento da defesa cibernética no mundo.

Uma das primeiras definições de ações cibernéticas em documentos oficiais do governo brasileiro, no ano de 2009, estabeleceu que por ações cibernéticas entendem-se todas aquelas ações realizadas com uso de TIC [1] para "[...] interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado [...]" (GSI/PR, 2009).

Na mesma direção, Nye (2012) afirmou que uma guerra cibernética é aquela na qual as ações hostis, realizadas no ciberespaço, causam efeitos ou são equivalentes à violência física de grandes proporções no espaço real.

Essas definições, além de mostrar de forma inconteste a capacidade bélica proporcionada pela utilização do ciberespaço, estabelecem condições e procedimentos para a realização de ações militares nesse ambiente operacional, uma vez que os ataques implementados podem ocasionar danos físicos e virtuais em objetivos táticos e estratégicos localizados no mundo real.

Principais ataques cibernéticos envolvendo Estados (últimos 20 anos)

Ano	Atacante	Atacado	Características
1999	Sérvia	Kosovo	Ataques mútuos para inviabilização dos sistemas de informação do lado oponente (possível participação de China e Estados Unidos) durante a guerra do Kosovo.
2007	Rússia	Estônia	Retaliação russa contra um protesto que ocorria na Estônia. Houve uso massivo de ataque do tipo DoS que derrubou os sistemas informatizados do governo estoniano como um todo (*Web-War I*).
2007	Israel	Síria	Ataque contra os sistemas de defesa aérea sírios. Fez os radares ignorarem os caças israelenses que não tiveram dificuldades para bombardear, com eficácia, as defesas sírias.
2008	Rússia	Geórgia	Antes do avanço das tropas, os russos executaram ataques de negação de serviço (DoS) para preparar o terreno, desabilitando as ferramentas de comando e controle do oponente.
2009	China	EUA	Americanos alegam ataque sofrido contra o banco de dados de projetos do Departamento de Defesa. Pouco tempo depois, a China passou a fabricar caças semelhantes ao modelo do projeto americano.
2010	-	Irã	Um ataque sobrecarregou e danificou o sistema de centrífugas da infraestrutura nuclear iraniana. A autoria não foi assumida, mas EUA e ISRAEL foram especulados como possíveis autores.
2015	-	Turquia	Após a Turquia declarar apoio a um grupo acusado de financiar o terrorismo, o grupo de ciberativismo [2], *Anonymous*, executou ataque do tipo DoS e derrubou os domínios do governo e das forças armadas turcas.
2016 - 2017	EUA	-	Ataques cibernéticos realizados na Síria e no Iraque para evitar o funcionamento de estruturas de comando e controle do grupo terrorista Estado Islâmico.

Os ataques cibernéticos realizados nos últimos anos deixaram claro que esses tipos de ações, normalmente, visam infraestruturas críticas [2] e/ou serviços essenciais à população. O Gabinete de Segurança Institucional da Presidência da República, em publicação de 2012, afirmou que os ataques cibernéticos normalmente têm como objetivos principais a inviabilização de serviços essenciais à sociedade.

Nesse contexto, o Brasil decidiu desenvolver o setor estratégico da defesa cibernética, elencando-o na estratégia nacional de defesa e iniciando o processo de criação e/ou atualização da doutrina relativa ao tema. A alocação de recursos e a disponibilização das estruturas necessárias para o funcionamento desse setor impulsionaram o seu desenvolvimento no país (BRASIL, 2012a).

Até o ano de 2016, o CDCiber era a única organização militar destinada exclusivamente à temática da defesa cibernética no Brasil. Atualmente, o Comando de Defesa Cibernética (ComDCiber) funciona como o órgão central de defesa cibernética no país. Essa organização militar agrega militares da Marinha, do Exército e da Força Aérea nas mesmas instalações, promovendo a integração entre as Forças, uma vez que possibilita a nomeação de militares de Forças Singulares para exercerem funções em uma organização militar enquadrada no organograma do EB.

Em que pese o avanço técnico e estrutural que a defesa cibernética brasileira vem sofrendo ultimamente, o setor merece um constante aprimoramento doutrinário. Atento a essa necessidade, o Ministério da Defesa publicou o manual Doutrina Militar de Defesa Cibernética (MD31-M-07), que coincidiu com uma série de publicações de manuais realizadas pelo EB, no contexto do processo de atualização e transformação da doutrina militar terrestre.

Dentre os manuais revisados e reestruturados pelo EB no ano de 2014, destacam-se dois que possuem *status* de manual de fundamentos (EB20-MF.10.102) e (EB20-MF.10.103). Ambas as publicações desenvolvem seus capítulos com características em comum, sendo perceptível a prevalência das "considerações civis" como aspectos essenciais a serem considerados para o emprego de força militar em qualquer cenário.

Nessa perspectiva, a guerra cibernética foi elencada como um dos principais elementos de apoio ao combate, em decorrência da

sua capacidade de ampliar a eficiência dos elementos de manobra (BRASIL, 2014b).

AS AÇÕES CIBERNÉTICAS À LUZ DO DIREITO INTERNACIONAL DOS CONFLITOS ARMADOS

Conforme estabelecido na literatura mais recente, para que uma ação possa ser analisada perante as normas do DICA, ela deve ocorrer no contexto de um conflito armado internacional (CAI) ou de um conflito armado não internacional (CANI). Deve, ainda, existir uma "intensidade mínima" das ações praticadas nesse conflito.

A possibilidade de enquadramento de uma ação cibernética nas normas do DICA é inconteste quando a contenda envolve dois ou mais Estados em um CAI e desde que as partes empreguem, no conflito, pessoal militar ou estruturas destinadas às operações cibernéticas. Todavia, no contexto de um CANI, o enquadramento das ações cibernéticas precisa ser melhor discutido, uma vez que, por definição sumária, o CANI é o conflito ocorrido quando uma das partes é um Estado e a outra não, devendo essa segunda parte possuir requisitos específicos de organização. A condição militar regular dos envolvidos ou mesmo o tipo de ações cibernéticas realizadas são caraterísticas imprescindíveis para o enquadramento das ações no DICA.

Melzer (2011) observou que, nos conflitos nos quais um indivíduo atue isoladamente contra um Estado, não há a organização necessária para a configuração de CANI, uma vez que lhe falta o requisito da estrutura interna hierarquizada. Em contrapartida, Biazatti (2015) destacou a decisão do Tribunal Penal Internacional, expedida em 2005, na qual ficou estabelecido que o critério de organização do grupo jamais pode ser utilizado como barreira para impedir a proteção às vítimas.

Nesse contexto, bastaria um "pouco de organização" de um grupo para configurar a existência de um conflito armado não internacional, ou seja, um grupo organizado que empreenda ações cibernéticas danosas no contexto de um conflito interno, poderia, sim, ter suas ações avaliadas à luz do DICA.

Em relação à intensidade mínima das ações, outro requisito necessário para o enquadramento de uma ação no DICA, as potencialidades lesivas das ações cibernéticas, assim como os impactos provocados nas infraestruturas críticas ou nos serviços essenciais, seriam suficientes para evidenciar a capacidade militar danosa que tal ferramenta possui. Isso, por si só, justifica a análise dessas ações no DICA.

Uma pesquisa de cunho qualitativo com abordagem descritiva, realizada no âmbito do EB, evidenciou a possibilidade de equiparação dos possíveis efeitos oriundos dos ataques cibernéticos aos dos ataques cinéticos. Essa pesquisa foi aplicada a grupos amostrais específicos, compostos por especialistas das diferentes áreas correlatas, tais como operadores de guerra cibernética e especialistas em Direito Internacional Humanitário.

As percepções colhidas dentro de cada grupo amostral foram bastante significativas e evidenciaram o potencial lesivo que as ações cibernéticas possuem. Essas opiniões foram colhidas com base em situações hipotéticas e em conflitos que envolveram, em sua plenitude, ações cibernéticas. Foram apresentadas situações que faziam referências a histórico de ataques cibernéticos reais e a estudos de casos esquemáticos, similares aos modelos utilizados pelo *International Institute of Humanitarian Law (IIHL*, na sigla em inglês).

Ao serem indagados sobre qual seria a resposta adequada contra um ataque cibernético que ocasionasse sérios danos ao sistema de comando e controle de um país e que causasse baixas pela perda de consciência situacional, 64,51% dos participantes indicaram uma ação cinética, com o uso da força, como resposta adequada, enquanto que 51,61% apontaram uma combinação de ações cinéticas e não cinéticas (defesa cibernética) como resposta indicada contra esses atacantes.

Ou seja, o esforço despendido pela Organização do Tratado do Atlântico Norte - OTAN durante a elaboração do Manual de *Tallinn*, no sentido de aplicar o DICA dos conflitos cinéticos aos conflitos cibernéticos, não foi totalmente despropositado. Essa medida tinha também como objetivo respaldar os conceitos preconizados pela doutrina norte-americana, a

qual prevê o emprego de respostas cinéticas (com o uso da força) contra ameaças cibernéticas, tal como a Rússia o faz.

Evidenciada a capacidade dos conflitos do tipo CAI ou CANI possuírem os requisitos da intensidade mínima e da permeabilidade dos ataques cibernéticos, ficou claro que as operações cibernéticas possuem todos os pré-requisitos necessários para serem apreciadas com base nas normas do DICA.

Dessa forma, é possível correlacionar a potencialidade danosa e o alcance das ações cibernéticas com os princípios desse ramo do direito, verificando a coerência entre eles. Essa correlação é importante, pois garante a legitimidade para a realização de operações de defesa cibernética, uma vez que ficará demonstrada a possibilidade de enquadramento dessa ações no DICA.

Antes disso, é válido relembrar alguns pontos das Convenções de Genebra e seus protocolos adicionais. O Protocolo Adicional I, em seu art. 57, estabelece que todas as operações militares devem ser conduzidas de forma a poupar as pessoas e os bens de caráter civil (CICV, 1998). Certamente, isso não implica a proibição do uso das ferramentas cibernéticas como capacidades militares. Nenhum país, até os dias de hoje, clamou junto à Organização das Nações Unidas ou outro fórum multilateral pela proibição desse tipo de ataque.

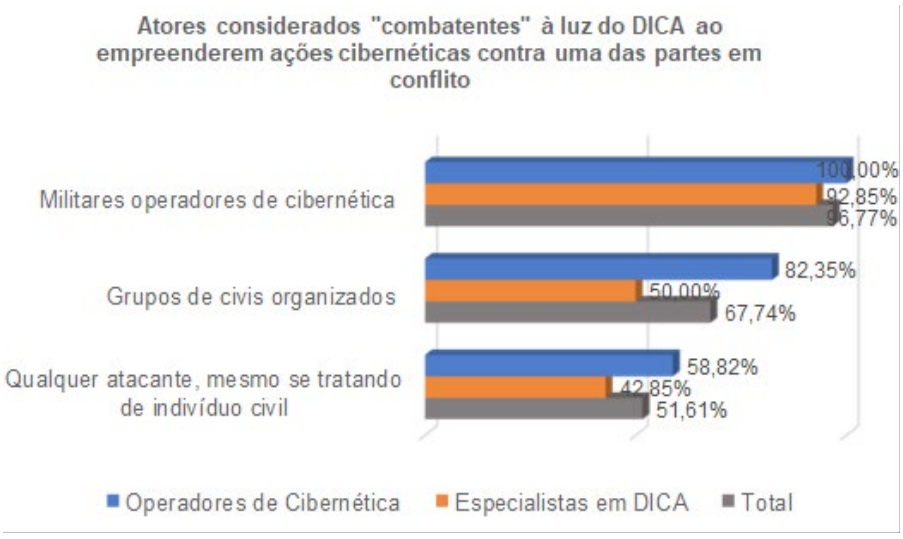
O texto citado apenas destaca que o uso da cibernética como ferramenta militar ou, mesmo, a utilização de qualquer outra tecnologia que venha a surgir, deverá se adaptar aos parâmetros previamente estabelecidos nas Convenções de Genebra, sempre atendendo aos princípios básicos do DICA: distinção, limitação, proporcionalidade, necessidade militar e humanidade.

Em um primeiro momento, os princípios da limitação e da necessidade militar merecem destaque, pois é a partir deles que se pode identificar a extensão do dano que uma ação militar pode gerar. Esses princípios estabelecem que os meios militares capazes de causar danos desnecessários, seja para o pessoal, seja para as instalações, não devem ser utilizados.

Em outras palavras, ações cibernéticas em contendas militares somente seriam permitidas caso fosse possível assegurar o alcance dos danos ocasionados por elas. A solução de tal problemática é fundamental para a percepção da permeabilidade do DICA sobre as operações cibernéticas e para a adequabilidade da doutrina militar vigente às novas demandas.

Outro princípio que merece destaque na inter-relação com as ações cibernéticas é o da distinção. Trata-se de princípio imprescindível para individualizar os envolvidos nos conflitos, separando os que possuem e os que não possuem o *status* de combatente à luz do DICA. Tal princípio é fundamental, pois congrega uma série de normas de deveres e de direitos do pessoal localizado na área de conflito.

Em uma operação cibernética realizada no contexto de um conflito militar, os operadores militares de guerra cibernética podem ser claramente enquadrados como combatentes, uma vez que "[...] os membros das Forças Armadas de uma parte envolvida no conflito, os membros das milícias e os membros dos corpos de voluntários que fizerem parte dessas Forças Armadas [...] são considerados combatentes à luz do sistema legal vigente" (BRASIL, 2011).



Percepção sobre o status de "combatente" para os diversos atores

Foi possível observar durante o estudo, que além da atuação de forças militares no ambiente cibernético, existiam também casos de grupos de civis que participaram de ataques cibernéticos e obtiveram resultados efetivos contra Estados e/ou contra forças militares. Nesses casos, o DICA não previu a possibilidade de intervenção de um atuador que não estivesse fisicamente presente no combate e sem pegar em armas. Ficou obscura, na definição estabelecida, a possibilidade de enquadramento no DICA desses grupos, por analogia.

Entretanto, o Protocolo Adicional I das Convenções de Genebra definiu que apenas aos combatentes é legítimo participar diretamente das hostilidades. Um ataque cibernético pode desencadear vantagens militares táticas e estratégicas e, ainda, ser fonte de hostilidades. Sendo assim, fica evidente que grupos civis podem participar de conflitos empreendendo ataques cibernéticos. Isso torna contraditório o conceito de não combatente estabelecido no documento.

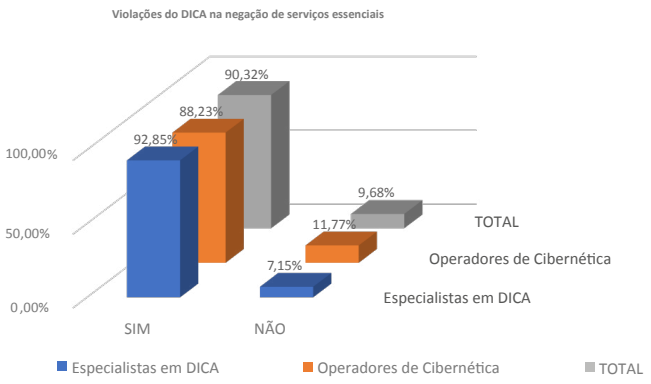
Na prática, até mesmo um único indivíduo civil, que faça uso de um meio cibernético para realizar ou participar de um ataque no contexto de um conflito armado perde a proteção que os civis gozam nos conflitos, ficando passível de represálias. Segundo o Comitê Internacional da Cruz Vermelha, quando um civil participa diretamente das hostilidades, ele perde o direito de não ser um alvo militar (CICV, 1998).

Ainda pelo princípio básico da distinção, os objetivos militares devem ser diferenciados dos de caráter civil. Uma situação didática que melhor exemplificaria tal princípio seria a realização de ataques cibernéticos contra um sistema de controle de tráfego aéreo que ocasionem acidentes e perda de vidas na aviação civil. Esses ataques, além de ilegítimos, seriam contrários aos princípios do DICA. Entretanto, no caso de o mesmo tipo de ataque ser empreendido contra o sistema de comando e controle do espaço aéreo de uma força militar, seria legítimo mesmo que provocasse baixas militares.

Na visão de especialistas em DICA e de operadores de cibernética, ficou evidente que as ações que provoquem danos em serviços essenciais ou em infraestruturas críticas para a sociedade violam os princípios do DICA, podendo ser julgadas à luz desse ramo do direito, mesmo quando desencadeadas por indivíduos civis.

Em se tratando do princípio da humanidade, tem-se que ele veda a imposição de sofrimento desnecessário às pessoas com o intuito de obrigar o inimigo a se render. Por meio desse princípio, é possível traçar uma relação dos efeitos danosos e da possibilidade de alcance das ações cibernéticas. O caso de uma ação militar realizada durante a Guerra do Golfo é um exemplo claro da potencialidade lesiva desse tipo de operação. O ataque em questão, o qual foi desencadeado por forças norte-americanas, deixou vários hospitais sem energia elétrica, o que resultou em baixas pela falha de equipamentos médicos de suporte à vida.

Nesse sentido, no caso de a interrupção no fornecimento de energia advir de um ataque cibernético, haveria uma violação ao princípio da humanidade e da proteção de civis e enfermos.



Percepção sobre violações do DICA em negação de serviços essenciais.

A ADEQUAÇÃO DA DOUTRINA MILITAR DE DEFESA CIBERNÉTICA AO DICA

Enquanto as publicações do EB, em suas revisões e atualizações realizadas no ano de 2014, trataram do processo de transformação doutrinária, o Manual de Doutrina Militar de Defesa Cibernética (MD31M-07), publicado pelo MD, ateve-se às questões específicas do uso militar do ambiente cibernético.

Por se tratar de um novo setor e uma nova doutrina, o MD31-M-07 não abarcou toda a gama de possibilidades da cibernética em decorrência da complexidade temática inerente a essa atividade.

Ciente da necessidade de atualização permanente do MD31-M-07 - a primeira edição de uma doutrina militar desse tipo no Brasil - o próprio MD previu um ciclo constante de atualização desse manual, estabelecendo que uma primeira atualização fosse realizada ainda durante o ano de 2017.

Esse manual elencou a possibilidade de se atingir infraestruturas críticas de um oponente sem, contudo, possuir alcance físico ou mesmo expor tropas (BRASIL, 2014d, p. 22).

Estabeleceu, ainda, que a incerteza, uma das características dos ataques cibernéticos, caracteriza-se pela impossibilidade de se estipular com precisão o alcance e os efeitos desejados em uma ação desse tipo, devido ao complexo número de variáveis presentes nos sistemas informatizados (BRASIL, 2014d, p. 21).

Trata-se de definição extremamente simplificada na qual o manual deixou de detalhar, em melhores condições, os alcances adequados e os limites desejados para a realização das ações de defesa cibernética.

Já o manual Operações de Informação (EB-20-MC-10.213), trata do planejamento e do emprego das operações cibernéticas passíveis de serem conduzidas pela Força Terrestre (F Ter) no contexto das operações de amplo espectro. Esse manual define as ações de guerra cibernética como sendo "ações (exploração, ataque e proteção) que empregam recursos do espaço cibernético, com o objetivo de: proteger ativos de informação; explorar e atacar redes do oponente, mantendo a capacidade de interferir no desenrolar das operações militares no espaço de batalha; ou afetar as condições de normalidade em uma determinada área ou região, atingindo gravemente o funcionamento de estruturas estratégicas e serviços essenciais destinados à população (BRASIL, 2014a, p. 4-8).

O Manual de Emprego do Direito Internacional dos Conflitos Armados (DICA) nas Forças Armadas (MD-34-M-03) preconizou a integração da doutrina e ratificou a necessidade da existência de coerência e de adequação da doutrina militar brasileira com o DICA. Estabeleceu, também, a necessidade de se permear a doutrina militar com os aspectos fundamentais desse ramo do direito, desde o nível estratégico até o tático, envolvendo os planejadores (no mais alto escalão de decisão) e os executores de maneira conjunta. Táticas, técnicas e procedimentos (individuais e coletivos) deverão estar alicerçados nos princípios do DICA de modo a garantir a execução eficiente das operações militares no âmbiente cibernético (BRASIL, 2011).

Compreender os meandros do DICA em face dos conflitos assimétricos, enfatizando a proteção de infraestruturas críticas, a proteção de civis e as restrições à utilização de determinados armamentos caracteriza-se como a principal demanda dos conflitos contemporâneos, pois sem legitimidade, dificilmente haverá o controle da narrativa dominante em um conflito.

A análise comparativa das publicações realizadas no âmbito das FFAA brasileiras tem evidenciado a necessidade de integração da doutrina militar no âmbito interno das Forças. Essa integração se faz necessária, especialmente, nos manuais de doutrina militar de defesa cibernética, no de operações de informação e no de emprego do DICA. Deve-se adequar continuamente esses dispositivos para proporcionar um entendimento constante da importância que o Brasil atribui à legitimidade das ações militares.

Esses dispositivos evidenciaram a tradição brasileira de respeito aos tratados de direitos humanos e ressaltaram que a adoção de medidas que visem a permitir a aplicação do DICA nos conflitos armados serão consideradas medidas preparatórias, de caráter essencial a serem desenvolvidas internamente em tempo de paz (BRASIL, 2011).

Existe a necessidade de atualização e/ou adequação das publicações nacionais no que se refere à correlação das ações cibernéticas e o DICA. Nessa atualização, devem ser estabelecidos parâmetros que possibilitem a aplicabilidade do DICA nas operações cibernéticas, uma vez que a legislação aplicada atualmente precisa ser mais efetiva frente aos desafios da inserção do ambiente cibernético no teatro de operações. Portanto, tornou-se imprescindível a incorporação do espaço cibernético como o quinto domínio operacional da guerra moderna.

Para a consecução desses objetivos, é necessário que se empreenda um esforço internacional conjunto no sentido de se promover maior entendimento e respeito aos princípios do DICA, conforme preconizado pelo MD-34-M-03, ao estabelecer que se deve permear a doutrina com os aspectos fundamentais inerentes a esse ramo do direito (BRASIL, 2011).

Outro grande desafio será assegurar a legitimidade das ações militares após a inserção do domínio cibernético no campo de batalha, devido à impossibilidade de se limitar o alcance e os efeitos desse tipo de ataque. Nesse contexto, as ações realizadas em ambientes cibernéticos deverão ser precedidas das mesmas precauções na aquisição e seleção de alvos, tal como ocorre com o uso de armamentos nas ações cinéticas.

A produção doutrinária brasileira passou a prever a utilização de recursos de defesa cibernética como atuadores não cinéticos. Essa permissão, porém, não incluiu o tema nos tratados de direito relacionados ao DICA que foram ratificados pelo Brasil. Todavia, não existiu anormalidade nessa omissão já que se tratava da primeira publicação de âmbito nacional relativa ao tema.

A incerteza do alcance e dos efeitos dos ataques desencadeados no ciberespaço demandam atenção especial dos militares operadores de cibernética, assim como dos chefes militares tomadores de decisão. A impossibilidade de mensurar e de assegurar a amplitude das consequências desse tipo de ação dificulta a criação de regulamentação, seja para resguardar a legitimidade das ações realizadas pelo EB, seja para identificar possíveis violações aos princípios do DICA.

A dificuldade de se calcular a extensão dos danos que podem ser causados pelas ações cibernéticas é o maior óbice para garantir a

legitimidade dessas ações junto às normas de direito. O fato de não se poder assegurar totalmente o alcance dos danos amplia a possibilidade de ocorrência de desrespeito aos princípios do DICA, sobretudo ao da distinção e ao da humanidade.

Da mesma forma, ações cibernéticas que comprometam o funcionamento de infraestruturas críticas que forneçam serviços essenciais à população, mas também, que possuam valor de objetivos militares, devem ser confrontadas pelos princípios da necessidade militar e da limitação de uso da força.

A proteção seletiva de pessoas e de instalações é norma cogente e amplamente respeitada no cenário internacional. Nessa vertente, o Brasil deve adaptar-se ao padrão adotado pelo regime internacional de uso militar do ambiente cibernético. O EB, a quem é atribuída a responsabilidade pelo desenvolvimento do setor cibernético brasileiro, não pode deixar de estudar a inter-relação entre o Direito Internacional Humanitário e as atividades do setor cibernético, analisando não só as limitações de uso, como também as prerrogativas de proteção passíveis de serem utilizadas nos casos de agressão externa.

CONSIDERAÇÕES FINAIS

O EB é o principal responsável pelo desenvolvimento do setor estratégico da defesa cibernética no Brasil. O MD31-M-07 (Doutrina Militar de Defesa Cibernética), apesar de recente, é uma publicação extremamente sintética que possui apenas 36 páginas, cabendo ao EB promover a adequação dessa norma às demandas atuais.

Naquele manual, os limites impostos às ações cibernéticas não ficaram totalmente claros podendo, inclusive, passar por ampliação por meio da inclusão de conceitos norteadores para garantir a legitimidade das ações perante o DICA. A hierarquia e os fundamentos doutrinários presentes nesse manual deverão balizar o desenvolvimento de novas diretrizes, assim como o emprego das ações cibernéticas.

Essa atualização/adequação seria extremamente importante para a orientação das futuras publicações atinentes às operações cibernéticas, uma vez que, dentro da hierarquia de publicações estabelecida pelo Centro de Doutrina do Exército, as do nível de doutrina militar precedem às de emprego operacional e tático, devendo a primeira orientar a elaboração das demais.

Dessa forma, a revisão da doutrina militar de defesa cibernética brasileira deverá diminuir a ocorrência de problemas legais que permeiam o emprego das tropas em operações militares. A realização de pesquisas para tornar os manuais doutrinários mais compatíveis com as normas vigentes no direito internacional deve ser um dos objetivos principais a serem explorados pela F Ter. Isso possibilitará a implementação de adequações nas futuras publicações relativas às operações cibernéticas no Brasil, tornando-as mais compatíveis com a doutrina difundida no cenário internacional, inspiradas pelo Manual de Tallinn, por exemplo.

Com a realização da atualização/adequação proposta, os principais pontos dos manuais MD31-M-07 Doutrina Militar de Defesa Cibernética e do EB20-MC-10.213 Operações de Informação abordados neste estudo, deverão ser esclarecidos, porém as características e os princípios da defesa cibernética, analisados com base nas normatizações do DICA, necessitam de estudos e de acompanhamentos constantes por se tratar de um tema extremamente complexo.

Atualmente, o aumento dos ataques cibernéticos realizados contra infraestruturas ou serviços essenciais à população corroboram com a necessidade dessa adequação. Devem ser incentivados, com prioridade em caráter de urgência, estudos que qualifiquem e quantifiquem as futuras decisões dos tribunais internacionais que possam vir a julgar danos decorrentes de ações cibernéticas. Tais estudos tornarão a legislação mais flexível e, ao mesmo tempo, poderão auxiliar na definição de limites de atuação para as tropas da Força Terrestre.

Em suma, o principal desafio a ser enfrentado pelos operadores de cibernética será o de assegurar a correta seleção de alvos no campo de batalha e a capacidade de mensurar os danos causados pelas operações, o que possibilitará a correta avaliação dos efeitos

das ações militares no ambiente cibernético, permitindo a inclusão dessa importante ferramenta nas operações militares.

De modo intrínseco, com a normalização dessas duas vertentes operacionais, grande parte da gama de leis atinentes ao DICA presentes no cenário nacional estaria sendo observada, corroborando com a tradição respeitosa e promulgadora atribuída ao Brasil, no que se refere ao Direito Internacional Humanitário. Extensivamente, as operações de defesa cibernética, realizadas pelos militares brasileiros, estariam totalmente respaldadas por uma legislação eficiente e devidamente adaptada às demandas mais recentes, visando assegurar a legitimidade das ações militares e favorecendo, assim, melhores condições para a obtenção de uma narrativa dominante.

REFERÊNCIAS

BRASIL. Exército. Estado-Maior. EB20-MC.10.213. Operações de Informação. Brasília, 2014a.

_____ EB20-MF.10.102. Doutrina Militar Terrestre. Brasília, 2014b.

BRASIL. Ministério da Defesa. Diretriz para a Difusão e Implementação do Direito Internacional dos Conflitos Armados (DICA) nas Forças Armadas. Portaria Normativa Nº 916/MD, de 13 de junho de 2008. Brasília, 2008.

_____. MD31-M-07 Doutrina Militar de Defesa Cibernética. Brasília, 2014d.

_____. MD33-M-02. Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas. Brasília, 2008a.

_____. MD-34-M-03. Manual de Emprego do Direito Internacional dos Conflitos Armados (DICA) nas Forças Armadas. Brasília, 2011.

_____. Política Cibernética de Defesa. Brasília, 2012.

_____. Política Nacional de Defesa e Estratégia Nacional de Defesa. Brasília, 2012a. 155 p.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Livro Verde: segurança cibernética no Brasil. Brasília, 2010.

BARROS, Otávio Santana Rêgo et al. Presidência da República. Secretaria de Assuntos Estratégicos. Desafios estratégicos para segurança e defesa cibernética. Brasília, 2011a.

BIAZATTI, Bruno de Oliveira. Ataques Cibernéticos e seus impactos na definição de conflitos armados não internacionais. In: Alethes - UFJF, v. 05, n. 09, pp. 257280, jul./dez., 2015.

BUZAN, Barry. WEAVER, Ole. WILDE, Jaap. Security: a new framework for analysis. Boulder and London: Lynne Rienner Publishers, 1998.

CARNEIRO, João Marinonio. A Guerra Cibernética: uma proposta de elementos para a formulação doutrinária do Exército Brasileiro. Tese de doutorado – Escola de Comando e Estado-Maior do Exército. Rio de Janeiro, 2012.

CARR, Jeffrey. Inside cyber warfare, 2ª ed. Sebastopol: O'Reilly Media, 2011.

CARVALHO, Paulo Sergio Melo de. A defesa cibernética e as infraestruturas críticas nacionais. 2011. Disponível em: <http://www.nee.cms.eb.mil.br/ attachments/article/101/cibernetica. pdf. Acesso em: 15 mar. de 2017.

CARVALHO, Regis de Souza de. Proposta de arquitetura para coleta de ataques cibernéticos às infraestruturas críticas. Dissertação (Mestrado) – Instituto Militar de Engenharia: Rio de Janeiro, 2014.

CINELLI, Carlos Frederico. Direito Internacional Humanitário: Ética e Legitimidade na aplicação da força em conflitos armados. Curitiba: JURUÁ, 2011.

CLARKE, Richard A; KNAKE, Robert K. Cyber War: The Next Threat to National Security and What To Do About It. Nova Iorque: HarperCollins, 290 p. 2010.

CLAUSEWITZ, Carl Von. Da guerra. São Paulo: Martins Fontes, 1996.

Comitê Internacional da Cruz Vermelha. Convenções de Genebra de 12 de agosto de 1949. Genebra: CICV, 1992.
_____. Protocolos Adicionais às Convenções de Genebra de 12 de agosto de 1949. Genebra: CICV, 1998.
_____. Violência e uso da força. Genebra: CICV, 2009.
CRUZ JÚNIOR, Samuel César da. A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual. Brasília: lPEA, 2013. 51 p.
CORDEIRO, Luís Eduardo. Análise da doutrina militar de defesa cibernética à luz do DIH/DICA. In: IX Encontro Nacional da Associação Brasileira de Estudos de Defesa. 2016. Florianópolis. Anais... Florianópolis: 2016.
Escola de Aperfeiçoamento de Oficiais. Apresentação de trabalhos acadêmicos e dissertações. 3. ed. Rio de Janeiro: Escola de Aperfeiçoamento de Oficiais, 2006. 108 p.
FRIEDMAN, Allan; SINGER, P. W. Cybersecurity and Cyberwar: what everyone needs to know. Oxford University Press. UK. 2014
HAMMES, T. X. A guerra de quarta geração evolui, a quinta emerge. Military Review. ed. brasileira. p. 16-27, set./out., 2007.
JOHNSON, Robert A. Prevendo a guerra do futuro. Doutrina Militar Terrestre em Revista, Brasília, p. 68-82, ed. 006, 2014.
LIANG, Qiao; XIANGSUI, Liang. Unrestricted Warfare. Beijing, 1999. Disponível em: https://www.egn.mar.mil.br/arquivos/cepe/guerraalemlimites.pdf. Acesso em: 16 maio 2016.
LOBATO, Luísa Cruz; KENKEL, Kai Michael. (2015). Discourses of cyberspace securitization in Brazil and in the United States. Revista Brasileira de Política Internacional, 58(2), 23-43.
LOPES, Gill. Reflexos da digitalização da guerra na política internacional do século XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá. 2013. Dissertação de Mestrado – Curso de Ciência Política, UFPE, Recife.
LOPES, Gill. Securitizando o Ciberespaço. In: ENCONTRO NACIONAL DA
Associação Brasileira de Relações Internacionais, 4. 2013, Belo Horizonte. Anais. Belo Horizonte: 2013.
NEVES, Eduardo; CLAYTON, Amaral (org). Manual de metodologia da pesquisa científica. Rio de Janeiro: EB/CEP, 2007. 204 p.
MARQUES, Helvétius da Silva. Direito Internacional Humanitário: limites da guerra. Rio de Janeiro: Esplanada, 2004.
MELZER, Nils. Cyberwarfare and international law. Geneva: United Nations Institute for Disarmament Research Resources, 2011.
MESSARI, N.; NOGUEIRA, J. Teoria das Relações Internacionais: Correntes e Debates. Rio de Janeiro: Elsevier, 2005.
MESSMER, E.. Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says. CNN, maio. 1999. Disponível em <www.edition.cnn.com>. Acesso em: 17 março 2017.
METZ, Steven. Strategic asymmetry. Military Review. Kansas: Fort Leavenworth. p. 23-31, jul./aug. 2001.
MEZZANOTTI, Gabriela. Direito, guerra e terror: os novos desafios do direito internacional pós 11 de setembro. São Paulo: Quartier Latin, 2007.
NASCIMENTO, Fransllyn S.S. Multidimensionalidade dos conflitos cibernéticos. Monografia – Universidade Federal de Roraima. Boa Vista, 2015.
NASCIMENTO, Otoniel Alves do. A Aplicação do Direito Internacional dos Conflitos Armados na Guerra de Quarta Geração. Trabalho de Conclusão de Curso - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2014.
NYE, Joseph S. Cyber Power. Cambridge: Belfer Center for Science and International Affairs at Harvard Kennedy School, 2010a.

_____. “Is Military Power Becoming Obsolete?”. Project Syndicate, Cambridge, 2010. Disponível em: <http://www.projectsyndicate.org/commentary/ nye78/English>. Acesso em: 3 de maio de 2016.
_____. Guerra e paz no ciberespaço. O Estado de S. Paulo, 15 de abril de 2012, internacional, p. A22. Disponível em: <http://www.estadao.com.br/noticias/ impresso,guerrae-paz--no-ciberespaco-,861242,0.htm>. Acesso em: 21 de junho de 2016.
_____. The Future of Power. New York: Public Affairs, 2011.
OLIVEIRA, Luis Henrique Almeida. Cyberwar: novas fronteiras da guerra. Monografia - Instituto de Ciência Política e Relações Internacionais. UNB, Brasília, 2011.
Organização do Tratado do Atlântico Norte (OTAN). Tallinn Manual on the International Law Applicable to Cyber Warfare. NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press, 2013.
PINHEIRO, Álvaro de Souza. O Conflito de 4ª Geração e a Evolução da Guerra Irregular. Coleção Meira Mattos: Revista das Ciências Militares. Rio de Janeiro, n. 16, 3. quadrim. 2007. Disponível em: <http://www.eceme.ensino.eb.br/ meiramattos/index.php/RMM/ article/view/258/227>. Acesso em: 9 de julho de 2016.
PINHEIRO, Fábio Ponte. A Cibernética como arma de combate. Trabalho de Conclusão de Curso - Escola Superior de Guerra, Rio de Janeiro, 2013.
PRADO FILHO, Hildo Vieira. A Transformação do Exército Brasileiro e o novo Sistema de Ciência, Tecnologia e Inovação do Exército: contribuições para a Soberania Nacional. Trabalho de Conclusão de Curso - Escola Superior de Guerra, Rio de Janeiro, 2014.
SWINARSKI, Christophe. Introdução ao estudo de direito internacional humanitário. Brasília: Comitê Internacional da Cruz Vermelha - Instituto Interamericano de Direito Humanos, 1996.
UNITED STATES. White House. International strategy for cyberspace: prosperity, security, and openness in a networked world. Washington, May 2011. Disponível em: http://www.whitehouse.gov/sites/default/fles/rss_viewer/interna-tioonal_ strategy_ for_cyberspace.pdf. Acesso em: 15 de abril de 2017.

NOTAS

[1] TIC ou tecnologias da informação e de comunicação correspondem a todos os artefatos tecnológicos que interferem e medeiam os processos informacionais e comunicativos dos seres. Ainda, podem ser entendidas como um conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de hardware, de software e de telecomunicações, a automação e a comunicação dos processos de negócios, da pesquisa científica e de ensino e aprendizagem.
[2] Ciberativismo é o conjunto de práticas utilizadas em defesa das mais diversas causas, seja ela política, socioambiental, sociotecnológica ou até mesmo cultural, mas que utilizam as redes cibernéticas como seu principal meio de difusão.