ESCOLA DE GUERRA NAVAL

CC ALESSANDRO DE PAULA LIMA

AÇÕES DE GUERRA CIBERNÉTICA NO CONFLITO RUSSO-GEORGIANO DE 2008:

uma análise à luz dos Princípios Fundamentais do Direito Internacional Humanitário

Rio de Janeiro

2019

CC ALESSANDRO DE PAULA LIMA

AÇÕES DE GUERRA CIBERNÉTICA NO CONFLITO RUSSO-GEORGIANO DE 2008:

uma análise à luz dos Princípios Fundamentais do Direito Internacional Humanitário

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

Orientador: CMG (FN-RM1) Wagner da S. Reis

Rio de Janeiro

Escola de Guerra Naval

2019

AGRADECIMENTOS

A Deus e à minha família, em especial minha esposa Lorena e meus filhos Luísa, Isadora e Felipe, torno público meu reconhecimento por serem o meu ponto de equilíbrio e fonte motivadora que impulsiona minha batalha diária em prol de minha realização pessoal e profissional.

Ao CMG (FN-RM1) Wagner da Silva Reis, pelo apoio, simplicidade e tranquilidade que me transmitiu na orientação deste trabalho.

Aos Instrutores e Oficiais-Alunos da turma do C-EMOS 2019, pelos conhecimentos transmitidos e convivência cordial que facilitaram a obtenção dos conhecimentos necessários para a consecução deste trabalho.

RESUMO

As Convenções de Genebra e seus Protocolos Adicionais são anteriores ao reconhecimento daquele que hoje é considerado o quinto domínio de condução da guerra: o Espaço Cibernético. Mesmo não estando presente explicitamente nos dispositivos legais do Direito Internacional Humanitário, diversos autores defendem que os seus princípios fundamentais são suficientes para impor limitações ao emprego de armas cibernéticas em conflitos armados. Por isso, com base nesse cenário, o objetivo desta pesquisa é responder à seguinte questão: em que medida as ações de guerra cibernética podem ser consideradas violações ao Direito Internacional Humanitário? Nesse sentido, por meio do uso do método dedutivo, optou-se pela realização de pesquisa documental e bibliográfica. Isso porque foi feita uma análise das ações de guerra cibernética colocadas em prática por ocasião do conflito entre Rússia e Geórgia de 2008 à luz dos princípios fundamentais do Direito Internacional Humanitário. Ressalta-se que, após feita a análise, concluiu-se que os princípios da distinção, limitação e proporcionalidade foram desobedecidos pela Rússia nas ações cibernéticas colocadas em prática no conflito. Já os princípios da necessidade militar e humanidade não puderam ser aplicados em virtude da característica não cinética da arma cibernética e da dificuldade de se medir os danos provocados, respectivamente. Além disso, a pesquisa indicou que as ações de guerra cibernética podem ser consideradas violações aos princípios fundamentais do Direito Internacional Humanitário, estando os Estados transgressores sujeitos ao julgamento por parte dos tribunais internacionais. Também, a título de precaução contra interpretações equivocadas a respeito da aplicação dos princípios fundamentais do Direito Internacional Humanitário, esta pesquisa indica que deve-se levar tal debate aos fóruns de discussão de modo a incluir tais limitações de forma explícita no arcabouço legal do Direito Internacional.

Palavras-chave: Princípios do DIH. *Jus in Bello*. Direito Internacional. Guerra cibernética. Conflito russo-georgiano.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

CCDCOE – Centro de Excelência de Defesa Cibernética Cooperativa da OTAN

COE – Conselho da Europa

CRC-ICS – *Cyber Research Center – Industrial Control Systems*

CRS – *Congressional Research Service*

DICA – Direito Internacional dos Conflitos Armados

DDoS – Ataque distribuído de negação de serviço

DIH – Direito Internacional Humanitário

EUA – Estados Unidos da América

ICJ – Corte Internacional de Justiça

MD – Ministério da Defesa do Brasil

OSCE – Organização para a Segurança e Cooperação na Europa

OTAN – Organização do Tratado do Atlântico Norte

PA-I – Protocolo I de 1977 adicional às Convenções de Genebra de 1949

SI – Sistema Internacional

UE – União Europeia

URSS – União das Repúblicas Socialistas Soviéticas

SUMÁRIO

1 INTRODUÇÃO

A guerra é um fenômeno que esteve presente em diversos momentos do processo de evolução da sociedade e tem sido utilizado frequentemente como instrumento para resolução de controvérsias entre grupos organizados beligerantes.

Carl Von Clausewitz (1780-1831), General Prussiano e pensador militar, é autor do livro intitulado "Da Guerra"[1]. Seu livro, publicado *post-mortem,* em 1832, tornou-se um dos mais respeitados clássicos da estratégia militar. Nele, Clausewitz define a guerra, de uma forma mais intimamente ligada ao duelo, como um ato de força para obrigar o inimigo a fazer a nossa vontade.

> A guerra nada mais é do que um duelo em grande escala. Inúmeros duelos compõem a guerra, mas uma imagem dela como um todo pode ser formada imaginando um par de lutadores. Cada um tenta através da força física obrigar o outro a fazer sua vontade. Seu objetivo imediato é atingir seu oponente de modo a torná-lo incapaz de continuar resistência (CLAUSEWITZ, 2008, p. 75, tradução nossa)[2].

De outra forma, Thomas Hobbes (1588-1679), filósofo, cientista e historiador inglês, definiu o homem como um ser agressivo que, dada sua condição natural, tende fortemente a utilizar o conflito como instrumento para atingir seus objetivos e a se posicionar perante um grupo organizado. Sendo assim, caso não houvesse uma força capaz de limitar tais impulsos naturais, o homem se tornaria "o lobo do próprio homem", isto é, "*homo homini lupus*". Em outras palavras, em seu estado natural, o homem tenderia a viver em um ambiente anárquico, em que todos lutariam contra todos (HOBBES, 2012).

Em geral, é possível dizer que a sociedade organizada tem buscado encontrar meios que limitem a ocorrência de conflitos e reduzam os danos e sofrimentos impostos aos beligerantes. E é justamente nesse sentido principal que surge o Direito Internacional Humanitário (DIH), ou Direito na Guerra, que tem como elementos centrais as quatro Convenções de Genebra de 1949 e os dois

---

1 Título original: Vom Kriege.

2 No original, em inglês: "War is nothing but a duel on a larger scale. Countless duels go to make up war, but a picture of it as a whole can be formed by imagining a pair of wrestlers. Each tries through physical force to compel the other to do his will; his immediate aim is to throw his opponent in order to make him incapable of further resistance."

Protocolos Adicionais de 1977.

Um aspecto importante a ser considerado é o espaço temporal no qual esses dispositivos foram inseridos no arcabouço legal do Direito Internacional. Assim, o que se pretende apontar é que, naquela época, havia apenas três domínios de condução da guerra oficialmente reconhecidos, que eram diretamente ligados ao espaço geográfico associado: domínios terrestre, naval e aéreo. Ou seja, as Convenções de Genebra e seus Protocolos Adicionais são anteriores ao reconhecimento daquele que hoje é considerado o quinto domínio de condução da guerra: o Espaço Cibernético[3]. De toda forma, mesmo não estando presente explicitamente nos dispositivos legais do DIH, a corrente majoritária de autores defende que seus princípios fundamentais seriam suficientes para impor limitações ao emprego de armas cibernéticas em conflitos armados.

O objeto de estudo, enquanto fração da realidade investigada, foi o conflito entre Rússia e Geórgia de 2008. Desse modo, o objetivo da pesquisa foi a análise das ações de guerra cibernética no contexto do conflito entre Rússia e Geórgia de 2008 à luz dos princípios fundamentais do DIH que norteiam ou limitam o uso da força pelas partes envolvidas em conflitos armados. Um dos fatores que direcionou a delimitação do objeto deste trabalho, é o fato de que este evento talvez tenha sido o primeiro conflito armado entre Estados no qual a arma cibernética foi empregada em conjunto com as ações de guerra tradicionais. Portanto, em face desse cenário, espera-se que, ao final, seja possível responder ao seguinte questionamento: em que medida as ações de guerra cibernética podem ser consideradas violações aos princípios fundamentais do DIH?

Ressalta-se que para empreender este estudo, o presente trabalho encontra-se estruturado em seis capítulos, sendo esta introdução o primeiro deles.

Em seguida, no segundo capítulo, apresenta-se um delineamento da trajetória histórica do DIH, o seu embasamento legal e, mais detalhadamente, cada um dos seus princípios fundamentais.

---

3 De acordo com a Doutrina militar de defesa cibernética, do Ministério da Defesa do Brasil, os outros quatro domínios de condução da guerra são: terrestre, naval, aéreo e espacial (BRASIL, 2014).

No terceiro capítulo, de modo a enfrentar um aprofundamento teórico que permita uma melhor compreensão e análise das ações, são abordados os conceitos e definições aplicados à guerra cibernética, as características do espaço cibernético, seu espectro de utilização e as possibilidades de emprego da arma cibernética.

Já no quarto capítulo, é feito um estudo acerca do conflito histórico objeto deste trabalho. Para tanto, são analisados os seus antecedentes, o modo como se desenvolveu o conflito, as ações de guerra cibernética nele colocadas em prática e os efeitos provocados nos alvos atingidos pelos ataques.

No quinto capítulo, busca-se compreender de que forma o DIH poderia ser aplicado como fator limitador ou orientador das ações de guerra no espaço cibernético. Após isso, é dado foco à análise dos ataques cibernéticos ocorridos no conflito sob a ótica de cada um dos cinco princípios fundamentais do DIH.

Finalmente, no sexto capítulo, são apresentadas conclusões. Neste capítulo, busca-se responder à questão de pesquisa que norteia este trabalho. Também neste capítulo são feitas reflexões sobre como inibir interpretações equivocadas a respeito da aplicação dos princípios fundamentais do DIH e, deste modo, esta pesquisa indica que deve-se levar tal debate aos fóruns de discussão de modo incluir tais limitações de forma explícita no arcabouço legal do Direito Internacional.

2 O DIREITO INTERNACIONAL HUMANITÁRIO

O DIH refere-se a um conjunto de regras internacionais, estabelecidas por tratados ou tendo como fonte o direito consuetudinário, que são destinadas especificamente a solucionar problemas decorrentes de conflitos armados internacionais ou não-internacionais e, por razões humanitárias, a restringir o direito das partes envolvidas em um conflito de empregar os métodos e meios de combate. Além disso, o DIH busca proteger pessoas e bens que são ou podem ser afetados por tais conflitos. Dois outros termos comumente empregados para se referir a tal conjunto de regras são: *Jus in Bello* e Direito Internacional dos Conflitos Armados (DICA) (SANDOZ; SWINARSKI; ZIMMERMANN, 1987).

Em apertada síntese, o DIH tem por objeto a proteção da pessoa que não participa ou deixou de tomar parte em determinado conflito e bens culturais e outros que não contribuam ao esforço dos contendores, além de permitir que os Estados beligerantes busquem atingir seus objetivos, com eficiência e eficácia, sem destruições ou baixas desnecessárias.

No intuito de propor uma clara definição e limitação do alcance deste estudo, considera-se também destacar que o DIH não se propõe a regulamentar as condições sob as quais os Estados podem recorrer à guerra. A proibição do uso da força entre os Estados e suas exceções (autodefesa, autorização para o uso da força e movimentos de autodeterminação dos povos), estabelecida na Carta das Nações Unidas de 1945, é regida por um ramo distinto do Direito Internacional, o *Jus ad Bellum*[4]

Conforme descreve Michael Byers (2007, p. 143),

> O direito humanitário internacional – J*us n Bello* – determina *como* as guerras podem ser combatidas. Diferencia-se das normas que determinam *quando* as guerras podem ser empreendidas: o Jus ad Bellum da Carta da ONU e a legítima defesa.

Levando-se em conta tais conceitos, faz-se impositivo o detalhamento sobre o emprego

4 Do Latim, direito à guerra.

de dois termos ou expressões distintas quando se estuda o Direito Internacional: guerra e conflito armado.

Após o término da Segunda Guerra Mundial (1939-1945), com o posterior processo de estabilização do Sistema Internacional (SI) sob uma nova Ordem Mundial, elevou-se o número de questões conflituosas motivadas por um movimento de descolonização. Dentre os conflitos ocorridos desde 1945, apenas uma pequena parte foi classificada por todas as partes como "guerra". A Comunidade Internacional percebeu, então, que esse conceito, na medida em que é definido como sendo um conflito entre dois ou mais Estados soberanos, não contemplaria todas as situações de beligerância da sociedade contemporânea (BORGES, 2006).

Assim, o termo "guerra" foi propositadamente substituído no DIH pela expressão "conflito armado". Isso ocorreu porque este termo tem uma aplicabilidade mais abrangente. Buscava-se superar, assim, a limitação do termo "guerra", o que permitiu ao DIH abranger um número muito mais elevado de situações conflituosas.

2.1 As origens do DIH

Mesmo tida como uma das práticas mais brutais da raça humana, a guerra se fez presente em grande parte do processo evolutivo das relações entre os Povos. Se nos primórdios não havia limitações ao uso da guerra nas relações internacionais, com o crescimento e desenvolvimento da sociedade humana, emergiu uma inquietude para a criação de regras que legitimassem o uso da força pelos Estados (BORGES, 2006).

As primeiras iniciativas no sentido de tentar limitar o uso indiscriminado da força durante os conflitos ocorreram nas grandes civilizações da Antiguidade. De acordo com Cinelli (2016), o Rei Hammurabi (1810 a.C–1750 a.C), da Babilônia, instituiu o Código que levou seu

nome. O código, dentre outras coisas, continha regras que tinham por objetivo proteger os mais fracos contra a violência dos mais fortes e determinava a libertação de reféns mediante o pagamento de resgates.

Na Grécia Antiga, por ocasião das guerras entre as cidades-estados gregas, os combatentes eram considerados possuidores de direitos iguais. Por isso, cultivava-se como princípio fundamental o respeito pela vida e pela dignidade das vítimas da guerra, além do zelo que era dispensado aos cadáveres e aos despojos dos mortos em combate (CINELLI, 2016).

No entanto, o surgimento do DIH ocorreu, realmente, em meados do século XIX, por meio de Francis Lieber (1798-1872) e Henry Dunant (1828-1910) que, diante de suas experiências traumáticas em conflitos armados, perceberam a necessidade do desenvolvimento e implementação de um DIH moderno e eficaz (BORGES, 2006).

Em 1861, Francis Lieber, filósofo político e professor germano-estadunidense de jurisprudência e ciência política da Universidade de Columbia (NY), organizou, a pedido do então Presidente estadunidense Abraham Lincoln, um sistema normativo que visava a orientar a condução de toda a guerra terrestre. Seu objetivo era o de evitar o sofrimento e de limitar o número de vítimas do conflito. Tal manual, que ficou conhecido como "Código Lieber", foi colocado em prática pela primeira vez em 1863, por ocasião da Guerra de Secessão (1861-1865). De fato, os números de baixas nesse conflito demonstraram a necessidade da sua aplicação. Por exemplo, no dia 17 de setembro de 1862, conhecido como "*America's Bloodiest Day*"[5], por ocasião da Batalha de Antietam, aproximadamente 23 mil combatentes morreram ou foram gravemente feridos (CINELLI, 2016). De todo modo, o Código Lieber serviu como base para diversos esforços normativos que se iniciaram na sociedade internacional no século XIX.

De outro modo, em 24 de junho de 1859, Henry Dunant, um empresário suíço natural de Genebra, enquanto se dirigia a Solferino, norte da Itália, a fim de encontrar o imperador francês Napoleão III, teve uma dura experiência ao presenciar a Batalha de Solferino. Esse duelo, que

5 "O dia mais sangrento da América" (tradução nossa).

envolveu franceses, italianos e austríacos, registrou ao final do dia cerca de 40 mil soldados mortos. O que impressionou o empresário foi a ausência de qualquer estrutura ou esforço organizado para o atendimento dos feridos e doentes, que eram abandonados à própria sorte nos campos de batalha, muitas vezes sendo roubados ou assassinados pelos habitantes locais. Assim, após esse evento, Dunant publicou a obra intitulada "*Un souvenir de Solférino*" (1862), onde descreve o que presenciou e evidencia duas ações que deveriam ter sido utilizadas para evitar aquele resultado traumático. Tais ações envolviam a criação de uma sociedade de socorro privada e a aprovação de um tratado internacional. Dunant iniciou, então, um movimento que culminou na fundação, em 1863, do Comitê Internacional de Ajuda aos Feridos que, em 1880, foi transformado no atual Comitê Internacional da Cruz Vermelha. Por tal envolvimento, Henry Dunant é considerado o legítimo fundador do DIH. (BORGES, 2006).

2.2 As fontes do DIH

O Estatuto da Corte Internacional de Justiça (ICJ), principal órgão judicial das Nações Unidas que tem como uma das funções resolver, de acordo com o Direito Internacional, os litígios jurídicos que lhe são submetidos pelos Estados, estabelece, no seu art. 38, que os julgamentos tomarão por base (INTERNATIONAL…, 2004):

a) As convenções internacionais, quer gerais, quer especiais, que estabeleçam regras expressamente reconhecidas pelos Estados litigantes;

b) O costume internacional, como prova de uma prática geral aceita como sendo o direito;

c) Os princípios gerais de direito, reconhecidos pelas nações civilizadas; e

d) As decisões judiciárias e a doutrina dos juristas mais qualificados das diferentes

nações, como meio auxiliar para a determinação das regras de direito.

De acordo com o *International Committee of the Red Cross* (2004), uma grande parte do DIH está contida nas quatro Convenções de Genebra de 1949. Posteriormente, as Convenções foram complementadas por dois outros acordos: os dois Protocolos Adicionais de 1977 relativos à proteção de vítimas de conflitos armados. Praticamente todos os Estados da comunidade internacional são signatários ou concordam em ficar vinculados a tais tratados. Além das Convenções de Genebra e seus Protocolos Adicionais, outros acordos proíbem ou restringem o uso de certas armas e táticas militares, protegendo certas categorias de pessoas e bens. São eles: a Convenção para a Proteção dos Bens Culturais em Caso de Conflito Armado e seus dois protocolos (1954), a Convenção sobre Armas Biológicas (1972), a Convenção de Armas Convencionais e seus cinco protocolos (1980), a Convenção sobre Armas Químicas (1993), a Convenção de Ottawa sobre minas antipessoal (1997) e o Protocolo Opcional à Convenção sobre os Direitos da Criança sobre o envolvimento de crianças em conflitos armados (2000).

2.3 Os Princípios Fundamentais do DIH

Conforme já foi dito, o DIH visa a atenuar os danos causados pelas guerras por meio da busca pelo equilíbrio entre as necessidades militares dos Estados partes no cumprimento de suas missões, com as exigências impostas por princípios de caráter humanitário.

Algumas vezes, tanto os tratados quanto as normas consuetudinárias do DIH não asseguram orientações que permitam uma abordagem suficientemente abrangente. Tal efeito pode então ser alcançado por meio dos chamados princípios fundamentais. Se bem assimilados, tais princípios serão facilmente identificados por ocasião do enquadramento das ocorrências nas respectivas regras positivadas, além de servirem como amparo para a eficácia jurídica em casos que

não permitam uma aplicabilidade objetiva dessas regras (CINELLI, 2016).

Para efeito deste trabalho, segue-se o que prevê o Ministério da Defesa (MD) Brasileiro para a determinação dos princípios fundamentais do DIH. Assim, sublinha-se que, de acordo com o Manual de Emprego do DICA nas Forças Armadas (2011), são os princípios fundamentais do DIH: Distinção, Limitação, Proporcionalidade, Necessidade Militar e Humanidade.

2.3.1 Princípio da Distinção

É sobre o Princípio da Distinção que se alicerça todo a estrutura do corpo normativo do DIH destinado à proteção de pessoas e bens. Como dito, tal princípio visa a justamente proteger as pessoas e bens que não são parte do conflito. Ele está apoiado no que prevê o art. 48 do Protocolo I de 1977 adicional às Convenções de Genebra de 1949 (PA-I) (BRASIL, 1993, s.p.):

> Art. 48 A fim de garantir respeito e proteção a população civil e aos bens de caráter civil, as Partes em conflito deverão sempre fazer distinção entre a população civil e os combatentes, entre os bens de caráter civil e os objetivos militares e, em consequência, dirigirão suas operações unicamente contra os objetivos militares.

Como pode-se observar, para a aplicação deste princípio, faz-se necessária uma a adequada distinção entre aqueles que são considerados população civil e os que possuem o *status* de combatente, além de um correto entendimento do que seria objetivo militar.

Em se tratando do primeiro caso, qual seja, a distinção entre população civil e combatentes, a I Convenção de Genebra (1864) apenas se referia aos militares, uma vez que partia do pressuposto de que os civis não participavam das hostilidades. A IV Convenção de Genebra (1949) é que trata de uma forma mais ampla da proteção dos civis. De uma forma mais direta, foi o PA-I o primeiro a definir o que viria a ser um civil. (CINELLI, 2016).

Para os propósitos do Princípio de Distinção em conflitos armados internacionais, todas as pessoas que não são membros das forças armadas de uma parte no conflito, nem participantes de um levante em massa, são civis e, como tal, têm direito a proteção contra ataques diretos, a menos e

pelo tempo que eles participarem diretamente nas hostilidades (MELZER, 2009).

Os integrantes de levantes em massa, do francês *leveé em masse*, são definidos no art. 4, letra A, § 6 da III Convenção de Genebra, que trata dos prisioneiros de guerra, privilégio daqueles que adquirem o *status* de combatentes (BRASIL, 1957, s.p.).

> 6. A população de um território não ocupado que, à aproximação do inimigo, pegue espontaneamente em armas, para combater as tropas de invasão, sem ter tido tempo de se organizar em força armada regular, desde que transporte as armas à vista e respeite as leis e costumes da guerra.

Para se qualificar como participação direta nas hostilidades, um ato específico deve atender aos seguintes critérios cumulativos (MELZER, 2009):

a) Limiar de dano: o ato deve ser capaz de afetar adversamente as operações militares ou a capacidade militar de uma das partes em um conflito ou, alternativamente, infligir morte, ferimento ou destruição a pessoas ou bens protegidos contra-ataques diretos;

b) Causalidade direta: deve existir um nexo causal direto entre o ato e o dano que este possa resultar, seja do ato em si ou de uma operação militar coordenada de que este seja parte integrante; e

c) Nexo de beligerância: o ato deve ser especificamente planejado para causar diretamente o limiar de danos requerido em apoio a uma parte em conflito e em detrimento de outra.

Além da necessária distinção entre civis e combatentes, conforme já citado no art. 48 do PA-I, há de se buscar também distinguir os bens de caráter civil dos objetivos militares. Os seja, os ataques deverão se limitar estritamente aos alvos classificados como objetivos militares (BRASIL, 1957).

Bens de caráter civil, de acordo com o § 1 do art. 52 do PA-I, são todos os bens que não são objetivos militares (BRASIL, 1957). Já objetivos militares, no que concerne aos bens, são aqueles objetos que, por sua natureza, localização, propósito ou utilização, contribuem de forma efetiva para a ação militar e cuja destruição parcial ou total, captura ou neutralização, nas circunstâncias dominantes na situação reinante, ofereça uma clara vantagem militar. Tal definição é

estabelecida no § 2 do art. 52 do PA-I (BRASIL, 1957).

Dessa forma, para que um bem de caráter civil seja classificado como objetivo militar legítimo, deve atender aos seguintes elementos:

a) Sua natureza, localização, propósito e utilização oferecem uma clara contribuição para a ação militar; e

b) Sua destruição total ou parcial, neutralização ou captura oferecem uma clara vantagem militar.

Importante também citar que o PA-I estabelece uma série de bens que possuem o *status* de protegidos (BRASIL, 1957):

a) Bens de caráter civil que não são objetivos militares (§ 1 do art. 52);

b) Bens culturais e dos lugares de culto (art. 53);

c) Bens indispensáveis à sobrevivência da população civil (art. 54);

d) Meio ambiente natural (art. 55); e

e) Obras e instalações contendo forças perigosas, por exemplo: diques, represas e centrais nucleares de energia elétrica (art. 56).

2.3.2 Princípio da Limitação

Em obediência ao Princípio da Limitação, o direito das partes beligerantes na escolha dos meios empregados para causar danos ao inimigo não é ilimitado. As partes devem descartar ações, meios e métodos que levem ao sofrimento desnecessário e a danos supérfluos ao inimigo (BRASIL, 2011).

Nesse sentido, o PA-I no seu art. 35 estabelece (BRASIL, 1957):

> 1. Em todo conflito armado, o direito das Partes em conflito a escolha dos métodos ou meios de combate não é ilimitado.
> 2. É proibido o emprego de armas, projéteis, materiais e métodos de combate de tal índole

> que causem males supérfluos ou sofrimentos desnecessários.
> 3. É proibido o emprego de métodos ou meios de combate que tenham sido concebidos para causar, ou dos quais se pode prever que causem, danos extensos, duradouros e graves ao meio ambiente natural.

O próprio conceito de DIH adotado neste estudo, atribuído por Sandoz, Swinarski e Zimmermann (1987) como o conjunto de regras internacionais que são destinadas especificamente a limitar o direito das partes envolvidas em um conflito de empregar os métodos e meios de guerra, contempla o princípio da limitação.

Segundo Cinelli (2016), de modo que seu efeito tenha uma abrangência adequada, o Princípio da Limitação possui três vertentes: em relação aos locais, às pessoas e aos métodos.

a) Em relação ao local: limita os ataques somente aos alvos considerados lícitos, ou seja, àqueles classificados como objetivos militares.

b) Em relação às pessoas: tal limitação é oriunda das normas consuetudinárias que protegem as pessoas. Os §§ 1 e 2 do art. 51 do PA-I estabelecem que (BRASIL, 1957, s.p.):

> 1. A população civil e as pessoas civis gozarão de proteção geral contra os perigos provindos de operações militares. Para tornar efetiva esta proteção, além das outras normas aplicáveis de Direito internacional, observar-se-ão em todas as circunstâncias as normas seguintes.
> 2. Não serão objeto de ataque a população civil como tal e nem as pessoas civis. São proibidos os atos ou ameaças de violência cuja finalidade principal seja aterrorizar a população civil.

De outro modo, a população civil deverá abster-se de tomar parte no conflito para fazer jus a tal proteção, conforme estabelece o § 3 do mesmo artigo (BRASIL, 1957, s.p.):

> 3. As pessoas civis gozarão da proteção outorgada por esta Seção, exceto se participam diretamente das hostilidades e enquanto dure tal participação.

c) Em relação aos métodos: busca influenciar os métodos e meios empregados no conflito. Como um exemplo da tentativa de limitação desses meios e métodos, o § 4 do art. 51 do PA-I prevê (BRASIL, 1957, s.p.):

> 4. São proibidos os ataques indiscriminados. São ataques indiscriminados:
> a) aqueles que não são dirigidos contra um objetivo militar específico;
> b) aqueles que empregam métodos ou meios de combate que não se podem dirigir contra um objetivo militar específico; ou
> c) aqueles que empregam métodos ou meios de combate cujos efeitos não seja possível limitar conforme o exigido pelo presente Protocolo (…)

Tal vertente está intimamente ligada ao Princípio da Proporcionalidade, que é tratada a seguir, na medida em que busca que os meios e métodos empregados para o cumprimento da missão não ultrapassem um limite razoável ou não provoquem sofrimento desnecessário ao inimigo.

2.3.3 Princípio da Proporcionalidade

Considerando este princípio, a utilização dos meios e métodos de guerra deve ser proporcional à vantagem militar concreta e direta. Em outras palavras, mesmo identificando um objetivo militar legítimo, tal objetivo somente deve ser atacado se os prejuízos e sofrimento forem proporcionais aos ganhos militares que se espera com aquela ação (BRASIL, 2011).

Tal princípio é evidenciado nos §§ 2 e 3 do art. 57 do PA-I, que trata das precauções no ataque (BRASIL, 1957, s.p.):

> 2. Com respeito aos ataques, as seguintes precauções deverão ser tomadas:
> a) aqueles que planejem ou decidam um ataque deverão:
> iii) abster-se de decidir de efetuar um ataque quando seja previsível que causará incidentalmente mortos ou feridos na população civil, danos a bens de caráter civil, ou ambas as coisas, que seriam excessivos em relação com a vantagem militar concreta e diretamente prevista;
>
> 3. Quando é possível eleger entre vários objetivos militares para se obter uma vantagem militar equivalente, optar-se-á pelo objetivo cujo ataque, segundo seja de prever, apresente menor perigo para as pessoas civis e os bens de caráter civil.

Cinelli (2016) traz um método prático para avaliar se um ataque atende ao princípio da proporcionalidade. Para validar a seleção de um alvo, o decisor deverá responder ao seguinte conjunto de cinco questões:

a) É possível identificar positivamente o alvo que quero atingir? Ou seja, tenho certeza que se trata de um objetivo militar legítimo?

b) Existem bens protegidos, civis ou não combatentes, escudos humanos involuntários ou preocupações ambientais significativas dentro do alcance da arma que desejo empregar para atacar o alvo?

c) É possível reduzir os danos colaterais alterando a arma ou método de engajamento no ataque ao alvo selecionado? De outra forma, haverá menos mortes se empregarmos outra arma ou método, sem o prejuízo do cumprimento da missão?

d) Caso negativo, qual a previsão de civis que acredito que serão feridos ou mortos em decorrência do ataque?

e) Os danos colaterais esperados com o ataque são excessivos em relação à vantagem militar que espero alcançar?

2.3.4 Princípio da Necessidade Militar

Conforme visto no item anterior, é permitido o uso proporcional da força, por ocasião de um conflito armado, com objetivo de forçar a rendição ou degradar a força do inimigo. Porém, a necessidade militar limita a escolha dos meios e métodos empregados para a consecução de um objetivo militar.

Nesse sentido, o Princípio da Necessidade Militar estabelece que, em todo conflito armado, o uso da força deve corresponder à vantagem militar que se pretende obter. Desse modo, a necessidade militar não justifica condutas desumanas, tampouco atividades que sejam proibidas pelo DIH (BRASIL, 2011).

Assim, os princípios da Proporcionalidade e Necessidade Militar estão intimamente ligados. Ou seja, as ações militares motivadas pela necessidade militar devem estar justificadas e alinhadas ao Princípio da Proporcionalidade.

2.3.5 Princípio da Humanidade

O Princípio da Humanidade proíbe que se provoque sofrimentos às pessoas (combatentes ou não) e destruição de propriedades, se tais atos não forem necessários para obrigar o inimigo a se render (BRASIL, 2011). Assim, a finalidade do princípio da humanidade é aliviar e evitar, a todo custo e em qualquer situação conflituosa, o sofrimento humano desnecessário.

2.3.6 Cláusula de Martens

A chamada Cláusula de Martens tem como base o direito consuetudinário e visa, em casos não explícitos nas diversas fontes do DIH, oferecer proteção a civis e combatentes contra condutas desumanas. Tal Cláusula, embora não se constitua em uma nova fonte de Direito Internacional, facilita o surgimento de novas regras consuetudinárias. (BYERS; NOLTE, 2003)

Ainda de acordo com Byers e Nolte (2003), a Cláusula de Martens está presente na maioria dos tratados de DIH, tendo sua origem na apresentação do delegado russo Friedrich von Martens (1845-1909) por ocasião da II Conferência de Haia de 1889.

A versão contemporânea da referida Cláusula está presente no § 2 do art. 1 do PA-I (BRASIL, 1957, s.p.):

> 2. Nos casos não previstos no presente Protocolo ou em outros acordos internacionais, as pessoas civis e os combatentes permanecem sob a proteção e o domínio dos princípios do Direito Internacional derivado dos costumes estabelecidos, dos princípios de humanidade e dos ditames da consciência pública.

Desse modo, após listar e aprofundar os estudos a respeito do DIH e seus Princípios Fundamentais, de modo a permitir um melhor entendimento e dimensionamento dos ataques cibernéticos ocorridos durante o conflito objeto deste trabalho, busca-se, a seguir, abordar os principais conceitos, possibilidades e o espectro de emprego da arma cibernética.

3 A GUERRA CIBERNÉTICA

Em um cenário em que o homem busca incessantemente o desenvolvimento científico e tecnológico, fronteiras antes não imaginadas foram ultrapassadas, em especial no ramo da tecnologia. A aspiração humana de experimentação constante em prol do seu desenvolvimento leva a uma maior percepção da influência que o desenvolvimento da tecnologia exerce na vida das pessoas e, consequentemente, nas relações complexas da sociedade internacional (BARROS, 2015).

Com essa evolução tecnológica cada vez mais acelerada, principalmente com o advento da internet, os Estados passaram a aumentar o investimento em pesquisas com vistas a desenvolver novas tecnologias que proporcionassem maior poder no âmbito das relações internacionais.

Nas definições de Joseph S. Nyle Jr (1937-), cientista político estadunidense, ter poder nas relações internacionais significa a habilidade de afetar os outros atores internacionais para obter o que deseja (NYE JR, 2011). Nesse sentido, ao observar-se o desenrolar da história, não é novidade que a informação tem sido utilizada como fonte de poder para o estabelecimento de quais seriam os Estados e atores mais influentes no âmbito internacional. Assim, a informação é uma das fontes de poder do Estado que, quando bem administrada, pode ser decisiva em uma situação de conflito (BARROS, 2015). Ou seja, conhecimento é poder e é possível até dizer que nunca na história humana as pessoas tiveram acesso a tanta informação (NYE JR, 2008).

Nesse ambiente de profundas transformações, surge um elemento cada vez mais presente nas relações internacionais: a Guerra Cibernética. Esse novo fator incorpora uma ameaça diferenciada à segurança dos Estados. Nessa nova realidade, os conflitos interestatais assumem uma dimensão virtual e passam a ser travadas por meio de ataques cibernéticos que podem paralisar serviços e paralisar ou comprometer serviços de interesses (PECEQUILO, 2009).

Dessa forma, apresentam-se, a seguir, os principais conceitos, definições, características e o emprego da arma cibernética.

3.1 Conceitos e definições da Guerra Cibernética

O nascimento da cibernética como ciência está associado aos trabalhos de Norbert Wiener (1894-1964), que na Segunda Guerra Mundial foi encarregado pelo governo estadunidense de resolver os problemas de controle automático da direção do tiro, na artilharia antiaérea. Wiener utilizou o termo "cibernético" tomando por base o vocábulo grego "kybernetiké", que significa a arte de governar um barco. O termo tinha um amplo uso no pensamento grego, em referência precisamente a fenômenos muito similares ao estudado pelo engenheiro estadunidense. Assim, ele próprio define a cibernética como controle e comunicação entre os seres vivos e a máquina (BARROS, 2015).

No Brasil, a Doutrina de Defesa Cibernética do MD define que Cibernética como a interação, o comando e o controle das redes de computadores, sistemas computacionais e sistemas de comunicações de interesse da Defesa Nacional (BRASIL, 2014).

A Guerra Cibernética pode então ser definida como a utilização de um computador, ou rede de computadores, com a finalidade de travar uma guerra no ciberespaço. Como efeito, podem ser retirados de operação serviços de internet, paralisados ou degradados serviços de uso geral da população (serviço bancário, fornecimento de água e energia elétrica, etc.) ou disseminados códigos maliciosos pela rede (WENDT, 2011).

Também, o MD estabelece que a Guerra Cibernética abrange essencialmente as Ações Cibernéticas. Tais ações visam a utilização defensiva ou ofensiva de informação ou de sistemas de informação, como o objetivo de garantir seu uso em benefício próprio ou explorar, negar, corromper ou destruir as capacidades do adversário nos níveis operacional e tático (BRASIL, 2014).

Tomando por base a definição acima, cabe definir o que seriam as Ações Cibernéticas. Na Marinha do Brasil o termo é empregado como "Ações de Guerra Cibernética". Nesse sentido, a Doutrina Militar Naval estabelece que as ações de guerra cibernética são aquelas que abrangem a

utilização de ferramentas disponíveis nos campos da tecnologia da informação e comunicações objetivando a proteção dos ativos de informação de interesse e, também, para deteriorar os ativos de informação do inimigo (BRASIL, 2017).

Por sua vez, o Manual de Tallinn[6] emprega o termo "Ataque Cibernético". O manual define um Ataque Cibernético, segundo o DICA, como uma Ação Cibernética, ofensiva ou defensiva, que pode vir a provocar ferimentos, morte de pessoas, a inutilização ou a destruição de objetos (SCHMITT, 2013).

Isso posto, trata-se, a seguir, das características do ambiente da guerra onde ocorrem as ações cibernéticas: o espaço cibernético.

3.2 O Espaço Cibernético

Após o término do período da Guerra Fria (1947-1989), com o fortalecimento do fenômeno da globalização e a evolução das tecnologias de informação, surgiu um novo domínio[7] da guerra, o espaço cibernético.

O espaço cibernético somou-se aos demais domínios até então reconhecidos: o terrestre, o marítimo, o aéreo e o espacial. Tais domínios são interdependentes, porém, o domínio cibernético tem a característica de permear os demais. Por isso, as atividades no espaço cibernético podem criar oportunidade de ação para atividades em outros domínios, assim como atividades em outros domínios também criam efeitos no espaço cibernético (BRASIL, 2014).

A definição de Espaço Cibernético, de acordo com a Doutrina Militar de Defesa Cibernética do MD, é o ambiente virtual, constituído por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas

6 Manual elaborado pela Organização do Tratado do Atlântico Norte (OTAN), que trata do Direito Internacional aplicável à Guerra Cibernética.

7 O termo "domínio" é usado com o mesmo sentido de "ambiente".

(BRASIL, 2014).

Há duas diferenças fundamentais entre espaço cibernético e os demais domínios.

A primeira diferença é que há uma certa hierarquização geográfica entre os outros domínios. Essa hierarquização começa com o domínio terrestre cercado pelo domínio marítimo. Esses, por sua vez, estão rodeados pelo domínio aéreo, e o domínio aéreo está cercado pelo domínio espacial. Em contraste, o espaço cibernético está inserido nos demais domínios (WELCH, 2011).

Uma segunda diferença fundamental é que o espaço cibernético foi construído pelo homem e está sob constantemente mudança. A maioria das redes de interesse estão interligadas, levando à percepção de que o espaço cibernético utilizado para as operações militares é uma rede única envolvendo aliados e adversários. Por essa característica de interligação, é praticamente impossível garantir o controle efetivo de todo o espaço cibernético ou de todas as redes de interesse (WELCH, 2011).

Por essas características, o espaço cibernético torna-se um campo propício para a violação de normas jurídicas, em especial aquelas atinentes ao Direito Internacional, uma vez que é frequentado por uma variedade de indivíduos e organizações. Tais elementos podem fazer uso de métodos de dissimulação dificultando a detecção de suas ações ou suas identidades (NYE JR., 2011).

Ainda, de acordo com relatório do *Cyber Research Center – Industrial Control Systems* (CRC-ICS), o espaço cibernético tornou-se uma zona de guerra aberta, em que os Governos de todo o mundo lutam pela supremacia em um teatro de operações novo e invisível. Como resultado, cada vez mais os Governos exploram o espaço cibernético buscando defender a soberania nacional e projetar o poder nacional.

Dessa forma, aborda-se, a seguir, as técnicas passíveis de serem utilizadas pelos atores envolvidos em conflitos no domínio cibernético.

3.3 As técnicas de Ataque Cibernético

Em relação às técnicas de ataque empregadas no espaço cibernético, há uma infinidade de medidas que podem ser utilizadas pelo inimigo para alcançar seus objetivos. De acordo com o *Strategic Cyberspace Operations Guide do US Army War College* (LEITZEL; HILLEBRAND, 2018), algumas dessas são:

a) *Backdoor*: nesta técnica um *software* malicioso é adicionado de forma não autorizada a um programa, de modo a permitir o acesso não autorizado a uma rede ou a outro *software*.

b) Ataque distribuído de negação de serviço (DDoS): técnica que envolve o uso de diversos computadores que inundam um servidor ou um roteador com mais solicitações de pacotes que o *site* pode responder ou processar. O resultado desse ataque é que o tráfego legítimo não consegue acessar o *site* e este fica em um estado desligado. Muitas vezes, *worms*[8] são plantados por meio de *botnets*[9] em computadores para criar máquinas zumbis que permitem que o invasor use essas máquinas como participantes desconhecidos no ataque.

c) *Keylogger*: *hardware* ou *software* malicioso que é instalado de modo invisível em uma máquina com o objetivo de monitorar, registrar e transmitir secretamente tudo o que um usuário digita. Dessa forma, o usuário pode facilmente obter senhas e outras informações pessoais do operador da máquina infectada.

d) Bomba lógica: um *software* ou sequência de instruções que desligam um sistema ou rede, e/ou destroem dados reformatando o disco rígido ou inserindo aleatoriamente lixo em arquivos de dados. Pode infectar um computador por meio do *download* de um programa de domínio público adulterado.

---

8 *Worm*: *software* malicioso contendo código capaz de obter acesso a computadores ou redes. Uma vez dentro do computador ou rede, provoca danos no computador ou na rede, excluindo, modificando, distribuindo ou manipulando os dados.

9 Junção das palavras em inglês “robot” e “network”. Por meio de cavalos de Troia busca infectar e controlar milhares ou até milhões de computadores. Dessa forma, pode controlar uma grande rede de máquinas zumbis, capaz de realizar ataques de DDoS ou outros tipos de ataque cibernético.

e) Cavalo de Troia: *software* ou utilitário que, disfarçadamente, faz-se parecer ser um programa ou utilitário comum e legítimo. No entanto, uma vez instalado, executa funções em segundo plano, de modo a permitir que outros usuários tenham acesso ao computador infectado ou enviem informações deste para outros computadores.

Assim, após apresentar as principais técnicas de ataque no espaço cibernético, trata-se, agora, de estudar o espectro em que se desenvolvem as ações cibernéticas.

3.4 O espectro de utilização do Espaço Cibernético

Apenas uma pequena parte das ações de guerra cibernéticas são equivalentes a um ato de guerra convencional (BROWN; TULLOS, 2012). As definições de ação de guerra cibernética e ataque cibernético, tratadas anteriormente, já fornecem uma ideia de que as ações no espaço cibernético ocorrem em diferentes níveis de dano e escala de feito.

Cabe salientar que as potenciais ações no espaço cibernético se estendem desde aquelas virtualmente indetectáveis, disruptivas[10] até aquelas com grande potencial destrutivo.

As ações desenvolvidas para obter acesso a um sistema podem conter diversas motivações, tal como facilitar futuras atividades criminosas, de espionagem ou militares. Essas ações podem passar despercebidas por bastante tempo ou até jamais serem descobertas. Podem também afetar negativamente a funcionalidade de um sistema de computador ou até mesmo destruir um sistema de forma parcial ou completa. Estes efeitos disruptivos ou destrutivos tendem a ser notados com o tempo. Porém, o autor da ação ou a origem do problema nem sempre são facilmente identificáveis (BROWN; TULLOS, 2012).

Sendo assim, as ações no espaço cibernético podem ser divididas nas seguintes categorias: operações de acesso, ações disruptivas e ataque cibernético.

10 Disruptivo: que provoca ou pode causar disrupção; que acaba por interromper o seguimento normal de um processo.

a) Operações de acesso: visam a entrada não autorizada em sistema do adversário. Esse acesso pode ser obtido por meio de instalação de *software*, burlando medidas de segurança, injetando códigos maliciosos ou explorando vulnerabilidades de um sistema.

b) Ações disruptivas: são ações que visam interromper o fluxo de informações ou a função dos sistemas de informação, sem causar danos físicos ou ferimentos.

c) Ataque cibernético: ações no ciberespaço cujos resultados presumíveis incluem danos ou destruição de bens, morte ou ferimentos em pessoas.

A figura a seguir (FIG. 1) ilustra o espectro das ações no espaço cibernético. Nela, pode-se observar que, quanto mais as ações se aproximem da faixa vermelha, mais estarão próximas as ações de guerra tradicionais no sentido dos danos ocasionados. Logo, mais sujeitas estarão às limitações impostas pelo DIH.

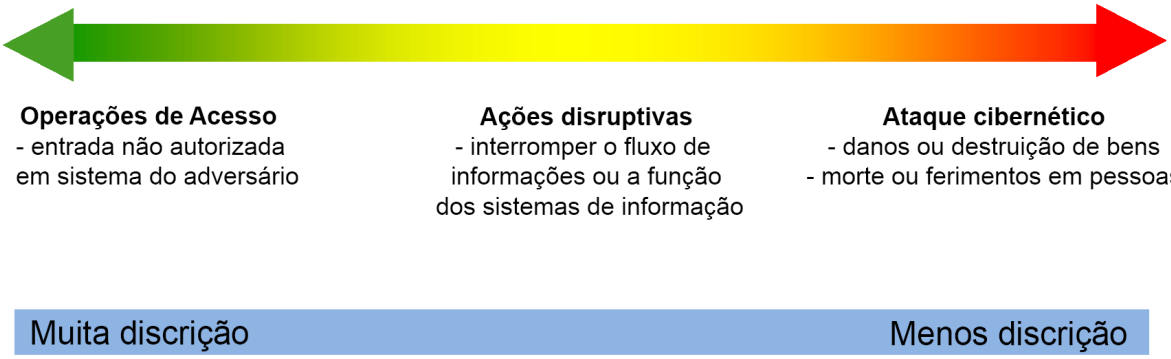

FIGURA 1 – Espectro das ações no espaço cibernético
Fonte: BROWN; TULLOS, 2012. (Adaptada pelo autor)

Dessa forma, é possível, portanto, estudar os antecedentes históricos e o desenvolvimento do conflito ocorrido entre Rússia e Geórgia em 2008, assim como as ações de guerra cibernética e os danos provocados por esses ataques no decorrer do conflito.

4 A GUERRA RUSSO-GEORGIANA

No dia 8 de agosto de 2008, enquanto os líderes mundiais se reuniam em Pequim, Capital da República Popular da China, para assistir à cerimônia de abertura dos Jogos Olímpicos daquele ano, tanques russos atravessavam a fronteira com a Geórgia. Na noite anterior, forças georgianas haviam respondido aos ataques de forças separatistas da Ossétia do Sul, um enclave étnico ao norte do país, dispendendo ataques sobre áreas civis de Tskhinvali, capital da região, com objetivo de tentar retomar o território na base da força. Moscou, que apoiava o governo separatista da Ossétia do Sul por mais de uma década, respondeu com uma invasão em larga escala, enviando aviões e colunas blindadas para aquela província, atacando importantes alvos militares e logísticos dentro da própria Geórgia. Iniciava-se assim o conflito que duraria apenas 5 dias (KING, 2008).

Importante ressaltar que, apesar da curta duração, o conflito tem sido considerado um marco do retorno da Rússia como um importante jogador no tabuleiro da política internacional contemporânea, alterando seu *status quo* na Ordem Mundial vigente desde o término da Guerra Fria.

4.1 Antecedentes históricos e o desenvolvimento do conflito

Tendo em vista o objeto definido para este estudo, as ações de guerra cibernética no conflito Russo-Georgiano de 2008, não tenciona-se o aprofundamento nas motivações políticas ou razões ideológicas que levaram as partes ao conflito. Busca-se assim, apresentar uma sequência cronológica dos fatos históricos que precederam as ações militares e uma breve descrição do desenrolar do conflito. Para tal, toma-se por base os dados constantes do relatório preparado por Jim Nichol (2009), especialista em assuntos Russos e Euro-asiáticos, para o *Congressional Research Service* (CRS) dos EUA.

A Geórgia é um país da Europa oriental cujo território está localizado no cáucaso, região situada entre o mar Negro e o mar Cáspio. Todo território atual do Estado pertencia ao Império Russo até seu declínio, resultante da Revolução Russa de 1917. No ano seguinte os georgianos declararam sua independência e anunciaram o surgimento da "República Democrática da Geórgia". Sua área englobava a região da Abecásia, república autônoma situada no norte do seu atual território, e a metade da região da Ossétia, localizada ao sul das montanhas do Cáucaso. A outra metade, a Ossétia do Norte, permaneceu como parte da Rússia.

Em 1920, a Ossétia do Sul realizou tentativas infrutíferas de declarar sua independência e, no ano seguinte, a Geórgia foi conquistada pelo Exército Vermelho, ocorrendo a instalação de um governo comunista leal a Moscou. Com isso, a Ossétia do Sul permaneceu como uma região autônoma dentro da "República Soviética da Geórgia".

Anos depois, em 1989, grupos separatistas na Ossétia do Sul iniciaram um movimento pela união de seu território com a Ossétia do Norte ou por sua independência. Assim, em 1991, com o colapso da então União das Repúblicas Socialistas Soviéticas (URSS), a Geórgia declarou sua independência e grupos da Abecásia e da Ossétia do Sul reivindicaram soberania sobre suas regiões. Por isso, a recusa do governo central da Geórgia em reconhecer as independências provocou violentos conflitos em ambas as regiões, levando os governos autoproclamados a solicitarem apoio da Rússia.

Em 1992, a Rússia intermediou um cessar-fogo. Também naquele momento, unidades russas, georgianas e ossetas estabeleceram bases em uma zona de segurança ao redor de Tskhinvali. Uma Comissão conjunta de controle promoveu a solução do conflito, tendo a Organização para a Segurança e Cooperação na Europa (OSCE) como entidade moderadora.

No final de 2003, Mikheil Saakashvili chegou ao poder na Geórgia em decorrência da chamada "Revolução das Rosas" e em janeiro de 2004 foi eleito presidente. Saakashvili assumiu com a promessa de realizar reformas nos campos democrático e econômico, além de reconquistar a

autoridade do governo central sobre as regiões separatistas. Assim, a Geórgia aumentou a pressão sobre a Ossétia do Sul reforçando o controle na fronteira, combatendo o contrabando na região e enviando centenas de policiais, militares e funcionários da inteligência para a Ossétia do Sul. A justificativa era que o Estado estava apenas reforçando seu contingente de manutenção de paz, até o limite de 500 soldados, conforme permitido pelo acordo de cessar-fogo. A Rússia também aumentou sua presença na região, auxiliando na entrada de centenas de elementos paramilitares.

Em 2005, o presidente Saakashvili anunciou um novo plano de paz para a Ossétia do Sul que oferecia autonomia substancial e um acordo de três estágios: desmilitarização, reabilitação econômica e solução política. Após o plano de paz proposto pela Geórgia receber apoio do Conselho Ministerial da OSCE, o mandatário da Ossétia do Sul, Eduard Kokoiti, emitiu uma proposta de paz que também continha marcos a serem atingidos, porém previa que a Ossétia do Sul deveria se tornar independente.

Em 2006, um referendo popular foi realizado na Ossétia do Sul para reafirmar sua posição de independência em relação à Geórgia. De acordo com os separatistas, 99% dos eleitores aprovavam o pleito e, em votação separada, Eduard Kokoiti foi eleito com 96% dos votos. Apesar disto, a OSCE e o Departamento de Estado dos EUA se recusaram a reconhecer o resultado. Em votação alternativa realizada entre georgianos da Ossétia do Sul, deslocados internos e outros Sul Ossetianos, o candidato pró-georgia Dmitriy Sanakoyev foi eleito governador da Ossétia do Sul, e um referendo foi aprovado visando à integridade territorial da Geórgia.

Em meados de julho de 2008, a Rússia realizou um exercício militar que demonstrou ser um ensaio para as ações militares na Geórgia que ocorreriam algumas semanas depois. Com o codinome “Cáucaso 2008”, o exercício, que envolveu mais de 8 mil militares, foi realizado nas proximidades da fronteira com a Geórgia. O cenário hipotético era de um ataque de forças não identificas nas regiões separatistas da Abecásia e da Ossétia do Sul. As forças russas treinavam um contra-ataque por terra, mar e ar com o objetivo de apoiar as unidades russas baseadas naquelas

regiões, proteger os "cidadãos russos" e oferecer ajuda humanitária. Em resposta, o Ministério das Relações Exteriores da Geórgia protestou alegando que o cenário constituía uma ameaça de invasão. Simultaneamente ao exercício militar russo, cerca de 1000 militares dos Estados Unidos da América (EUA), 600 tropas georgianas e forças simbólicas da Armênia, Azerbaijão e Ucrânia realizaram um exercício na Geórgia com codinome "*Immediate Response 2008*", com o objetivo alegado de incrementar a interoperabilidade das tropas em operações da OTAN e da coalizão no Iraque.

Na noite de 7 de agosto de 2008, a Ossétia do Sul acusou a Geórgia de lançar um ataque de artilharia contra Tskhinvali, cidade do sul da Ossétia do Sul, enquanto a Geórgia relatou um intenso bombardeio de algumas aldeias georgianas na zona de conflito. Em seguida, a Geórgia anunciou um cessar-fogo unilateral e pediu que a Ossétia do Sul fizesse o mesmo. Logo após, a Geórgia alegou que as forças da Ossétia do Sul intensificaram os ataques, declarou o fim do cessar-fogo e decidiu enviar forças terrestres à Ossétia do Sul.

Em 8 de agosto, em resposta à incursão georgiana na Ossétia do Sul, a Rússia lançou ataques aéreos em grande escala na região e em outros pontos do território da Geórgia. Naquele mesmo dia, aviões russos destruíram aeródromos georgianos, incluindo duas bases aéreas nos arredores de Tbilisi, capital georgiana.

Em 9 de agosto, forças separatistas iniciaram uma ofensiva em Abecásia, com maciça movimentação de tropas, armamentos pesados e bombardeio de vilarejos georgianos.

Em 10 de agosto, após tropas russas ocuparem a maior parte da Ossétia do Sul, a Geórgia emitiu uma nota declarando cessar fogo e informou que retiraria suas tropas de toda a Ossétia do Sul.

Em 12 de agosto, o governo russo anunciou que o objetivo da operação de obrigar a Geórgia a restaurar a paz havia sido alcançado e que havia ordenado o fim das operações.

Cinco dias depois a guerra praticamente havia acabado. Com a mediação do presidente

francês Nicolas Sarkozy, exercendo a presidência da União Europeia (UE), as partes concordaram com os termos do acordo de paz. O acordo exigia que as partes interrompessem as hostilidades e recuassem as tropas para as posições que ocupavam antes do início do conflito.

4.2 As ações de guerra cibernética no contexto do conflito

A Guerra Russo-Georgiana, além de deixar clara a atitude dos governantes russos em prol da manutenção das suas áreas de influência na região do Cáucaso, mostrou também ao mundo as potencialidades do uso de armas cibernéticas no contexto das ações militares em conflitos armados.

De acordo com estudo elaborado pelo Centro de Excelência de Defesa Cibernética Cooperativa da OTAN (CCDCOE)[11], publicado em 2010, antes ainda do dia 08 de agosto, data que marcou o início da invasão russa à Geórgia, os guerreiros cibernéticos já atuavam no domínio cibernético. Sendo mais preciso, a Geórgia registrou as primeiras ações cibernéticas entre os dias 19 e 20 de julho de 2008. Tais ações persistiram até o final de agosto, apesar de as operações militares terem sido encerradas por um acordo de cessar-fogo em 12 de agosto (TIKK; KASKA; VIHUL, 2010).

Em um primeiro momento, as ações visaram principalmente páginas na internet do governo da Geórgia e de meios de comunicação. A técnica empregada pelos *hackers*[12] consistiu em lançar ataques DDoS executados, principalmente, por *botnets*.

Desse modo, em 19 de julho, o *site* oficial do presidente georgiano Mikheil Saakashvili ficou indisponível por mais de 24 horas devido a um ataque DDoS. Foi observado pelo menos um servidor de comando e controle baseado na *Web* atingindo o *site* com uma variedade de ataques

11 O CCDCOE é um centro de defesa cibernética multinacional e interdisciplinar da OTAN, cuja missão é apoiar seus países membros com especialidades interdisciplinares exclusivas na área de defesa cibernética. Disponível em: <https://ccdcoe.org>, acesso em 03 de junho de 2019.

12 *Hacker*: pessoa com capacidade de manipular ou modificar um sistema ou rede de computador.

simultâneos. (TIKK; KASKA; VIHUL, 2010).

Então, exatamente no momento em que o combate terrestre foi deflagrado pelos russos, as ações no domínio cibernético cresceram em complexidade e intensidade.

Em 8 de agosto, o *site* do presidente da Geórgia, do governo central, e as páginas iniciais do Ministério das Relações Exteriores e do Ministério da Defesa sofreram pesados ataques DDoS. Portais de notícias e fóruns de discussão on-line simpáticos à Geórgia também foram atacados. Como resultado dos ataques prolongados, os *sites* governamentais atacados permaneceram indisponíveis pelo menos até 11 de agosto (TIKK; KASKA; VIHUL, 2010).

Ou seja, já no início do conflito com a Rússia, como resultado das ações cibernéticas colocadas em prática, o governo georgiano teve sua capacidade de articulação e consciência situacional bastante degradadas. O ataque DDoS foi tão eficaz que os georgianos perderam o acesso a qualquer fonte de notícia ou informação externa através da internet, além de também não conseguirem sequer enviar *e-mails* para fora do país.

No intuito de defender seu espaço cibernético e interromper os ataques DDoS, buscando recuperar o controle das suas redes, os georgianos tentaram bloquear todo o tráfego originado na Rússia. Porém, os russos reagiram rapidamente redirecionando seus ataques de modo a transparecer que os pacotes vinham China (CLARKE; KNAKE, 2015).

No dia 9 de agosto, um sábado, o maior banco comercial da Geórgia amanheceu sob ataque. E, na medida em que as ações cibernéticas ofensivas se mostravam claramente superiores às tentativas de defesa, o setor bancário georgiano desligou seus servidores, imaginando que a interrupção temporária do sistema bancário *on-line* seria menos danosa do que correr o risco de ter dados críticos de seus sistemas comprometidos. Impedidos de atingir os servidores dos bancos da Geórgia, os russos fizeram com que as máquinas infectadas por *botnets* enviassem uma enxurrada de tráfego para o sistema bancário internacional, fingindo serem ações originadas na própria Geórgia. Em consequência, a maioria dos bancos estrangeiros encerraram suas conexões com o

setor bancário georgiano. Além disso, os sistemas de cartões de crédito e de telefonia móvel também vieram abaixo (CLARKE; KNAKE, 2015).

Em 11 de agosto, o Ministério de Relações Exteriores da Geórgia divulgou um comunicado à imprensa anunciando que ações de guerra cibernética, deflagradas pela Rússia, desativaram *sites* georgianos, obrigando o governo da Geórgia a criar *sites* alternativos. A declaração foi divulgada por meio de um *site* que aquele Ministério havia criado no serviço de hospedagem de blogs do Google (TIKK; KASKA; VIHUL, 2010). O governo russo alegou que tais ações no espaço cibernético eram uma resposta popular às ações da Geórgia e que estavam fora do seu controle. (CLARKE; KNAKE, 2015; MINISTRY…, 2008).

De acordo com Tikk, Kaska e Vihul (2010), não há dúvidas a respeito do envolvimento da comunidade *hacker* russa. A coordenação e o apoio às ações ocorreram principalmente no idioma russo e foram realizados na Rússia ou em fóruns russos. Apesar disso, não foi encontrada qualquer ligação evidente da administração russa com os ataques.

Por fim, o último grande ataque cibernético contra *sites* georgianos foi lançado na tarde do dia 27 de agosto, semanas após o acordo de paz entre as partes. O principal alvo foi o Ministério de Relações Exteriores da Geórgia que, junto com outros *sites*, foi alvo de mais um ataque DDoS. Assim, no dia 28 de agosto ocorreu uma desaceleração dos ataques. Tal fato é atribuído ao sucesso da Geórgia em bloquear as ações dos atacantes (TIKK; KASKA; VIHUL, 2010).

4.2.1 Efeitos das ações cibernéticas

É possível destacar que a principal técnica empregada durante o conflito foi o ataque de DDoS, sendo os principais alvos *sites* de órgãos georgianos, públicos e privados, incluídos órgãos de imprensa, empresas de comunicações e instituições financeiras.

Os ataques DDoS interromperam a comunicação de *sites* essenciais para o governo

georgiano nos primeiros dias do conflito. Este foi, sem dúvida, o período mais crítico. Isso porque o governo georgiano viu reduzida sua consciência situacional a respeito do andamento do conflito e perdeu a capacidade de manter o fluxo vital de informações para sua população e para a comunidade internacional. A indisponibilidade dos *sites* das instituições centrais do governo pode, adicionalmente, ser vista como provocador de um efeito negativo sobre o moral da Geórgia e a confiança do povo georgiano.

As ações cibernéticas também afetaram a prestação de alguns serviços públicos importantes. Em consequência dos ataques DDoS ocorridos em 9 de agosto, o Banco Nacional da Geórgia ordenou que os demais bancos deixassem de oferecer serviços eletrônicos. A população georgiana foi privada destes serviços por um período de dez dias (TIKK; KASKA; VIHUL, 2010).

Um aspecto importante para se avaliar a extensão e resultados das ações cibernéticas, seria dimensionar o prejuízo monetário provocado. No entanto, considerando que tais ações coincidiram com os danos físicos causados pelas ações cinéticas decorrentes do conflito armado, não seria fácil chegar a uma estimativa confiável.

Compreende-se tal dificuldade porque, para se chegar a uma estimativa conclusiva dos danos, seria necessário um esforço coordenado de todas as partes envolvidas, quais sejam: governo, setor privado e usuários. Um fator que poderia vir a se mostrar um obstáculo seria a relutância do setor privado em fornecer dados exatos sobre o tipo e o tamanho dos danos ocorridos (TIKK; KASKA; VIHUL, 2010).

Em suma, pode-se afirmar que é possível pontuar e descrever os tipos de danos que ações no domínio cibernético podem provocar no contexto de um conflito armado, porém, não é certo que dados conclusivos sobre a extensão de tais danos sejam alcançados.

Outrossim, no próximo capítulo trata-se da aplicabilidade do J*us in Bello* como fator limitador ou orientador das ações de guerra no domínio cibernético. Após isto, analisa-se, os ataques cibernéticos ocorridos no conflito à luz dos cinco Princípios Fundamentais do DIH.

5 A GUERRA CIBERNÉTICA E O DIH

A guerra Russo-Georgiana de 2008, que talvez tenha sido o primeiro conflito armado em que ataques cibernéticos foram empregados em conjunto com ações militares convencionais, ilustra a capacidade de geração de danos no campo de batalha cibernético e possibilita o debate sobre a aplicabilidade do DIH sobre essa nova modalidade de guerra (SWANSON, 2010).

Com a evolução tecnológica as armas cibernéticas estão cada vez mais presentes nos combates contemporâneos. Tais conflitos não se consistem mais apenas em ações cinéticas sobre o território inimigo. Além disso, a guerra no domínio cibernético emprega as armas tecnológicas com o objetivo de derrubar ou comprometer infraestruturas vitais do adversário. Assim, como a sociedade moderna depende cada vez mais de estruturas informacionais interconectadas, não é de se espantar que tais elementos tornem-se alvos por ocasião de hostilidades. Além disso, o baixo custo e a possibilidade de operá-las de forma quase anônima são importantes atrativos para a ampla possibilidade de emprego da arma cibernética no campo de batalha contemporâneo (SWANSON, 2010).

Uma vez que um ataque cibernético não seja de natureza verdadeiramente cinética, como os armamentos tradicionalmente empregados nos conflitos armados, algumas pessoas podem enxergar que o DIH não seria um instrumento legal hábil para orientar e limitar ações de guerra no espaço cibernético. Além disso, os dispositivos presentes no DIH são anteriores ao surgimento do domínio cibernético da guerra.

De outro modo, o ataque cibernético caracteriza-se justamente por ser um conjunto de ações desenvolvidas no espaço cibernético cujos resultados presumíveis incluem danos ou destruição de bens, morte ou ferimentos em pessoas. Portanto, em função dessas possíveis consequências é que pode-se depreender que um ataque cibernético pode ser inserido no contexto de um conflito armado, de forma que o DIH seja aplicável no sentido de orientar e limitar o alcance

e efeito de tais ações.

Além da possibilidade de causar danos tangíveis ao inimigo, a presença da chamada Cláusula de Martens, constante do § 2 do art. 1 do PA-I, corrobora com a possibilidade da aplicação do DIH em casos de ações de guerra cibernética no contexto de conflitos armados. De acordo com essa cláusula, mesmo que uma determinada ação não conste literalmente das normas do DIH ou de outros acordos internacionais, as pessoas civis e os combatentes permanecem sob a proteção e o domínio dos princípios do Direito Internacional derivado das normas consuetudinárias.

5.1 Análise das ações cibernéticas à luz dos Princípios Fundamentais do DIH

Um critério decisivo para que uma determinada ação possa ser enquadrada no contexto de um conflito armado é a avaliação de danos possíveis ou provocados. Desse modo, para estar sujeita à aplicação dos dispositivos normativos do DIH uma ação deve intencionar provocar danos, destruições ou mortes.

Em relação ao conflito objeto deste trabalho, embora o governo russo tenha negado oficialmente participação nos ataques cibernéticos à Geórgia, considera-se a Rússia como autora das ações tendo em vista as fortes evidências encontradas pelas investigações realizadas à época.

Dentre as ações colocadas em prática, são abordadas aqui aquelas que se posicionam espectro das ações no ciberespaço entre as ações disruptivas e os ataques cibernéticos. Relembrando o que já foi tratado anteriormente, ações disruptivas são aquelas que visam interromper o fluxo de informações ou a função dos sistemas de informação, sem causar danos físicos ou ferimentos. Já um ataque cibernético configura-se em ações no ciberespaço cujos resultados presumíveis incluem danos ou destruição de bens, morte ou ferimentos em pessoas.

Assim, os principais alvos que sofreram com os efeitos das ações desencadeadas no espaço cibernético foram: páginas na internet do governo georgiano, portais de notícias privados,

sistema bancário georgiano, sistemas de telefonia móvel e de cartões de crédito. Ou seja, as ações comprometeram serviços governamentais e alguns serviços essenciais à população civil georgiana.

Dessa forma, analisa-se, a seguir, tais ações sob a ótica de cada um dos princípios fundamentais do DIH.

a) Princípio da Distinção: tal princípio, apoiado no que prevê o art. 48 do PA-I, tem como objetivo primordial proteger as pessoas e bens que não são parte do conflito. Com base nesse princípio, as partes devem dirigir suas operações unicamente contra os objetivos militares legítimos, poupando civis e os bens de caráter civil.

Em relação aos civis, claramente tal princípio foi desrespeitado pois os ataques DDoS colocados em prática tiveram reflexo em grande parte da população georgiana, ao comprometer serviços essenciais como o sistema bancário, de telefonia e de cartões de crédito.

Já em relação aos objetivos militares, é possível considerar que os bens de caráter civil alvos dos ataques (páginas do governo, sistema bancário, portais de notícia favoráveis à causa georgiana, sistema bancário e de telefonia) não seriam classificados como bens protegidos e seu comprometimento ofereceria uma clara vantagem militar para a Rússia. Porém, não contribuiriam de forma efetiva para a ação militar da Geórgia. Assim, considera-se também que, em relação aos objetivos militares, o Princípio da Distinção não teria sido obedecido.

b) Princípio da Limitação: tal princípio visa a impedir que as partes no conflito utilizem meios e métodos indiscriminados, podendo vir a causar sofrimento desnecessário e danos supérfluos ao inimigo. Analisando o conflito, considera-se que as ações não teriam obedecido a tal princípio pois os ataques não se limitaram aos objetivos militares legítimos, provocaram prejuízos diretos à população civil e utilizaram métodos de ataque indiscriminados. Tal princípio está intimamente ligado ao Princípio da Proporcionalidade que é analisado a seguir.

c) Princípio da Proporcionalidade: tal princípio estabelece que a utilização dos meios e métodos de guerra devem ser proporcionais à vantagem militar esperada. No caso em estudo, apesar

de os danos provocados pelas ações terem sido de curta duração e a dificuldade de serem mensurados, os atacantes não alvejaram apenas objetivos militares legítimos, mas causaram danos à civis e não se ocuparam em reduzir possíveis danos colaterais. Dessa forma, o Princípio da Proporcionalidade também teria sido desrespeitado.

d) Princípio da Necessidade Militar: tal princípio estabelece que, em todo conflito armado, o uso da força deve corresponder à vantagem militar que se pretende obter. Tendo em vista que um ataque cibernético não é uma ação cinética, ao não fazer uso da força, considera-se que não seria possível aplicar tal princípio às ações no espaço cibernético colocadas em prática por ocasião do conflito.

e) Princípio da Humanidade: tal princípio tem por finalidade aliviar e evitar, a todo custo e em qualquer situação conflituosa, o sofrimento humano desnecessário. Ou seja, proíbe que se provoque sofrimentos às pessoas (combatentes ou não) e destruição de propriedades, se tais atos não foram necessários para obrigar a rendição do inimigo. Assim, considerando que os danos provocados pelas ações de guerra cibernética foram de curta duração e que os danos causados não foram dimensionados, considera-se que tal princípio não foi ultrapassado.

De toda forma, como visto, mesmo que as ações de guerra cibernética não constem literalmente das normas do DIH, nem do direito consuetudinário, os tribunais internacionais competentes poderiam se apoiar na Cláusula de Martens para coibir ou levar a julgamento Estados que por ventura vierem a violar os princípios fundamentais do DIH.

6 CONCLUSÃO

O propósito deste trabalho foi analisar as ações de guerra cibernética no contexto do conflito entre Rússia e Geórgia de 2008 à luz dos princípios fundamentais do DIH que norteiam ou limitam o uso da força pelas partes envolvidas em conflitos armados. A escolha do conflito deveu-se ao fato deste constituir um caso em que ficou patente o emprego da arma cibernética em conjunto com o emprego de ações de guerra tradicional.

Ademais, o fato de o domínio cibernético ter sido reconhecido e explorado, no contexto de conflitos armados entre Estados, algum tempo após a assinatura dos tratados que originaram as Convenções de Genebra e seus protocolos adicionais, constitui um importante tema de pesquisa a respeito da aplicabilidade do DIH como fator orientador e limitador do emprego da arma cibernética em conflitos entre Estados.

Desse modo, buscou-se responder ao seguinte questionamento: em que medida as ações de guerra cibernética podem ser consideradas violações aos princípios fundamentais do DIH?

Ressalta-se que, no decorrer da pesquisa, observou-se que o DIH é parte de um conjunto de regras do Direito Internacional que tem por objetivo limitar os danos causados às partes envolvidas em conflitos armados internacionais ou não internacionais, assim como proteger as pessoas que não tomam parte nas ações.

Nesse sentido, e de modo a permitir uma maior abrangência e alcance do DIH, a comunidade internacional passou a utilizar a expressão “conflito armado” em substituição ao termo “guerra”. Isso deveu-se ao processo de transformações do sistema internacional após o término da Segunda Guerra Mundial.

Ao longo desta pesquisa, também foi apontado que as iniciativas de tentar limitar o uso da força em conflitos armados remontam às grandes civilizações da antiguidade. Como exemplo podemos citar o Código instituído pelo Rei Hammurabi (1810 a.C – 1750 a.C). Ainda assim,

observou-se que o DIH tem seu surgimento em meados do século XIX, por meio de Francis Lieber e Henry Dunant, sendo este último o idealizador da criação do atual Comitê Internacional da Cruz Vermelha. Por tal efeito, Dunant é considerado o legítimo fundador do DIH.

De acordo com o estatuto da Corte Internacional de Justiça, as decisões a cerca dos litígios jurídicos submetidos pelos Estados tomam por base principalmente as convenções internacionais, o direito consuetudinário e os princípios gerais do direito reconhecidos pelas nações civilizadas. Grande parte das normas do DIH está contida nas quatro Convenções de Genebra de 1949 e em seus dois protocolos adicionais de 1977. Porém, quando os tratados e as normas consuetudinárias não permitem uma abordagem suficientemente abrangente, os princípios da Distinção, Limitação, Proporcionalidade, Necessidade Militar e Humanidade surgem como um amparo para a eficácia da aplicabilidade dessas regras do DIH.

Em meio a essas informações, cabe também destacar que, ao longo da história, a informação tem sido utilizada como fator de influência e poder entre os Estados. É nesse sentido que o emprego de armas que exploram o domínio cibernético ganha importância nos conflitos contemporâneos.

Desse modo, com o fortalecimento do fenômeno da globalização, em especial após o fim da Guerra Fria, o ciberespaço somou-se aos domínios marítimo, terrestre, aéreo e espacial como domínios operacionais da guerra até então reconhecidos. Tais domínios são interdependentes, com o cibernético permeando os demais.

Nesse contexto, a guerra cibernética constitui-se da utilização de um computador ou rede de computadores com o objetivo de paralisar ou degradar serviços e infraestruturas do inimigo. Com a sociedade moderna cada vez mais dependente de serviços e estruturas informacionais interconectadas, tais elementos tornaram-se alvos por ocasião das hostilidades. Isso porque o baixo custo e a dificuldade de se identificar as fontes e autores dos ataques, ampliou a possibilidade do emprego desta nova arma no campo de batalha contemporâneo.

Em face desse cenário, percebeu-se, ao longo deste estudo, que as ações cibernéticas podem variar desde acessos não autorizados aos sistemas do adversário, até ações que resultem em danos ou destruição de bens, morte e ferimentos de pessoas. Devido ao dano causado, estas últimas aproximam-se mais das ações de guerra tradicionais, e logo estarão mais sujeitas às limitações impostas pelas normas do DIH.

Em relação ao conflito objeto do estudo, verificou-se que tal evento constituiu um marco do retorno da Rússia como um importante jogador no tabuleiro das relações internacionais contemporânea. Verificou-se também que o conflito iniciado em agosto de 2008, com duração de apenas 5 dias, teve como antecedente histórico o processo de independência da Geórgia em relação à Rússia, cujo território englobava as regiões da Abecásia, república autônoma situada no norte do seu atual território, e da Ossétia, cujo território foi dividido entre os dois países. Consequentemente, tais tensões não acomodadas exerceram papel preponderante na deflagração do conflito.

A guerra Russo-Georgiana, além de deixar clara a disposição da Rússia em prol da manutenção de suas áreas de influência na região do cáucaso, mostrou também ao mundo as potencialidades do emprego da arma cibernética. Os ataques cibernéticos iniciaram-se semanas antes das primeiras ações cinéticas por parte da Rússia e persistiram até o término do conflito, contribuindo para a degradação da consciência situacional por parte das autoridades georgianas a respeito do conflito. Tais ações praticamente interromperam o fluxo de informações georgianas para a sua população e para a comunidade internacional.

Os resultados atingidos no campo de batalha pela Rússia, frutos em boa parte das ações de guerra cibernética, possibilitaram o debate na comunidade internacional e a análise neste estudo a respeito da aplicabilidade do DIH sobre essa nova modalidade de guerra. E, conforme já dito, um dos fatores que suscitaram tal discussão foi o aspecto não cinético da arma cibernética.

Dessa maneira, no decorrer do estudo, observou-se que um critério decisivo para que uma ação no domínio cibernético possa ser enquadrada no contexto de um conflito armado, logo

estando sujeita à aplicação das normas do DIH, é a avaliação de danos provocados. Para tal, a ação cibernética deve, ao menos, ter a intenção de provocar danos, destruições ou mortes.

Conforme foi visto, os ataques cibernéticos colocados em prática pela Rússia, tiveram como alvo páginas da internet do governo georgiano, portais de notícias privados, sistema bancário, serviço de telefonia e de cartões de crédito. Assim, verificou-se que tais ações e efeitos podem ser analisados à luz dos princípios fundamentais do DIH.

Dessa forma, conclui-se que os Princípios da Distinção, Limitação e Proporcionalidade foram desobedecidos pela Rússia nas ações cibernéticas colocadas em prática no conflito.

Já em relação aos Princípios da Necessidade Militar e Humanidade, conclui-se que tais princípios não puderam ser aplicados às ações cibernéticas no conflito, em virtude da característica não cinética da arma cibernética e da dificuldade de se medir os danos provocados, respectivamente.

Assim, respondendo ao questionamento proposto pelo estudo, infere-se que as ações de guerra cibernética podem ser consideradas violações aos princípios fundamentais do DIH, estando os Estados transgressores sujeitos ao julgamento por parte dos tribunais internacionais.

Além disso, a título de precaução contra interpretações equivocadas a respeito da aplicação dos princípios fundamentais do DIH, deve-se levar tal debate aos fóruns de discussão de modo incluir tais limitações de forma explícita no arcabouço legal do Direito Internacional.

REFERÊNCIAS

BARROS, Renata Furtado de. **Guerra Cibernética**: os novos desafios do Direito Internacional. Belo Horizonte: D`Plácido, 2015. 178 p.

BORGES, Leonardo Estrela. **O direito internacional humanitário:** a proteção do indivíduo em tempo de guerra. Belo Horizonte: Del Rey, 2006. xviii. 164 p.

BRASIL. **Decreto nº 42.121, de 21 de agosto de 1957**. Promulga as convenções concluídas em Genebra a 12 de agosto de 1949, destinadas a proteger vítimas de defesa. Brasília, DF, 21 ago. 1957. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1950-1959/decreto-42121-21-agosto-1957-457253-publicacaooriginal-1-pe.html.>. Acesso em: 4 maio 2019.

_____. **Decreto nº 849, de 25 de junho de 1993**. Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados. Brasília, DF, 25 jun. 1993. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0849.htm. Acesso em: 4 maio 2019.

_____. Estado-Maior da Armada. **EMA 305 – Doutrina Militar Naval.** 1. ed. Brasília, DF, 2017.

_____. Ministério da Defesa. **MD31-M-07:** Doutrina militar de defesa cibernética. 1. ed. Brasília, DF, 2014.

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

BROWN, Gary D.; TULLOS, Owen W. **On the Spectrum of Cyberspace Operations.** Small Wars Journal, [S. l.], 11 dez. 2012. Disponível em: <https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations.>. Acesso em: 3 maio 2019.

BYERS, Michael. **A lei da guerra: direito internacional e conflito armado**. Rio de Janeiro: Record, 2007. 263 p.

_____; NOLTE, Georg. **United States hegemony and the foundations of international law.** New York: Cambridge University Press, 2003.

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.

CLAUSEWITZ, Carl von Michael Eliot. **On War.** New Jersey: Princeton University Press, 2008. 751 p.

CINELLI, Carlos Frederico Gomes. **Direito Internacional Humanitário:** ética e legitimidade na aplicação da força em conflitos armados. Curitiba: Juruá, 2011. 312 p.

CYBER RESEARCH CENTER. **Cyber Space:** the fifth domain of war. 2016. Disponível em: <https://www.crc-ics.net/documents/CRC-ICS-2016_Cyber-Space_the_fith_domain_of_war_2016-v2.6.pdf>. Acesso em: 19 abr. 2019.

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

HOBBES, Thomas. **Leviatã, ou Matéria, Forma e Poder de um Estado Eclesiástico e Civil.** São Paulo-SP: Martin Claret Ltda., 2012.

INTERNATIONAL COMMITTEE OF THE RED CROSS. **What is International Humanitarian Law?** Genebra, Suíça, 2004. Disponível em: <https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf.> Acesso em: 17 maio 2019.

INTERNATIONAL COURT OF JUSTICE. Statute of the International Court of Justice. Disponível em: <https://www.icj-cij.org/en/statute>. Acesso em: 28 jul. 2019.

KING, Charles. The Five-Day War - Managing Moscow After the Georgia Crisis. **Foreign Affairs**, EUA, EUA, 1 nov. 2008. Disponível em: <https://www.foreignaffairs.com/articles/russia-fsu/2008-11-01/five-day-war.>. Acesso em: 2 jun. 2019.

LEITZEL, Benjamin; HILLEBRAND, Gregory. **Strategic Cyberspace Operations Guide.** Pennsylvania: [s. n.], 2018. Disponível em: <https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf.>. Acesso em: 3 maio 2019.

MELZER, Nils. Interpretative guidance on the notion of direct participation in hostilities under International Humanitarian Law. **International Committee of the Red Cross**, Genebra, Suíça, 2009. Disponível em: <https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf.>. Acesso em: 25 maio 2019.

MINISTRY OF FOREIGN AFFAIRS OF GEORGIA. **Cyber Attacks Disable Georgian Websites**. August 11, 2008. Disponível em: <georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html>. Acesso em: 02 jun. 2019.

NICHOL, Jim. **Russia-Georgia Conflict in August 2008**: Context and Implications for U.S. Interests. Congressional Research Service, Washington-EUA, 2009. Disponível em: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a496306.pdf.>. Acesso em: 2 jun. 2019.

NYE JR., Joseph S. **The future of power.** New York: Public Affairs, 2011. 235 p.

_____. **The powers to lead.** New York: Public Affairs, 2008. 241 p.

PECEQUILO, Cristina Soreanu. **Manual do candidato:** política internacional. Brasília: Fundação Alexandre de Gusmão, 2009 354p.

SANDOZ, Yves; SWINARSKI, Christophe; ZIMMERMANN, Bruno. **Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949**. Genebra, Suíça: International Committee of the Red Cross, 1987. 1625 p.

SCHMITT, Michael N. **Thallinn Manual on the International Law Applicable to Cyber Warfare.** New York: Cambridge University Press, 2013, 215p.

SWANSON, Lesley. **The Era of Cyber Warfare:** Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. Loyola of Los Angeles International and Comparative Law Review, Los Angeles, 22 mar. 2010. Disponível em: <https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1010&context=ilr.> Acesso em: 5 jul. 2019.

TIKK, Eneken; KASKA, Kadri; VIHUL, Liis. **International Cyber Incidents:** Legal Considerations.Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010. Disponível em: <https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf.>. Acesso em: 3 jun. 2019.

WELCH, Gen. Larry D. **Cyberspace – The Fifth Operational Domain**. [S.l.]: Institute for Defense Analyses - IDA, 2011. Disponível em: <https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf.>. Acesso em: 20 abr. 2019.

WENDT, Emerson. Ciberguerra, Inteligência Cibernética e Segurança Virtual: alguns aspectos. **Revista Brasileira de Inteligência**, Brasília, DF, abril 2011. Disponível em: <http://www.abin.gov.br/conteudo/uploads/2018/05/RBI6-Artigo2-CIBERGUERRA-INTELIGÊNCIA-CIBERNÉTICA-E-SEGURANÇA-VIRTUAL-alguns-aspectos.pdf.>. Acesso em: 21 abril 2019.