ESCOLA DE GUERRA NAVAL

CC CAIO VINÍCIUS CESAR FEITOSA

MANUAL DE TALLINN:

o Direito Internacional aplicável à Guerra Cibernética e sua contribuição à dissuasão

Rio de Janeiro

2014

CC CAIO VINÍCIUS CESAR FEITOSA

MANUAL DE TALLINN:

o Direito Internacional aplicável à Guerra Cibernética e sua contribuição à dissuasão

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

Orientador: CF (RM1) Cláudio Luiz de Lima Martins.

Rio de Janeiro

Escola de Guerra Naval

2014

Dedico este trabalho

À minha mãe Sra. Silvina Cesar de Araújo Feitosa, *in memoriam.*

AGRADECIMENTOS

Inicialmente, agradeço à minha esposa Isabella por todo o carinho e incentivo e a minhas filhas Marina, Deborah e Beatriz, pela paciência nas ausências e amor.

Ao meu orientador Capitão-de-Fragata (RM1) Lima Martins e aos meus colegas da turma Lúcio Meira pelas contribuições diárias.

“Lutar e vencer todas as batalhas não é a glória suprema; a glória suprema consiste em quebrar a resistência do inimigo sem lutar.”

(Sun Tzu)

RESUMO

A análise da aplicabilidade do Manual de *Tallinn* e sua estreita interação com o Direito Internacional vigente foi o direcionamento escolhido para ser abordado no estudo, visto que, em uma análise prévia, tais conceitos são indissociáveis. A contextualização da Guerra Cibernética, a caracterização dos tipos de ataques e a identificação dos atores e métodos possibilitarão a compreensão das ações no ciberespaço. Um dos cenários possíveis de aplicação desta nova maneira de fazer a Guerra está no contexto de um conflito armado, com o envolvimento de Estados. A aplicação do Direito Internacional busca soluções de controvérsias, em preservação da raça humana e a garantia de sobrevivência e paz nos conflitos armados. Estratégias de dissuasão buscam desincentivar o início ou a efetivação de uma ação mais hostil. Este trabalho tem como objetivos: analisar a validade de utilização do Manual como uma ferramenta que contribui para uma estratégia de dissuasão e verificar qual o limite para que ataques cibernéticos sejam comparados como uso da força. Para tanto, assume como premissa que o referido manual é uma interpretação à atual legislação vigente e pode garantir a legitimidade das ações cibernéticas nos casos em que as regras estabelecidas não forem cumpridas. Outro fator limitador é comparar as características do documento apenas com partes de uma teoria de dissuasão cibernética, para isso foi considerado que a teoria de Goodman, um consagrado autor de estratégias de dissuasão, é válida. A relevância do estudo está na contribuição para a segurança dos Sistemas de Tecnologia de Informação existentes e na identificação e compreensão de suas vulnerabilidades, além da apresentação das consequências de ações cibernéticas nas relações internacionais. Para tanto, foram coletadas entrevistas de seus autores e realizadas uma revisão de literatura em publicações, obras e artigos sobre Guerra Cibernética, Manual de *Tallinn* e Dissuasão Estratégica. A análise do material comprova que o citado documento é considerado um elemento que contribui para a dissuasão e, em caso de falha nessa estratégia, em observância a suas regras e aos limites impostos pelos requisitos “Schmitt-Criteria”, que qualificam o ataque como uso da força, legitima retaliações em revide a um ataque cibernético sofrido, em ação de legítima defesa, inclusive com a utilização de meios convencionais como ataques armados.

Palavras-chave: Guerra Cibernética, ciberguerra, dissuasão cibernética, Direito Internacional, Manual de *Tallinn.*

SUMÁRIO

1 INTRODUÇÃO

Em um mundo altamente conectado, a *Internet* e as chamadas Tecnologias de Informação (TI) passaram a estar integradas em todos os aspectos da sociedade humana, fato especialmente preocupante, uma vez que nem todos os usuários da rede têm agido com fins pacíficos.

Cada vez mais as Infraestruturas Críticas (IEC)[1] são controladas por sistemas digitais interligados no ciberespaço[2] e quando a dependência nestes sistemas complexos aumenta, também cresce a vulnerabilidade da sociedade com seu uso indevido.

Nessas circunstâncias torna-se evidente que, em um contexto de hostilidades e/ou beligerância entre dois Estados, a exploração das redes de computadores de um oponente constitui uma maneira eficiente de obter vantagens sobre o mesmo; no contexto militar, a exploração dos sistemas de informação computadorizados estabelecidos pelas forças inimigas durante o transcurso de suas operações, pode levar à superioridade no campo de batalha. É justamente destas duas situações de que trata a Guerra Cibernética (GCiber) ou Ciberguerra que surge como uma grande ameaça à segurança internacional no século XXI.

Este estudo tem como objetivo contextualizar a GCiber e levantar os principais desafios decorrentes dos ataques e conflitos cibernéticos à luz da atual legislação internacional. Para isto, identificará e discutirá o papel do Manual de *Tallinn*, analisará as respectivas questões legais associadas e a possibilidade de sua utilização como ferramenta de contribuição para uma estratégia de dissuasão.

Diante deste cenário, se faz necessário responder aos seguintes questionamentos: O Manual de *Tallinn* pode ser considerado um elemento que contribui para a dissuasão na

1 Por infraestruturas críticas entendem-se as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade.

2 Ciberespaço também conhecido como Espaço Cibernético é o ambiente intangível formado por ativos de TI, onde dados e informações digitais são criados, armazenados, modificados, trafegados e processados. Possui as seguintes características: alcance global, ausência de fronteiras e dinamismo.

solução de conflitos no espaço cibernético? E assim, em caso de falha nessa estratégia, qual seria o limite para se considerar ato de Guerra e ensejar legítima defesa, de acordo com a mesma norma?

Será considerado como hipótese a de que o Manual de *Tallinn* fornece legitimidade nas ações cibernéticas e permite, nos casos de violações de suas regras, uma retaliação com a utilização do uso da força, inclusive na forma de ataque convencional.

Cabe ressaltar que para alcançar os objetivos desta pesquisa as metodologias utilizadas foram: análise bibliográfica e método comparativo. Utiliza-se de documentos normativos internacionais, entrevistas, obras e artigos relacionados ao tema.

Para efeito, a abordagem do trabalho foi estruturada da seguinte forma: o segundo capítulo examinará alguns princípios básicos de Direito Internacional (DI) e descreverá brevemente algumas questões legais que estão associadas aos conflitos armados. No terceiro capítulo se fará uma análise de como se configura uma GCiber, suas principais características, limitações e alcance, será verificada a questão da legalidade do recurso à ciberguerra, da problemática da qualificação de um ciberataque como um ataque armado, além de definir seus principais atores. No quarto capítulo se fará a apresentação do Manual de *Tallinn,* sua interligação com os conceitos dos capítulos anteriormente abordados, serão citadas as principais regras relacionadas ao tema e será ampliado o conceito de qualificação de um ciberataque, além de tratar o delicado problema da atribuição de responsabilidade em um ciberataque. Em continuação, no quarto capítulo, a obra passa ganhar contornos normativos e possibilitará que seja feita uma comparação do Manual de *Tallinn* com alguns fundamentos básicos de uma teoria de dissuasão. O quinto capítulo encerra este trabalho com uma conclusão do que foi exposto.

2 COMPREENSÃO DA BASE JURÍDICA

Para iniciar o desenvolvimento do assunto, este capítulo apresenta os conceitos e definições do Direito Internacional (DI) que estão relacionados com as soluções de controvérsias e manutenção da paz entre Estados.

2.1 Vertentes do Direito Internacional

As Nações Unidas têm como propósitos as manutenções da paz e a segurança internacionais e, para alcançar esses objetivos utiliza-se da Carta das Nações Unidas que menciona, dentre outros: o desenvolvimento de relações amistosas entre as nações, a solução pacífica de controvérsias; a responsabilidade coletiva dos Estados pela observância dos direitos humanos e das liberdades fundamentais; as ações relativas às ameaças à paz, ruptura da paz e atos de agressão e os acordos regionais (ONU, 1945). A Carta fundamenta o ramo do DI que se preocupa em definir quais as situações um Estado estará autorizado a utilizar o "uso da força" na solução de controvérsias em casos de ataques, o *jus ad bellum*[3].

Neste contexto, a Carta das Nações Unidas também especifica que a força armada de um Estado não será usada a não ser no interesse comum e passa a tratar de duas situações: a agressão, que é ilegal, e as contramedidas, que podem se dar pela via da legítima defesa, individual ou coletiva ou pelas medidas tomadas por iniciativa do Conselho de Segurança (CS) (ACCIOLY; SILVA; CASELLA, 2002).

Entende-se como agressão o uso da força armada por um Estado contra a soberania, integridade territorial ou independência política de outro Estado, ou de qualquer forma incompatível com a Carta das Nações Unidas[4].

---

3 Direito à Guerra.

4 Resolução 3314 da Assembleia Geral das Nações unidas – Definição de Agressão.

Assim, surge o seguinte questionamento: na atualidade, quais seriam os cenários possíveis em que um Estado poderia estar autorizado a iniciar um conflito armado?

Para responder ao questionamento deve-se atentar que o DI limita e restringe o início de um conflito armado por parte de um Estado. O Artigo 51 da Carta da ONU assim define:

> […] Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um membro das Nações Unidas, [...] As medidas tomadas pelos Membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao CS e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou restabelecimento da paz e da segurança internacionais. (BYERS, 2007, p. 74 e 75, grifo nosso).

Alguns juristas preferem não usar o termo *jus ad bellum* em seus apontamentos, pelo fato da não existência efetiva de um direito à Guerra, mas sim o direito à legítima defesa propriamente dita. Deyra (2001) reitera o raciocínio *em lide* quando acrescenta que a expressão "Direito à Guerra" encontra-se atualmente abandonada a partir do momento em que caducou o conceito do Estado de beligerância, ou, pelo menos, desde a adoção do princípio da proibição do recurso à força. A Carta da ONU consolida os conceitos acima retratados e exerce um papel fundamental na limitação do uso da força, pelo fato de ser a legislação de aceitação universal[5] e por estabelecer um ponto focal na diplomacia internacional.

Paralelamente, existe outro ramo do DI que expressa uma mudança da cobertura legal, que passa da Guerra para o conflito armado propriamente dito, identificado pela terminologia "Direito dos Conflitos Armados" (*jus in bello*)[6]. Tal mudança tornou claro que as regras que protegem as vítimas e limitam os meios e os métodos de combate são aplicáveis a todas as situações[7] nas quais as hostilidades têm lugar e não ficam limitadas às Guerras

5 A ONU possui hoje 193 Países Membros. Disponível em:<http://www.un.org/en/members/index.shtml>. Acesso em: 27 jul. 2014.
6 Significa literalmente Lei na Guerra.
7 Grifo nosso.

formalmente declaradas (KOLB; HYDE, 2008). Essa vertente impõe o princípio da distinção entre combatentes e não combatentes, dentre outros, e leva à proibição dos não combatentes sofrerem qualquer ato de violência. Essa definição conduz aos princípios básicos do DI (BRASIL, 2014), que assentam em: distinção, limitação, humanidade, necessidade militar e proporcionalidade. A distinção seria entre civis e militares; a limitação dentro da proibição de atacar aqueles que estão fora de combate; a humanidade na proibição de infligir sofrimentos desnecessários e princípio da necessidade e princípio da proporcionalidade no uso da força. (KOLB; HYDE, 2008).

Observa-se no exposto acima que o DI não abrange apenas conflitos formalmente declarados e pode ser ampliado para quaisquer hostilidades em diversas situações. Dentro do contexto deste trabalho será verificada a aplicabilidade do DI nas modernas ações cibernéticas[8] que, aparentemente, passam a se apresentar como um novo armamento nos tempos modernos. Nesta linha de raciocínio, cabe ressaltar que a possibilidade de surgimento de novas tecnologias de combate, foi anteriormente declarada pela Corte Internacional de Justiça (CIJ), no Parecer Consultivo sobre a Legalidade da Ameaça ou Uso de Armas Nucleares (ONU, 1996), ao esclarecer que a não existência de instrumento legal específico sobre determinado armamento, de nova invenção, não o exclui do campo de aplicação do direito, entendimento este reforçado pelo Comitê Internacional da Cruz Vermelha (CICV)[9] e também pelo artigo 36 do Protocolo I (1977), adicional às Convenções de Genebra (ANEXO A), quando define que um Estado, durante o estudo, preparação, aquisição ou adoção de uma nova arma, de novos meios ou de um novo método de guerra, tem a obrigação de determinar se o seu emprego seria proibido, em algumas ou em todas as circunstâncias, pelas disposições do citado Protocolo ou por qualquer outra regra do DI.

8 O conceito de cibernéticas será melhor aprofundado ao longo do presente trabalho.

9 Informação obtida na entrevista do assessor jurídico do CICV, Laurent Gisel. Disponível em: <http://www.icrc.org/por/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm>. Acesso em: 29 jul. 2014.

Verifica-se, portanto, que a atual legislação não limita e não restringe novas tecnologias e amplia para a responsabilidade dos Estados o cumprimento fiel do DI.

2.2 Perspectivas Futuras

Os meios e métodos de Guerra estão sempre em constante evolução desde que as Convenções de Genebra (1949) foram criadas, entretanto, o DI é o ordenamento jurídico aplicável às ações implementadas pelas partes durante um conflito armado. Deve-se atentar ao fato de que poderá haver necessidade de desenvolvimento de normas e regulações que garantam a proteção necessária para os civis, à medida que novas tecnologias, como por exemplo as cibernéticas, evoluam ou que se entendam efetivamente o seu impacto sobre a humanidade (GISEL, 2013). Para suprir esta necessidade, no quarto capítulo será feita uma análise do Manual de *Tallinn*, pois representa uma nova normatização nos assuntos cibernéticos.

Com o objetivo de possibilitar um melhor encadeamento de ideias, a fim de melhor exemplificar estes conceitos, no próximo capítulo será feito um detalhamento das novas tecnologias chamadas cibernéticas e sua relação com o DI.

3 A GUERRA CIBERNÉTICA

A Guerra, fruto do desenvolvimento tecnológico dos tempos modernos, tem apresentado novos métodos e ferramentas que geram dúvidas a respeito do real potencial destrutivo. Neste contexto, centrado em incertezas, encontra-se a possível existência da chamada Guerra Cibernética!

Este capítulo tem como objetivo definir e classificar a GCiber quanto ao seu emprego; analisar os conceitos e definições da GCiber; caracterizar as ações cibernéticas e seus principais agentes além de relacionar os métodos e técnicas a serem utilizados nos ataques cibernéticos.

3.1 Definição de Guerra Cibernética

Guerra pode ser definida como: “a luta durante certo lapso de tempo entre forças armadas de dois ou mais Estados, sob a direção dos respectivos governos” (ACCIOLY; SILVA; CASELLA, 2002, p. 470).

O nascimento da Cibernética como Ciência está associado aos trabalhos de Norbert Wiener (1894-1964) que durante a Segunda Guerra Mundial (1939-1945) foi encarregado pelo governo norte-americano de resolver os problemas de controle automático de direção de tiro. Wiener alcunhou o termo cibernético do grego “kybernetiké”, que significa “a arte de governar um barco” e, posteriormente ampliou a definição para a “ciência do controle e da comunicação entre os seres vivos e as máquinas” (FILHO, 2007, p. 137).

Verifica-se que as duas definições acima estão alinhadas à definição de Guerra Cibernética segundo a especialista jurídica do CICV, Cordula Droege[10](2011), quando afirma:

10 Cordula Droege fez parte do grupo de especialistas que elaboraram o Manual de *Tallinn*. Entrevista concedida ao CICV Disponível em:<http://www.icrc.org/por/resources/documents/interview/2011 /cyber-warfare-interview-2011-08-16.htm> Acesso em: 25 jul 2014.

“são os meios e métodos de guerra que contam com informações tecnológicas e são usados no contexto de um conflito armado”, nesta mesma linha de raciocínio, a ONU (2011) define GCiber como o uso de computadores ou meios digitais por um Estado, ou com o seu conhecimento e aprovação explícita, contra outro Estado ou contra a propriedade privada de outro Estado, incluído: acesso intencional, a interceptação de dados ou danos a infraestrutura digital e o controle digital, a produção e distribuição de dispositivos que podem ser utilizados para destruir as atividades domésticas[11].

Nota-se que nas definições apresentadas se fazem presentes as expressões: “entre Estados” e “Conflito Armado” que evidencia o fato da consideração destes dois elementos na caracterização de uma operação cibernética como uma ação de Guerra propriamente dita.

Face ao que foi exposto e ao levar em consideração o que foi abordado no capítulo anterior, surgem alguns questionamentos que este trabalho tem o propósito de elucidar. Quando uma GCiber se configura à luz da legislação internacional e quando ela pode ser considerada um conflito armado?

Para obter a resposta, a seguir, serão mencionados alguns conceitos com o propósito de caracterizar a GCiber que auxiliará a identificação das suas capacidades e limitações.

3.2 Ações Cibernéticas

A Marinha do Brasil (MB) trata do assunto ao considerar ações cibernéticas como: ofensivas e defensivas destinadas a explorar, danificar ou destruir informações digitais, ou ainda negar o acesso às suas informações (BRASIL, 2007, p.1-3). Para isto utilizam-se de sistemas de informação e de redes de computadores. Definição alinhada com a Doutrina de

11 Resolução 1113 (2011) do Conselho de Segurança da ONU. Disponível em: <http://www.upeace.org/ upmun c/2011/pdf/SC%20Cyberwarfare.pdf>. Acesso em: 27 jun. 2014.

Operações Conjuntas que as dividem em três tipos de ações: a Exploração Cibernética, o Ataque Cibernético e a Proteção Cibernética (BRASIL, 2011, p.1-3).

A Exploração Cibernética consiste em ações de busca, nos Sistemas de TI de interesse, a fim de obter dados, de forma não autorizada, para a produção de conhecimento e/ou identificar as vulnerabilidades desses sistemas. O Ataque Cibernético compreende ações para interromper, negar, degradar, corromper ou destruir informações armazenadas em dispositivos e redes computacionais e de comunicações do oponente e a Proteção Cibernética abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações além de incrementar as ações de Segurança Cibernética em face de uma situação de crise ou conflito armado. Os principais atores envolvidos nestas ações serão identificados no próximo item.

3.3 Atores cibernéticos e seus métodos de ataque

Jason Andress e Steve Winterfeld, em "Cyber Warfare"(2011), consideram que os "soldados cibernéticos"[12] são divididos em atores estatais e não-estatais. Os estatais geralmente são os atores que representam a maior ameaça. Eles estão a serviço de um Estado e, não necessariamente, fazem parte de uma força armada. Possuem recursos, disciplina, são recrutados e treinados, além de dispor de capacidade de planejamento para grandes ataques. Têm o poder para fornecer e receber dados de inteligência e meios para obter informações de vulnerabilidades de seus possíveis alvos. Podem ter claras razões para atacar outros Estados e normalmente compreendem e respeitam as regras e leis estabelecidas no DI.

Os não estatais são aqueles que, como o próprio nome diz, não estão a serviço de um Estado, são subdivididos em: *script kiddies, malware authors, scammers, blackhats, hacktivists, and patriot hackers* (ANDRESS; WINTERFELD, 2011): *Script Kiddies* ("Garoto

12 O autor considera também a expressão "Guerreiros Cibernéticos".

do *scripts*") são muitas vezes os menos qualificados, mas o mais comum dos atacantes não-estatais. O termo é usado para descrever alguém sem nenhuma habilidade especial no ataque de sistemas, geralmente usam *scripts*[13] e ferramentas simples que foram escritas por outras pessoas, a fim de realizar seus ataques. Suas ações são muitas vezes bem-sucedidas, em grande parte devido ao mau Estado de segurança nos sistemas que serão atacados e à quantidade de ferramentas de penetração disponíveis; os *Malware Authors* ("Autores de *malware*") *s*ão aqueles do tipo muito especializado. Os atacantes que realmente escrevem originais de *malware*[14], com certa dose de habilidade, será necessário conhecimentos de programação e dos sistemas operacionais de destino; os *Scammers* ("Golpista") *s*ão considerados os mais "baixos" dos "baixos" quando se trata de atacantes, não possuem habilidades técnicas com ferramentas de ataque, pois preferem preferem outros métodos de obtenção de informações. São chamados de "golpistas" porque utilizam de artifícios de Engenharia Social[15], com o objetivo de enganar suas vítimas e assim obter as informações que desejam; os *Blackhats* ("Chapéu preto") *s*ão os "bandidos" do mundo *Hacker* e geralmente não têm cuidado especial com regras e leis e nem com os efeitos nocivos que seus ataques podem causar. *Blackhats* se distinguem dos *Whitehats* ("Chapéu branco"), os "mocinhos", que são frequentemente encontrados trabalha para frustrar os esforços dos *Blackhats* e *Greyhats* ("Chapéu cinza"), aqueles que estão em processo de transição. Os *Blackhats* possuem um certo nível de habilidade em atacar e explorar os sistemas e redes e podem ser motivados tanto para a realizar seus ataques apenas pela emoção de explorar um sistema como também, de uma maneira mais técnica e planejada, em penetrar em sistemas complexos e usá-los para atacar outros dispositivos na mesma rede; os *Hacktivists*

13 *Script* é um conjunto de instruções em código, ou seja, escritas em linguagem de computador, que executa diversas funções no interior de um programa de computador.

14 Palavra originária do inglês *Malicious software* (software malicioso). Existem vários tipos de códigos maliciosos como: vírus, vermes, *phishing, rootkits*, cavalos-de-tróia e *spyware*.

15 Engenharia Social é a técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. É considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido "conto do vigário" utiliza engenharia social.

(Hacktivistas) são, em essência, os *Hackers*[16] que usam seus conhecimentos para dar suporte a um determinado ponto de vista ou ideal. Hacktivismo se define como o uso não violento, legal ou ilegal de ferramentas digitais em busca de objetivos políticos. As ferramentas do hacktivista incluem: desconfiguração ("pichação") de *Website*[17], envio de *e-mail* em massa, *Denial of Service* (DoS)[18] ou ataques *Distributed Denial of Service* (DDoS)[19] e sequestro de *Domain Name Service* (DNS)[20]. A motivação do *Hacktivist* é orientada de alguma forma por interesses, sempre focados em influenciar opiniões. Causas que são defendidas por hacktivistas: a liberdade de expressão, direitos civis, direitos religiosos, direitos sociais, humanitários e políticos. Definição compartilhada por Bayuk, Jennifer L. e*t al*, no *Cyber Security Policy Guidebook* (2012), quando os definem como uma junção de *Hack* e *Activist* capaz de escrever código fonte[21] e manipular *bits*[22] para atingir seus objetivos. Os atos de hacktivismo são motivados pela crença de que o uso de seus códigos terá efeitos semelhantes aos do ativismo comum ou manifestações civis (ANDRESS; WINTERFELD, 2011; BAYUK *et al*; 2012).

Os *Patriot Hackers* (*Hackers* Patriotas) podem ser considerados como um subconjunto de Hacktivistas. Eles utilizam as mesmas ferramentas e métodos, mas geralmente

16 Hacker é o ator mais conhecido e difundido nos dias de hoje. O responsável por encontrar soluções não convencionais e não triviais para problemas e para isso, deve ser alguém possuidora de conhecimentos técnicos cuja paixão é inventar programas e desenvolver novas formas de processamento de informação.

17 Website é o sistema de documentos reunidos de várias mídias num suporte computacional, implementado por sistemas eletrônicos de comunicação que são interligados e executados na *internet*.

18 Negação de Serviço. Atividade maliciosa pela qual um atacante utiliza um computador ou dispositivo móvel para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

19 Consiste em ataques de negação de serviço distribuído realizado com o uso de uma rede de computadores sob controle do atacante (botnet). Bot é um Programa que, além de incluir funcionalidades de vermes, dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. O processo de infecção e propagação do bot é similar ao do worm, ou seja, o bot é capaz de se propagar automaticamente e explorar vulnerabilidades existentes em programas instalados em computadores. Botnet é a rede formada por centenas ou milhares de computadores infectados com bots. Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de spam, etc.

20 Do inglês Domain Name System. O sistema de nomes de domínios, responsável pela tradução, entre outros tipos, de nome de máquinas/domínios para o endereço IP correspondente e vice-versa.

21 Código fonte é o conjunto de palavras ou símbolos escritos de forma ordenada que contém instruções em uma das linguagens de programação existentes, de maneira lógica.

22 Bit (simplificação para dígito binário, "BInary digiT" em inglês) é a menor unidade de informação que pode ser armazenada ou transmitida. Usada na Computação e na Teoria da Informação. Um bit pode assumir somente 2 valores, por exemplo: 0 ou 1, falso ou verdadeiro respectivamente.

tomam as ações, em prol de um determinado Estado com um foco mais nacionalista, embora não no sentido oficialmente patrocinado. Em algumas ocasiões, eles geraram rumores de que tenham desempenhados atividades a serviço de um Estado, inclusive com remuneração para realizar tais atividades. Uma dessas ocasiões, em dezembro de 2009, envolveu o roubo e publicação de milhares de *e-mails* da Universidade de *East Anglia*, unidade de pesquisa climática. Foi creditado que os atacantes envolvidos no incidente agiram em nome da Rússia, a fim de desacreditar a necessidade de redução das emissões de carbono para ajudar a combater o aquecimento global (ANDRESS; WINTERFELD, 2011). Suas atividades geralmente são de natureza mais precisa e dirigida do que as dos Hacktivistas.

Outro fato que merece destaque é o de que não são categorias excludentes, os atores envolvidos podem atuar em várias atividades ao mesmo tempo. O ANEXO B amplia esses conceitos e apresenta as fontes de ameaças representadas por esses atores, suas respectivas motivações e as possíveis consequências.

3.4 Repercussões da Guerra Cibernética

Verifica-se que os dois atores possuem capacidades técnicas, motivações diversas e conhecimentos que podem fazer com que pessoas, bens e IEC sejam facilmente atingidos com a possibilidade de gerar danos catastróficos, fato constatado pela total dependência de sistemas informacionais do tipo *Supervisory Control and Data Acquisition* (SCADA)[23] (CLARKE; KNAKE, 2010). Quando esses sistemas ou as redes de um Estado sofrem ataques, os serviços básicos como abastecimento de água potável, assistência médica e eletricidade podem ser interrompidos, além da possibilidade de interferência no funcionamento de infraestruturas vitais como represas, diques ou usinas nucleares. O bem-estar, a integridade

23 Sistema de Supervisão e Aquisição de Dados é o *software* que controla redes de sistemas de infraestruturas crítica. Possui capacidade de juntar e analisar dados em tempo real.

física ou até a vida de milhões de pessoas podem ser seriamente afetados. O ataque mais repercutido na comunidade internacional foi o do verme *Stuxnet*, em uma instalação nuclear em *Natanz* em 2010, que danificou as capacidades do Irã no enriquecimento de urânio que causou danos em suas centrífugas (ANDRESS; WINTERFELD, 2011).

Ao se analisar as potencialidades dos ataques cibernéticos, resta saber em que contexto esses atores desempenharão suas ações. Se ocorrerão durante um conflito entre Estados, como descrito nas definições de Guerra, ou se surgirão por motivações diversas, como as ações desempenhadas pelos *Hacktvistas*. Se foram originadas por combatentes ou por não combatentes. Cabe ressaltar que mesmo os atores não estatais podem ser responsabilizados e punidos por seus atos, pois a proteção de atacar civis cessa quando eles participam diretamente nas hostilidades, mesmo que não sejam membro de uma força armada ou a serviço de um Estado (DEYRA, 2001).

Conforme observado no capítulo anterior, todas as partes envolvidas em conflito devem tomar precauções constantes para a proteção de civis, pois regras e limites devem ser seguidos com aplicação direta a todos os meios e métodos de guerra. Está aí o fato de os especialistas (GISEL, 2013) reafirmarem a relevância do DI a essa nova tecnologia, já que é crucial para identificar formas de limitar o potencial custo humanitário das operações cibernéticas em conflitos armados.

Neste sentido, com o objetivo de implementar as tomadas de precauções a fim de reduzir o impacto negativo em vidas humanas, vale reproduzir a seguir o comentário final que foi extraído do livro verde[24] da Defesa e que serve de base para a compreensão de algumas medidas recentemente adotadas por alguns Estados, que serão exploradas no próximo capítulo, com a criação de uma referência jurídica denominada “Manual de Tallinn”:

24 Livro verde é uma publicação do Departamento de Segurança da Informação e Comunicações da Presidência da República que contém diretrizes estratégicas para formulação da Política Nacional de Segurança Cibernética no Brasil.

> As emergentes ameaças cibernéticas mostram o quanto é preciso incrementar tanto a segurança da informação quanto a cooperação internacional no sentido de evitar ou reduzir efeitos negativos de operações cibernéticas antagônicas. O tema ameaça cibernética deve ser resolvido em escala mundial, envolvendo o maior número de partes, de leis, e de agências de todas as Nações. Convenções têm de ser reescritas uma vez que a guerra cibernética confunde princípios como os da proporcionalidade, neutralidade e distinção. As regras cibernéticas necessitam ser melhor discutidas. (HEICKERO, 2010 citado por BRASIL, 2010, p. 51, tradução do autor).

A fim de melhor exemplificar esses conceitos e verificar como podem ser contextualizados no ramo do DI, o próximo capítulo passará a descrever possíveis cenários à luz do documento chamado "Manual de Tallinn" que surge em encontro com a necessidade exposta de se discutir melhor o tema, principalmente em fóruns internacionais. Giles (2014) cita que existe uma tendência mundial de debates internacionais para tratar do direito nas ações cibernéticas.

4 O MANUAL DE TALLINN

> Um dos desafios que os Estados enfrentam no contexto de ciberguerra tem a ver com a abrangência e forma de aplicabilidade do direito internacional nas operações de ciberguerra onde as ideias de ataque ou defesa se mantêm instáveis desde o seu advento. (SCHMITT *et al,* 2013, p. 17)[25].

4.1 Processo de criação

O *Cooperative Cyber Defense Center of Excellence*[26] (CCDCOE), a convite da Organização do Tratado do Atlântico Norte (OTAN), em 2009, formou um grupo independente de especialistas para elaborar o *Tallinn Manual on the International Law Applicable to Cyber Warfare*[27], projeto que contou com o patrocínio e colaboração de 11 Estados[28] e teve como abordagem principal os aspectos jurídicos da GCiber. Foi considerada a primeira orientação do mundo sobre a aplicação do DI vigente para a GCiber, além de ter sido proposto como a referência para consultores jurídicos nas agências governamentais.

A capital da Estônia aparece no título não é por acaso, o CCDCOE foi criado em 2008, um ano depois da cidade ter sofrido um dos ciberataques mais expressivos. O ataque surgiu em decorrência da decisão do governo de remover os corpos de alguns soldados soviéticos e o monumento do Soldado de Bronze, símbolo da ocupação soviética durante a Segunda Guerra Mundial, do centro de *Tallinn* para o cemitério das Forças Armadas. Moscou interpretou o assunto como uma atitude desumana e passou a ameaçar com sanções econômicas o seu vizinho báltico (CLARKE; KNAKE, 2010, p. 21). Na ocasião, Estônia

---

25 Michael N. Schmitt é o diretor do projeto de criação do Manual e presidente do Departamento de Direito Internacional da *U.S. Naval War College* (Escola de Guerra Naval dos EUA).

26 Centro de Excelência Colaborativa de Defesa Cibernética (tradução nossa). *NATO Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE) foi formalmente criado em 14 maio 2008, a fim de aumentar a capacidade de defesa cibernética da OTAN. Localizado em *Tallinn*, na Estônia, o Centro representa um esforço internacional com a participação de: República Checa, Estônia, França, Letônia, Lituânia, Alemanha, Hungria, Itália, Polônia, Eslováquia, Espanha, Holanda, Reino Unido e Estados Unidos como nações patrocinadoras e Áustria como colaborador.

27 Manual de *Tallinn* – sobre o Direito Internacional aplicável à Guerra Cibernética.

28 Estônia, Alemanha, Hungria, Itália, Letônia, Lituânia, Países Baixos, Polônia, Eslováquia, Espanha e Estados Unidos.

declarou-se a primeira vítima de um ciberataque. O Estado teve seus servidores sobrecarregados o que impossibilitou o uso de sistemas bancários online, sítios de jornais e de serviços governamentais (CLARKE; KNAKE, 2010, p. 22). O que aconteceu na Estônia foi um ataque DDoS e, na ocasião, houve a acusação de que a Rússia teria originado o ataque[29]. Entende-se que a criação deste Centro de Excelência foi uma resposta direta da OTAN a este ataque, mesmo que, na ocasião, não tenha sido identificado o seu respectivo autor.

O grupo de especialistas foi formado por 20 advogados civis e militares influentes de países da OTAN, peritos técnicos no domínio da Segurança Cibernética, representantes do Ciber Comando dos Estados Unidos da América (EUA) e também do CICV, conforme descrito na introdução do Manual (SCHMITT *et al*, 2013).

O trabalho resultou em um conjunto de 95 regras relacionadas aos conflitos com o uso das Tecnologias da Informação e Comunicação (TIC)[30], além de descrever os meios e métodos de ataque, correlacionando-os com os princípios jurídicos internacionais aplicáveis a cada um deles.

4.2 Relacionamento com o Direito Internacional

Seus autores enfatizam a ideia de que o Manual apresenta ser uma publicação normativa baseada na legislação vigente, uma interpretação do DI nas ações cibernéticas e não se tratar de uma nova regulação internacional. Schmitt (2013b), em entrevista[31], momentos antes do seu lançamento, declarou: “Todo mundo está vendo a internet como o

29 EURONEWS. Disponível em: < http://pt.euronews.com/2007/05/01/russia-e-estonia-nao-ultrapassam-crise-monumental/>. Acesso em: 27 jun. 2014.

30 As Tecnologias da Informação e Comunicação ou TIC correspondem a todas as tecnologias que interferem e mediam os processos informacionais e comunicativos dos seres. Podem ser entendidas também como um conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de *hardware, software* e telecomunicações, a automação e comunicação dos processos de negócios, da pesquisa científica e de ensino e aprendizagem.

31 Entrevista concedida à *ABC NEWS*. Disponível em: http://abcnews.go.com/International/arming-virtual-battle-dangerous-rules-cyberwar/story?id=18888675&page=2 e http://www.federalnewsradio.com /86/3038173/In- Depth-interviews---September-14. Acesso em: 24 jul. 2014.

Oeste selvagem […] O que eles esquecem é que o direito internacional se aplica a armas cibernéticas como a qualquer outro tipo de arma".

Por outro lado, a Rússia defende uma posição contrária ao Ocidente. O porta-voz do Ministério da Defesa russo Konstantin Peschanenko saiu com uma declaração nesse sentido, em abril de 2013, quando disse que: "enquanto a Rússia está tentando impedir a militarização do ciberespaço, exortando a comunidade internacional a adotar um código de conduta neste domínio, os Estados Unidos e seus aliados já estão aceitando as regras para processar a Guerra Cibernética" (CHERNENKO, 2013, p.1, tradução nossa; GILES[32], 2014).

Verifica-se que um grande limitador para que a norma possa um dia ser universal, em forma de tratado, é o fato de que somente representantes de Estados pertencentes à OTAN fizeram parte do grupo que ficou responsável pela sua elaboração. Giles (2014) argumenta que potenciais adversários no ciberespaço, como Rússia e China, não foram incluídos como colaboradores na elaboração do documento. A Rússia defende que devem ser realizados esforços não para regular a GCiber, mas sim para a proibição de sua utilização (GILES, 2014). Verifica-se que os dois lados em oposição entram em consenso, aparentemente, na não necessidade de nova regulação internacional.

A citada publicação normativa não é um documento oficial e também não é a doutrina regular da OTAN (SCHMITT *et al*, 2013), entretanto, enquanto permanece a discussão, ela continua a ser tratada como uma compilação de opiniões de especialistas no assunto que, de certa maneira, servirá para legitimar os casos em que for aplicada, principalmente quando estiverem envolvidos membros da OTAN. Seus autores afirmam que se trata de uma interpretação do DI vigente (SCHMITT *et al*, 2013). Premissa essa que será considerada no decorrer deste trabalho.

32 Keir Giles é o diretor do *Conflict Studies Research Centre (CSRC)*, um grupo de *experts* vinculado ao Ministério da Defesa do Reino Unido.

4.3 Regras

A maior parte das regras é dedicada a ataques cibernéticos que acompanham o conflito armado tradicional, adaptado às especificidades do espaço cibernético, além de outras disposições legais. O estabelecimento das regras permite uma visualização hipotética de possíveis cenários em que a GCiber pode ser aplicada.

Para melhor ilustrar estas afirmativas, foram selecionadas algumas regras (SCHMITT *et al*, 2013, tradução nossa) que abordam este tipo de aplicação com a respectiva análise limitada ao teor de conteúdo proposto neste trabalho:

a) Regra 5: "Um Estado não deve conscientemente permitir que as infraestruturas cibernéticas, situadas no seu território ou sob seu controle governamental exclusivo, possam vir a ser utilizadas para atos que causem prejuízos ou danos ilegais a outros Estados";
b) Regra 7: "se uma ciberoperação teve origem em uma rede governamental, isto não é uma evidência suficiente para atribuir a operação ao Estado, entretanto, tal fato passa a ser um indicador que aquele Estado em questão está associado com a operação";
c) Regra 11: "definição do uso da força: uma ciberoperação se constitui como uso da força quando sua escala e feitos são comparáveis a uma operação convencional".
d) Regra 13: "Autodefesa contra um ataque armado: Um Estado que seja alvo de uma operação cibernética, de mesma potencialidade e nível de um ataque armado, pode exercer o seu direito inerente de legítima defesa";
e) Regra 22: "Um conflito armado Internacional existe sempre que houver hostilidades entre dois Estados ou mais, podendo ser incluídas ou limitadas por ciberoperações";
f) Regra 30: "Definição de Ataque Cibernético: O manual define que um ataque

cibernético é uma operação, seja ofensiva ou defensiva, que é passível de causar lesão, morte a pessoas ou dano e destruição de objetos";

g) Regra 80: "A fim de evitar prejuízos graves para a população civil, um cuidado especial deve ser tomado durante os ataques cibernéticos contra determinadas instalações especiais, como: barragens, diques e estações geradoras elétricas nucleares, bem como suas vizinhanças".

Observa-se que um Estado pode ser responsabilizado pelos ataques realizados no seu território ou com a utilização de sua infraestrutura, mesmo que esteja localizada em um outro Estado. Por exemplo: se um grupo de *hackers,* com base no Estado hipotético Branco, receber instruções, treinamento e infraestrutura governamental de AZUL, realizar ataques DDoS infecta computadores em PRETO, a responsabilidade poderá ser atribuída para AZUL, de acordo com a Regra 5.

Ao considerar um outro cenário, relacionado ao possível financiamento de *hackers* estrangeiros envolvidos em sabotagem contra um determinado sítio governamental, nota-se que não pode ser considerado como um ataque cibernético pois não se trata de uma operação ofensiva que seja passível de causar lesão, morte a pessoas, de acordo com a Regra 30. As operações cibernéticas psicológicas que não levam à destruição e que são exclusivamente destinadas a minar a credibilidade das estruturas de governo e econômico não podem ser descritas também como deste tipo. Tal fato fica evidenciado nas atividades de atores não estatais, como os *Hacktivists* e os *Patriot Hackers,* entretanto, se esses atores passem a participar diretamente das hostilidades com a realização de ataques cibernéticos em apoio a uma parte em conflito, eles passam a perdem a sua proteção, conforme visto no capítulo anterior.

É importante observar que os conceitos acima explorados envolvem uma

tendência de separação entre os mundos cibernéticos (ou virtuais) e cinéticos (ou reais), principalmente quando surge o questionamento a respeito da problemática da qualificação de um ciberataque como um ataque armado. As regras 11 e 13 tratam de uso da força e ataque armado e serão tratadas detalhadamente a seguir.

4.4 Ataque Cibernético como Ataque Armado

Michael N. Schmitt, em finais da década de noventa, criou seis critérios para avaliar em que medida um ciberataque pode ser considerado um ataque armado. São os chamados "Schmitt-Criteria" que foram novamente apresentados na "*4th International Conference on Cyber Conflict" (2012)*[33] em evento coordenado pela OTAN, são eles:

a) gravidade (*severity*): os ataques armados ameaçam danos físicos e destruição da propriedade num grau muito mais elevado que outras formas de coerção;
b) iminência (*immediacy*): as consequências negativas de uma ação armada ou as ameaças das mesmas geralmente ocorrem com mais rapidez do que outras formas de coerção;
c) caráter direto (*directness*): as consequências de uma coerção armada estão mais diretamente ligadas ao *actus reus* (ato de culpabilidade), do que outras formas de coerção que dependem de vários fatores para atuar;
d) caráter invasor (*invasivness*): na coerção armada, o ato que provoca danos normalmente traduz-se num atravessar da fronteira nacional, enquanto que os atos de Guerra econômica geralmente ocorrem fora das suas fronteiras;
e) mensuralidade ou extensão (*measurability*): enquanto que as consequências de uma

33 CCDOE-NATO, (2012), Disponível em: <http://www.ccdcoe.org/publications/2012proceedings/5_3_Ziolkowski_IusAdBellumInCyberspace.pdf.p. 300-301 > .Acesso em: 14 maio 2014.

ação armada são geralmente fáceis de verificar (por exemplo, certo nível de destruição), as consequências de outras formas de coerção são mais difíceis de definir;

f) legitimidade (*presumptive legitimacy*): na maioria dos casos, o uso da força, seja sob o prisma da lei doméstica ou da lei internacional, é presumivelmente ilegal, exceto se estivermos perante uma disposição que a permita.

Observa-se que os requisitos denominados "Schmitt-Criteria" auxiliam a identificação de quando uma ação cibernética pode ser qualificada como uso da força quando se faz uma comparação da ação propriamente dita com as especificidades características de um ataque armado que é mais visível. O conceito teórico passou a ser ampliado no manual (SCHMITT *et al,* 2013) e passou a ser acrescido de mais dois requisitos na análise:

g) Caráter Militar (*Military Character*): A ligação entre a operação cibernética em questão e as operações militares aumenta a probabilidade de caracterização como uso da força. Esta afirmação é apoiada pelo conceito de uso da força ter sido tradicionalmente entendido como implica força empregada pelas forças armadas militares;

h) Envolvimento do Estado (*State Involvement*): O grau de envolvimento do Estado em uma operação cibernética se encontra ao longo de uma percepção continuada de operações realizadas por um Estado em si (por exemplo, as atividades de sua forças ou as agências de inteligência). Quanto mais clara e mais próxima de uma ligação entre um Estado e as operações cibernéticas, mais aumentará a probabilidade de percepção de que outros Estados as caracterizem como uso da força.

Ao ser constatado uma ação cibernética como uso da força, implicações do DI poderão ser impostas, inclusive com a possibilidade de avocar a legitima defesa. Cada caso é

um caso e deve ser analisado separadamente, entretanto, nota-se que tais requisitos facilitam esta distinção. Aliado a esse conceito, o manual enfatiza que o limite está na escala e consequências (perda de vidas, danos ou destruição).

O ataque cibernético, em tempo de paz, pode ser equiparado ao uso da força ou ataque armado, e, assim, permite que um Estado tenha o direito de se autodefender, inclusive com a possibilidade de utilização de armas convencionais, conforme observado no segundo capítulo e na regra 13 do manual.

Cabe ressaltar que, em algumas ocasiões, os Estados Unidos da América interpretaram um ataque preventivo e preemptivo como argumento justificador para o uso da força em legítima defesa. Tal comportamento ficou evidenciado na chamada "Guerra ao Terror"[34] [e] na Doutrina Bush[35] (BYERS, 2007). Na ocasião, no contexto da Segunda Guerra do Golfo (2003), a possibilidade de existência de armas de destruição em massa foi um dos motivos justificador para os EUA alegar um ataque preventivo ao Iraque, inclusive com a utilização de ataques convencionais.

Ainda resta esclarecer uma questão jurídica importante: qualificar uma operação cibernética como uso de força não é ainda a circunstância autorizadora do uso da violência física como exercício da legítima defesa, pois a Carta das Nações Unidas, ao discipliná-lo, diz se referir a uma resposta a um "ataque armado"[36].

Por outro lado, a regra 11 consolida o conceito de que uma ciberoperação pode sim ser considerada como uso da força, na medida que os danos sofridos por ciberataques for equivalente aos prejuízos causados por ataques convencionais.

34 Trata-se de uma Guerra idealizada pelos Estados Unidos identificada como uma "cruzada mundial contra o terror" em defesa da "paz mundial" e da sua segurança interna. O terrorismo, os governos que lhe dão apoio e abrigo e os países que desenvolvem armas de destruição em massa e que contestam o poder norte-americano, foram colocados como os principais alvos. Passaram a ser classificados em um agrupamento denominado "Eixo do Mal". Num primeiro momento, de forma declarada, constavam neste grupo: o Iraque, o Irã e a Coreia do Norte.

35 Teve origem em consequência dos atentados de 11 set. 2001. Trata-se de nova Estratégia de Segurança Nacional dos Estados Unidos da América. O documento rejeita categoricamente a necessidade de uma ameaça iminente. Considera ações antecipatórias de autodefesa, mesmo sem o aval de organismos internacionais como a ONU.

36 Artigo 51 da Carta das Nações Unidas.

Assim, ao analisar o exposto, é possível que uma operação cibernética seja ilegal para o DI, sem que o Estado ofendido possua o direito de responder com violência física. O grande fator diferencial nesta caracterização será a responsabilidade dos Estados envolvidos e a potencialidade dos danos sofridos.

4.5 Estabelecimento de responsabilidade aos Estados

O Manual de Tallinn lida com a questão de invocar a responsabilidade do Estado pelos atos de seus nacionais. Neste sentido, a regra de responsabilização do Estado por atos de particulares está expressa no artigo 8º do Projeto da Comissão de Direito Internacional das Nações Unidas Sobre a Responsabilidade Internacional dos Estados que considerar-se-á ato do Estado a conduta de uma pessoa ou grupo de pessoas se esta pessoa ou grupo de pessoas estiver de fato em ação por instrução ou sob direção ou controle daquele Estado, ao executar a conduta (ACCIOLY; SILVA; CASELLA, 2002). Até aqui fica clara a questão da interpretação da lei alinhada com os interesses próprios dos atores envolvidos. Como exemplo: caso se deseje legitimar um possível ataque, em retaliação a um ataque cibernético sofrido, se tentará enquadrar como legítima defesa, conforme visto na regra 13, para assim invocar a Carta da ONU e, para isto, terá que se responsabilizar os ataques a um Estado, pois somente assim o revide seria legítimo. A responsabilidade do Estado poderá ser alcançada quando se conseguir atribuir que pessoa ou grupo de pessoas estejam em ação por instrução ou sob direção ou controle daquele Estado, pessoas que podem ser atores estatais ou não estatais no contexto de uma GCiber.

4.6 Perspectivas futuras

Como foi observado, vimos que existe um único ciberespaço compartilhado por usuários militares e também por civis. A garantia de que os ataques sejam dirigidos somente contra objetivos militares e que haja o cuidado constante de poupar a população civil e a sua infraestrutura são os principais desafios. Os Estados devem ser extremamente cautelosos quando recorrem aos ataques cibernéticos.

Com o objetivo de inibir ações cibernéticas e tenta evitar danos incontroláveis, no próximo capítulo será verificado se o referido manual pode ser utilizado como uma ferramenta que contribui para uma estratégia de dissuasão.

5 ESTRATÉGIA DE DISSUASÃO

Neste capítulo será feita a apresentação de alguns conceitos de estratégia de dissuasão que permitam ser comparadas com a aplicabilidade do manual, para que assim seja possível responder ao principal questionamento deste trabalho.

5.1 Compreensão da Dissuasão Estratégica

O Glossário das Forças Armadas apresenta o seguinte conceito de dissuasão: "atitude estratégica que, por intermédio de meios de qualquer natureza, inclusive militares, tem por finalidade desaconselhar ou desviar adversários, reais ou potenciais, de possíveis ou presumíveis propósitos bélicos" (BRASIL, 2007).

O objetivo da dissuasão é desincentivar o início ou a efetivação de uma ação mais hostil, entendimento compartilhado por Goodman[37] (2010) quando define que o uso da estratégia de dissuasão reflete a tentativa de se evitar a necessidade de utilização do uso da força militar ou da agressão propriamente dita, e, desta maneira, pode-se utilizar mecanismos e artifícios para que eventuais agressores passem a tomar uma postura de desistência quanto a possibilidade de realização de ataques.

Mas quais são essas ferramentas e artifícios?

O mesmo autor define que a dissuasão cibernética possui oito características: o interesse, a declaração de dissuasão, as medidas de negação, as medidas de punição, a credibilidade, a confiança, o medo e o cálculo custo-benefício.

---

37 Will Goodman é um especialista no tema: Dissuasão Cibernética. Ele é assessor para assuntos de defesa no Senado americano. Foi citado em vários artigos e livros, dentre eles: *Nuclear Weapons in the Information Age* (Stephen J. Cimbala); *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy* (Thérèse Delpech) e *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World (*editado por Derek S. Revero).

Primeiramente, o Estado faz uma declaração de dissuasão para proteger seus interesses e faz com que possíveis agressores passem a adotar uma postura de não ataque.

As medidas de negação e punição são exatamente os componentes da dissuasão que apresentam o que pode acontecer caso a declaração não seja respeitada. A negação possui um aspecto defensivo de dissuasão e está dividido em dissuasão por prevenção e também por futilidade. Dissuasão pela prevenção significa que se um ataque é lançado, medidas defensivas interromperão o ataque em curso e a futilidade que mesmo que um ataque consiga violar suas defesas, ele não conseguirá ter o efeito desejado no alvo. Tanto a prevenção como a futilidade eficaz significam que os ataques vão inevitavelmente falhar e, assim, neste contexto, poderão servir para impedir a tentativa de ataque pelo agressor. A punição possui o aspecto ofensivo da dissuasão e consiste na retaliação, na interdependência e na contraprodutividade, como por exemplo: sanções, embargos ou até um revide na sua forma convencional.

A represália, entra neste contexto, pois, durante ou após um ataque, o defensor pode lançar um contra-ataque que imponha custos sobre o atacante que superem os benefícios obtidos com o ataque inicial. Interdependência e contraprodutividade são os termos menos familiarizados. Interdependência significa que tanto o atacante e o defensor possuem um interesse em comum. Quanto mais ambas as partes concordam com a comunhão de interesse, mais caro se torna um ataque para o atacante e defensor da mesma forma. Contraprodutividade relaciona objetivos táticos de um atacante com seus objetivos estratégicos. Um defensor pode convencer os potenciais agressores de que um ataque taticamente bem sucedido poderá frustrar os objetivos estratégicos. Por exemplo, se os Estados Unidos punir as famílias dos homens-bomba, os terroristas podem ser impedidos de atentados suicidas; no entanto, essa abordagem seria moralmente repugnante para os Estados Unidos (normativamente contraproducentes) e teria efeitos negativos sobre os objetivos mais

amplos dos EUA (estrategicamente contraproducentes). A retaliação, interdependência e contraprodutividade juntos compõem a dissuasão pela punição.

A credibilidade significa que a declaração efetuada é credível pelo inimigo, como um raciocínio lógico do cálculo do agressor sobre a capacidade da defesa. Por exemplo, ninguém acreditaria em uma ameaça de retaliação nuclear se um Estado possuir apenas capacidades convencionais. Para ser credível, um defensor também deverá ter a intenção de usar os recursos. Um atacante não questionaria se os Estados Unidos têm armas nucleares, por exemplo, mas um invasor pode questionar se os Estados Unidos usariam para retaliar contra um ataque convencional.

A confiança se estabelece ao agressor acreditar que, caso ele respeite o que está contido na declaração, não haverá um ataque e, portanto, lhe será assegurado que não sofrerá as punições declaradas pela dissuasão.

O medo consiste na baixa probabilidade de tomar uma ação indesejável devido a um possível ator hostil temer a negação ou as medidas de punição apresentadas.

Por último, garantia significa dar a um adversário uma razão para não realizar o ataque. Na maioria das vezes a garantia vem na forma de medidas de segurança. Em alguns casos, no entanto, pode significar outros benefícios vinculados, como a ajuda externa ou até um *status* comercial especial.

Estes elementos combinados, juntos, formam uma estratégia de dissuasão forte e eficaz. Resta saber de que maneira tudo isto pode ser implementado e como tudo isto pode estar relacionado ao contexto cibernético, abordagem principal deste trabalho.

Assim, a partir desta teoria, passaremos a analisar e verificar se o Manual de *Tallinn* apresenta características que estejam alinhadas aos conceitos e definições apresentados.

5.2 Características do Manual para a contribuição da dissuasão

O Manual teve sua criação logo após ter sofrido um ataque cibernético. Em uma resposta direta a este ataque, a OTAN mostrou ao mundo que aquela região agora passa a ter um centro de excelência no combate a possíveis ações cibernéticas adversas em uma clara demonstração de seus interesses na região, além do fato de gerar credibilidade em suas futuras ações. O documento possui uma vertente unilateral em contraponto às posições divergentes existentes entre alguns Estados, principalmente entre a Rússia e o Ocidente; estabelece regras, delimita e especifica o "Uso da Força" em alguns casos, define as medidas de punição e negação, bem como, pode gerar medo de sofrer represálias; teve sua divulgação formalizada e declarada que corresponde ao primeiro componente (declaração da dissuasão). O manual permite uma interpretação do DI vigente, o que confere legitimidade nos casos em que uma regra estabelecida seja violada, raciocínio validado pela consideração de que mesmo que não seja uma legislação universal, a atual cobertura jurídica possibilitaria sua aplicação. A confiança e a garantia ficam estabelecidas na medida que todas as regras e o DI sejam respeitados. Soma-se a estas características, o fato de frequentemente serem realizados exercícios práticos[38], em uma demostração de preparo e emprego da capacidade cibernética da OTAN.

Verifica-se que praticamente os aspectos acima mencionados estão relacionados diretamente com as oito características de Goodman, entretanto, existem outras teorias de dissuasão que podem confirmar ou rejeitar este conceito que não serão apresentadas neste trabalho pois será considerada a premissa de que esta é uma teoria válida. Não faz parte da

38 *Locked Shields* é um exercício, em tempo real, anual de defesa de ataques cibernéticos, organizado pelo CCDOE, que reúne cerca de 300 participantes de 17 países. Disponível em: <https://www.ccdcoe.org/international-cyber-defence-exercise-locked-shields-2014-begins-today-0.html>. Acesso em: 04 ago. 2014.

abordagem deste trabalho maiores detalhamentos de teorias de dissuasão e sim a verificação das características do Manual de *Tallinn* neste processo.

Em decorrência do que foi exposto, surge outro grande questionamento a ser abordado por este trabalho. O que acontece se a dissuasão falhar, como se desenrolariam os passos seguintes no contexto cibernético abordado no manual?

5.3 Implicações da aplicabilidade do manual em caso de falha na dissuasão

Para responder ao questionamento deve-se compreender que o limite entre a paz e a Guerra, nos conflitos ditos cibernéticos, estaria contido quando, na ocorrência de ataques, fossem causados sofrimentos e danos catastróficos ao Estado oprimido que, por sua vez, dentro de suas possibilidades, poderia adotar medidas para realização de um contra-ataque, que poderia ser de maneira convencional, armada, com o intuito de garantir sua integridade e soberania, conforme visto nos capítulos anteriores.

O Manual define e legitima, detalhadamente, esse revide, e passa a exercer papel essencial nessas considerações pois suas regras passam a tratar os possíveis cenários e as consequências decorrentes de ataques sofridos.

5.4 Considerações finais

A ameaça por dissuasão se torna uma ferramenta de paz e tranquilidade, uma vez que as ações ficam apenas nos discursos, o que não possibilita o escalonamento da crise. O maior exemplo disso é a dissuasão nuclear que manteve o mundo salvo na época mais dura da Guerra Fria (1945-1991).

Conforme observado no capítulo anterior verifica-se que têm ocorrido diversos ataques cibernéticos, contudo, ainda não foi possível atribuir a responsabilidade a nenhum Estado. Em outras palavras, ainda não foi possível falar na existência de uma Guerra Cibernética, entretanto, tal fato não significa que ela não venha ocorrer futuramente. A própria inexistência de um "conflito cibernético" até os dias de hoje reitera o fato de que, por enquanto, a dissuasão passa a ser uma peça fundamental na análise deste tipo de combate.

6 CONCLUSÃO

Diante da apresentação da estreita ligação entre o Direito Internacional na Guerra Cibernética e o Manual de *Tallinn*, visto que os dados coletados deixam claro que não se pode falar de uma sem a outra, procurou-se buscar os fatores em comum, o posicionamento dos atores e a análise dos diversos fatores que interferem nas relações entre os Estados.

Verificou-se que as Nações Unidas têm como propósitos as manutenções da paz e segurança internacionais e a busca constante na solução pacífica de controvérsias, entretanto, o direito inerente da legítima defesa individual ou coletiva pode ser avocado, no caso de ocorrência de um ataque armado contra um membro desta organização. Ao ser analisada outra vertente do DI, depreendeu-se que o Direito dos Conflitos Armados estabelece a proteção das vítimas e limitam os meios e os métodos de combate nas hostilidades e são aplicáveis a todas as situações. Ao se ampliar o alcance do DI para quaisquer ações hostis, reconheceu-se que não há necessidade de declaração formal de Guerra para o cumprimento desta vertente do DI.

Verificou-se que uma dessas situações em que o DI pode ser aplicado abrange as chamadas operações cibernéticas que para ser considerada uma ação de Guerra deverá estar inserida no contexto de um conflito armado entre Estados. Assim, a Guerra Cibernética surge como uma nova tecnologia de combate no contexto de um conflito armado e os Estados que a utilizem têm a obrigação de determinar se o seu emprego é proibido pelas disposições contidas no DI.

O Manual de *Tallinn* surge da necessidade de um ordenamento jurídico específico para as ações cibernéticas em busca da garantia da proteção necessária para os civis. Constatou-se que o documento é considerado a primeira orientação do mundo sobre a aplicação do DI vigente para a Guerra Cibernética. O trabalho consolida 95 regras relacionadas aos conflitos com o uso das Tecnologias da Informação e Comunicação e

descreve os meios e métodos de ataque, correlacionando-os com os princípios jurídicos internacionais aplicáveis a cada um deles. A análise do material coletado possibilitou verificar que as regras possibilitam uma visualização hipotética de possíveis cenários em que a Guerra Cibernética pode ser aplicada. Existe uma tendência de apresentar o manual como uma nova regulação internacional oficial, entretanto, seus autores enfatizam a ideia de que a norma é uma publicação baseada na legislação vigente, uma interpretação do DI nas ações cibernéticas.

Comparando as diferentes pesquisas abordadas foi possível constatar discordâncias e posicionamentos distintos em relação à legitimidade e à aplicabilidade do manual. Verificou-se que a Rússia defende uma posição contrária ao Ocidente por não apoiar a militarização do ciberespaço e pela existência exclusiva de representantes da OTAN na elaboração do manual, entretanto, os dois lados concordam que não há necessidade de elaborar uma nova regulação internacional oficial. A despeito dos diferentes pontos de vista apresentados, conforme demonstrado ao longo do estudo, a norma se define como uma compilação de opiniões de especialistas no assunto que servirá para legitimar os casos em que for aplicada.

Ao analisar as ameaças cibernéticas, verificou-se que os ataques são gerados tanto por atores estatais como não estatais que possuem capacidades técnicas, motivações diversas e conhecimentos que podem afetar o bem-estar, a integridade física e a vida de milhões de pessoas. A vulnerabilidade aos ataques está na dependência de sistemas do tipo SCADA que controlam as redes de IEC. Uma dificuldade apresentada no estudo foi qualificar uma ação cibernética como uso da força, análise evidenciada pela utilização dos requisitos evidenciados pelo conceito teórico denominado “Schmitt-Criteria”. Verificou-se que tal diferenciação depende da escala e consequências (perda de vidas, danos ou destruição) e envolvimento de Estados. Outra dedução importante advinda da pesquisa é o fato de que ao

ser constatado uma ação cibernética como uso da força, implicações do DI poderão ser impostas, inclusive com a possibilidade de avocar a legitima defesa que pode ser de maneira convencional.

No que concerne às tentativas de se evitar a necessidade de utilização do uso da força militar ou da agressão propriamente dita, verificou-se que estudiosos de dissuasão estratégica afirmam que o objetivo desta é desincentivar o início ou a efetivação de uma ação mais hostil por parte dos Estados, e, desta maneira, poderiam ser utilizados artifícios para que eventuais agressores passem a tomar uma postura de desistência na realização de ataques. Os fatores que mais contribuem para a utilização do Manual de *Tallinn* como ferramenta que contribui para a dissuasão foi o confronto com obras e partes de teorias dissuasórias. Ao ser utilizada a teoria de Goodman, um consagrado teórico de dissuasão cibernética, chegou-se a conclusão de que as características da aplicabilidade do Manual de *Tallinn* contemplam os oito aspectos da análise que conduz a uma estratégia dissuasória eficaz.

Portanto, com base nas considerações tecidas e nas análises efetuadas no desenvolvimento deste, estima-se que o trabalho atingiu o seu propósito ao validar a contribuição do Manual de *Tallinn* na dissuasão para solução de conflitos no espaço cibernético e também por estabelecer o limite para se considerar ato de Guerra e ensejar legítima defesa, que por sua vez, verificou-se que pode ser na forma de ataque convencional.

A própria inexistência de um "conflito cibernético" até os dias de hoje reitera o fato de que por enquanto a dissuasão cumpre seu papel fundamental e, neste contexto, o Manual de *Tallinn* se apresenta como um grande elemento nas tratativas de assuntos cibernéticos no Sistema Internacional.

REFERÊNCIAS

ACCIOLY, Hildebrando; SILVA, Geraldo E. do Nascimento e; CASELLA, Paulo B. *Manual de Direito Internacional Público*. 15. ed. São Paulo: Saraiva, 2002. 566 p.

ANDRESS, Jason; WINTERFELD, Steve. *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners.* Waltham: Syngress, 2011. 321 p.

BAYUK, Jennifer L *et al*. *Cyber Security Policy Guidebook.* New Jersey: Wiley, 2012. 288 p.

BRASIL. *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação***,** Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia, Admilson Gonçalves Júnior e Raphael Mandarino Junior. Brasília: GSIPR/SE/DSIC, 2010. 151 p. Disponível em: <http://dsic.planalto.gov.br/documentos/ publicacoes/ 2_Guia_SICI .pdf>. Acesso em: 23 jul. 2014.

_____ . Estado-Maior da Armada. *EMA 135 – Doutrina Básica da Marinha*. 1 rev. Brasília: 2014.

_____ . _____ . *EMA 416 – Doutrina de Tecnologia da Informação da Marinha.* 1 rev. Brasília: 2007.

_____. Segurança Cibernética no Brasil/ Gabinete de Segurança Institucional. *Livro verde*, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. Brasília: GSIPR/SE/DSIC, 2010. 63 p. Disponível em: <http:// dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 23 jul. 2014.

_____ . Ministério da Defesa. *MD35-G-01*. *Glossário das Forças Armadas*. 4. ed. Brasília: 2007.

_____ . _____ . *MD30-M-01*, *Doutrina de Operações Conjuntas*. 1 vol. Brasília: 2011.

BYERS, Michael. *A Lei da Guerra: Direito Internacional e Conflito Armado.* Rio de Janeiro: Record, 2007, 263 p.

CHERNENKO, Elena. *Russia warns against NATO document legitimizing cyberwars.* Kommersant Vlast, Moscou, 29 maio 2013. Disponível em: <http://kommersant.ru/doc/2193838>. Acesso em: 04 ago. 2014.

CLARKE, Richard A.; KNAKE, Robert K. *Cyber War: The next threat to National Security and what to do about it*. New York: Harper Collins, 2010. 290 p.

DARNSTAEDT, Thomas; ROSENBACH, Marcel; SCHMITZ, Gregor P. *Arming for Virtual Battle: The Dangerous New Rules of Cyberwar.* SPIEGEL, Berlim, 07 abr. 2013. Disponível em:<http://abcnews.go.com/International/arming-virtual-battle-dangerous-rules-cyberwar /story?id=18888675&page=2 e e h. Acesso em: 04 ago. 2014.

DEYRA, Michel. *Direito internacional humanitário.* Lisboa: Procuradoria-Geral da República/Gabinete de Documentação e Direito Comparado, 2001.

DROEGE, Cordula. *Não há brechas jurídicas no ciberespaço*. Genebra: 2013. Entrevista concedida ao CICV. Disponível em: http://www.icrc.org/por/resources/ documents/interview/ 2011/cyber-warfare-interview-2011-08-16.htm. Acesso em: 29 jul. 2014.

FILHO, Cléuzio F. *História da Computação: O caminho do pensamento e da tecnologia*. Porto Alegre: EDIPUCRS, 2007. 204 p.

GILES, Keir. *Legality in Cyberspace: An Adversary View – Russian Cyberspace Conflict Concepts and Initiatives*. Washington DC: U.S. Army War College (USAWC) Press publications, 2014, 93 p.

GISEL, Laurent. *Que limites o Direito da Guerra impõe sobre os ataques cibernéticos?* Genebra: 2013. Entrevista concedida ao CICV. Disponível em: <http://www.icrc.org/por/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm>. Acesso em: 29 jul. 2014.

GOODMAN, Will. *Cyber Deterrence: Tougher in Theory than in Practice? Strategic Studies Quarterly.*. Washington DC: Senate (United States) - Committe on Armed Services. 2010.135 p. Disponível em: < http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf>. Acesso em 29 jul. 2014.

KOLB, Robert; HYDE, Richard. *An introduction to the international law of armed conflicts*. Oxford-Portland: Hart Publishing, 2008.

ONU. Assembleia Geral. *The Charter of the United Nations*. Nova Iorque, ONU, 1945. Disponível em: <http://www.un.org/en/documents/ charter/index.shtml>. Acesso em: 23 jul. 2014.

_____ , _____. *Resolução 3314 - Definição de Agressão.* New York, ONU, 1973.

_____ , Conselho de Segurança. *Resolução 1113 - Definição de Guerra Cibernética.* New York, ONU, 2011.

_____ , Corte Internacional de Justiça. *Parecer Consultivo Sobre a Legalidade da Ameaça ou Uso das Armas Nucleares*. Nova Iorque, ONU, 1996, p.226. Disponível em: <Disponível em: http://www.icj-cij.org/docket/files/95/7495.pdf>. Acesso em: 23 jul. 2014., p. 226

SCHMITT, Michael N. (Ed.). *Tallinn Manual on the International Law applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013a. 216 p.

SCHMITT, Michael N. *International Law and Cyber Warfare.*Washington D.C: 2013b. Entrevista concedida ao *Atlantic Council's Cyber*. Disponível em: <http://www.c-span.org /video/ ?311806-1/panelists-explain-new-cyber-warfare-manual>.Acesso em: 29 jul. 2014.

ZIOLKOWSKI, Katharina. *Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force*. Tallinn: NATO CCD COE Publications, 2012, 15 p.

ANEXO A

As Fontes do Direito Internacional Humanitário (DIH)

Fonte	Título	Data	Nº de Artigos
Convenção de Genebra	Melhoria da Condição dos Feridos no Campo de Batalha	1864	10
II Conferência de Haia	Leis e Costumes da Guerra em Terra	1899	60 (55 em Anexo)
IV Conferência de Haia	Leis e Costumes da Guerra em Terra	1907	64 (56 em Anexo)
Protocolo de Genebra	Para a Proibição do Uso na Guerra de Gás Asfixiante e dos Métodos de Guerra Bacteriológica	1928	---
I Convenção de Genebra	Para Melhoria das Condições dos Feridos e Doentes das Forças Armadas no Terreno	1864 (revista em 1949)	77 (13 em Anexo)
II Convenção de Genebra	Para Melhoria das Condições dos Feridos, Doentes e Náufragos das Forças Armadas no Mar	1949	63
III Convenção de Genebra	Relativa ao Tratamento dos Prisioneiros de Guerra	1929 (revista em 1949)	143
IV Convenção de Genebra	Relativa à Proteção de Civis em Tempo de Guerra	1949	180 (21 em Anexo)
Convenção de Genebra	Proibindo o Desenvolvimento, Produção e Armazenamento de Armas Bacteriológicas e Tóxicas e sobre a sua Destruição	1975	15
Protocolo I	Relativa à Proteção das Vítimas de Conflitos Armados Internacionais (amplia a definição dos mesmos às guerras de libertação nacional)	1977	102
Protocolo II	Relativa à Proteção das Vítimas de Conflitos Armados Não Internacionais (completa o art.o 3 comum às quatro Convenções de Genebra)	1977	28
Protocolo III	Relativa à Adoção de um Emblema Adicional Distintivo	2005	17

Fonte: EASTWEST INSTITUTE. *Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace*, 2011. p. 13 (adaptação).

ANEXO B

Exemplos de ameaças causadas por seres humanos

Fontes de Ameaça	Motivação	Possíveis Consequências
Hacker, Cracker	Desafio Egocentrismo Protesto Rebeldia *Status* Dinheiro	*Hacking*; Engenharia social; Negação de serviço; Pichação de *sites*; Invasão de sistemas, infiltrações; Acesso não autorizado.
Criminosos digitais	Destruição de informações Acesso a dados sigilosos Divulgação ilegal de informações Ganho monetário Alterações não autorizadas de dados	Atos virtuais fraudulentos (interceptação de dados, ataque homem-no-meio, IP *spoofing*, etc.); Intrusão de sistemas. Suborno por informação; Ataques a sistemas (negação de serviço);
Terroristas	Chantagem Destruição Vingança Exploração Ganho político Cobertura da mídia	Ataques com bombas; Guerra de informação; Ataques a sistemas (negação de serviço distribuído); Invasão e dominação de sistemas; Alteração de sistemas.
Espiões	Vantagem competitiva Espionagem econômica	Garantir vantagem de um posicionamento defensivo; Garantir uma vantagem política; Exploração econômica; Furto de informações; Violação da privacidade das pessoas; Engenharia social; Invasão de sistemas; Invasão de privacidade; Acessos não autorizados em sistemas (acesso a informação restrita, de propriedade exclusiva, e/ou relativa à tecnologia).
Pessoas: mal treinadas, insatisfeitas, mal-intencionadas, negligentes, imprudentes, desonestas, demitidas.	Curiosidade Egocentrismo Informações para serviço de Inteligência Ganhos financeiros Vingança Ações não intencionais ou omissões (erro na entrada de dados, erro na programação).	Agressão a funcionário; Chantagem; Busca de informação sensível; Abuso dos recursos computacionais; Fraudes; Furto de ativos; Suborno de informação; Inclusão de dados falsos; Corrupção de dados; Interceptação de informação; Desvio de informação; Uso de programas ou códigos maliciosos; Sabotagens; Invasão de sistemas; Acessos não autorizados a sistemas.

Fonte: ABNT, 2008a, p. 40-41.