ESCOLA DE GUERRA NAVAL

CC LEONARDO PIRES BLACK PEREIRA

A GUERRA CIBERNÉTICA E O DIREITO INTERNACIONAL:
a aplicação do DICA no ciberataque realizado nas facilidades de enriquecimento de urânio do Irã em Natanz com a utilização da arma cibernética *Stuxnet*.

Rio de Janeiro

2015

CC LEONARDO PIRES BLACK PEREIRA

A GUERRA CIBERNÉTICA E O DIREITO INTERNACIONAL:
a aplicação do DICA no ciberataque realizado nas facilidades de enriquecimento de urânio do Irã em Natanz com a utilização da arma cibernética *Stuxnet*.

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

2015

RESUMO

Atualmente, no campo do Direito Internacional dos Conflitos Armados há uma série de questões sobre a condução da guerra no chamado "quinto" domínio de guerra - o cibespaço. Referente aos aspectos legais, há dificuldades para lidar com questões complexas inseridas nesse domínio. Nesse contexto, após um ciberataque, ocorrido em 2010, às facilidades de enriquecimento de urânio iranianas em Natanz, em que foi utilizado a arma cibernética *Stuxnet* -um *worm* de computador que infectou e danificou os sistemas de controle e as centrífugas, respectivamente - vem à tona a necessidade de refletirmos sobre as questões jurídicas envolvidas na concepção do DICA e se adere aos seus preceitos fundamentais, que são constituídos pelas Convenções de Genebra e Haia, seus três Protocolos Adicionais e seus princípios: a distinção entre combatentes, a limitação das armas, a proporcionalidade dos seus efeitos, a necessidade militar e a humanidade. Ademais, será realizado uma análise se esse ciberataque foi considerado um "ataque armado". Por meio de uma pesquisa documental e bibliográfica, chega-se à conclusão que não há um vazio legal, e sim, um já existente arcabouço jurídico que poderá ser aplicado para enfrentar os desafios impostos pelos conflitos cibernéticos, inclusive no evento relacionado ao *Stuxnet*. Também serão apresentados os critérios de uso da força propostos por Jean Pictet baseados em três modelos, que na visão estadunidense, considera a *effects-based approach* a mais adequada, ou seja, a abordagem baseada nos efeitos. Além disso, serão apresentados alguns tópicos de relevância inseridos no Manual *Tallinn*, publicado recentemente pela OTAN, que tem como propósito estabelecer regras internacionais para a Guerra Cibernética, à luz do Direito Internacional.

Palavras-chave: Direito Internacional dos Conflitos Armados. *Stuxnet.* Manual *Tallinn.* Guerra Cibernética. Direito Internacional. Convenções de Genebra. Protocolos Adicionais.

LISTA DE ABREVIATURAS E SIGLAS

CCDCOE - Centro de Excelência Cooperativa sobre Defesa Cibernética

CICV - Comitê Internacional da Cruz Vermelha

CJG - Corte Internacional de Justiça

CS - Conselho de Segurança

DARPA - Agência de Projetos de Pesquisa Avançados de Defesa do Pentágono

DG - Direito da Guerra

DI - Direito Internacional

DIC - Direito Internacional Consuetudinário

DICA - Direito Internacional dos Conflitos Armados

DIH - Direito Internacional Humanitário

DIP - Direito Internacional Público

DRDO - Organização de Desenvolvimento e Pesquisa de Defesa

EUA - Estados Unidos da América

GC - Guerra Cibernética

MB - Marinha do Brasil

NSA - *National Security Agency*

ONG - Organização não governamental

OTAN - Organização do Tratado do Atlântico Norte

PLC - *Programmable Logic Controller*

SCADA - *Supervisory Control And Data Acquisition*

USCYBERCOM - *U.S. Cyber Command*

SUMÁRIO

1 INTRODUÇÃO

Atualmente, os Estados, os atores não estatais, diversos setores da sociedade e os indivíduos tornaram-se interconectados e interdependentes em um nível nunca antes visto. Ao mesmo tempo, a dependência de sistemas baseados em redes de computadores tem aumentado exponencialmente, proporcionando assim, o surgimento de um "quinto" domínio de guerra[1], ao lado dos domínios já conhecidos (terra, mar, ar e espaço) - o ciberespaço.[2] Mas eis que surge a questão: até que ponto pode existir Direito Internacional (DI) aplicado a esse novo domínio?

Os conflitos no ciberespaço estão crescendo nos últimos anos e em um ritmo acelerado. A Internet é a revolução tecnológica mais rápida e poderosa da história da humanidade, que agora é domínio de espiões, criminosos organizados, sabotadores e *crackers*.[3] Comenta-se, na comunidade de segurança cibernética[4], sobre o que deve ser feito para resolver esse problema, que demanda soluções inseridas dentro do vernáculo da guerra.

Nesse contexto, este trabalho de pesquisa tem o propósito de identificar a aplicabilidade do Direito Internacional dos Conflitos Armados (DICA) no ciberataque[5] ocorrido nas facilidades de enriquecimento de urânio do Irã de Natanz em 2010, com o uso da arma cibernética *Stuxnet*, um *worm*[6] de computador que infectou e danificou as centrífugas

---

[1] O ciberespaço foi reconhecido como um novo domínio de guerra, por doutrina do Pentágono. Disponível em: <http://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>. Acesso em: 25jun. 15.

[2] Ciberespaço é definido como um domínio global dentro do ambiente de informação que consiste em redes interdependentes de infra-estruturas de tecnologia da informação e dados residentes. Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf >. Acesso em 22 jun. 2015.

[3] *Cracker* é o termo que designa programadores maliciosos que agem com o intuito de violar ilegal ou imoralmente sistemas cibernéticos. Disponível em: <http://www.artigonal.com/ti-artigos/entendendo-as-diferencas-entre-hacker-e-cracker-3353750.html>. Acesso em: 28 jun. 2015.

[4] Segurança Cibernética é definida como uma prevenção de danos para proteção e restauração de computadores, sistemas e seviços de comunicações eletrônicas, incluindo as informações nelas contidas, para garantir a sua disponibilidade, integridade, autenticidade, confidencialidade e não-repúdio. Disponível em: <http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf>. Acesso em 21 jun. 2015.

[5] Ciberataque é definido como uma operação cibernética, seja ela de caráter ofensivo ou defensivo, em que, razoavelmente, espera-se que cause lesão ou morte de pessoas, ou danos ou destruição de objetos. Disponível em: <https://ccdcoe.org/tallinn-manual.html>. Acesso em 23 jun. 2015.

[6] *Worm* é definido como uma categoria de programa malicioso que explora as vulnerabilidades de um Sistema Operacional para sua propagação. Sua concepção é bastante semelhante a um vírus. Ao contrário do vírus, ele pode reproduzir-se e duplicar-se por si só, não precisando juntar-se a um programa executável existente. Disponível em: <http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf>. Acesso em: 27 jun. 2015.

daquela facilidade, bem como o seu sistema de controle; e uma análise se foi considerado um ataque armado na concepção do DICA, aderindo aos preceitos de suas Convenções e princípios fundamentais; no que se refere aos aspectos legais, se existe um arcabouço jurídico em vigor que pode ser aplicado para enfrentar os desafios impostos pelos conflitos cibernéticos para seu enquadramento legal.

A relevância do tema paira sobre a condução da guerra no domínio cibernético e os questionamentos sobre os aspectos legais envolvidos à luz do DICA. A verdadeira dificuldade com relação a Guerra Cibernética (GC)[7] não reside na ausência de normas, por si só, mas sim nas complexidades que surgem na determinação dos elementos necessários para torná-la legal.

Ademais, também será relevante identificar os principais esforços realizados por um grupo de especialistas internacionais que trabalharam sob a égide do Centro de Excelência Cooperativa sobre Defesa Cibernética (CCDCOE) da Organização do Tratado do Atlântico Norte (OTAN) na elaboração do Manual *Tallinn*, lançado em 2012, que embora não seja um parecer jurídico consolidado daquela organização, contém um conjunto de recomendações que contribui significativamente para a clarificação do DI aplicável à GC.

Para a consecução do propósito, foi realizado uma pesquisa documental e bibliográfica, baseados na leitura de fontes bibliográficas, consultas à artigos científicos e será desenvolvido em 6 capítulos, a começar por esta Introdução.

O segundo capítulo será apresentado em duas seções. A primeira seção explicará os efeitos da revolução da informação na GC nos dias atuais e a necessidade do domínio do conhecimento para dispersar a "névoa da guerra". A segunda seção descreverá, de forma breve, a relação existente entre a GC e a Trindade de Clausewitz, em que um ciberataque simultâneo pode ocasionar a "paralisia estratégica" de um Estado, preservando a base teórica do passado.

---

[7] Guerra cibernética (GC) é definida como uma penetração não autorizada, em nome ou em apoio a um governo, em um computador, ou rede de outra nação, ou qualquer outra atividade que afete um sistema de computador, cujo objetivo é adicionar, alterar ou falsificar dados, causar a interrupção ou danos a um computador, dispositivo de rede ou objetos controlados por um sistema de computadores (CLARKE, KNAKE, 2015, p.183).

O terceiro capítulo será apresentado também em duas seções. A primeira seção explicará a Operação denominada Olympic Games, orquestrada pelos Estados Unidos da América (EUA), iniciada nos primeiros meses do governo do Presidente Barack Obama (1961-) e concebida para acelerar ciberataques, especialmente, às instalações de enriquecimento de urânio iranianas, fazendo com que as "armas cibernéticas" despontassem como um novo paradigma na GC e ampliasse o seu uso. A segunda seção descreverá detalhes desse ciberataque.

O quarto capítulo, como o anterior, será apresentado também em duas seções. Na primeira seção, serão abordadas as origens do DICA, tendo como base as quatro Convenções de Genebra de 1949 e seus Protocolos Adicionais. Na segunda seção, serão elencados os cinco princípios fundamentais DICA.

O quinto capítulo também será apresentado em duas seções. Na primeira seção, serão apresentados os aspectos do DICA aplicados à GC, o jus *ad bellum* e o *jus in bello*, diretamente relacionados ao ciberataque com o *Stuxnet*, analisando os seus impactos normativos. Também iremos abordar os critérios de uso da força propostos por Jean Pictet baseados em três modelos, que na visão estadunidense, considera a *effects-based approach* a mais adequada, ou seja, a abordagem baseada nos efeitos.

Já na segunda seção, serão identificados os principais pontos do conteúdo do Manual *Tallinn*, que é um esforço, junto à comunidade internacional, para a pesquisa e educação do DI a respeito dos principais aspectos jurídicos relacionado à GC, o que demandará um uma cooperação global para implementá-los e vontade política dos Estados, os quais devem se preocupar com a atuação cada vez mais ativa de atores não estatais.

Finalmente, o sexto capítulo encerrará com a Conclusão do presente trabalho, em que serão apresentadas as considerações finais e os aspectos jurídicos relevantes que envolvem a aplicação do DICA no "campo de batalha virtual", relacionado ao uso da arma cibernética *Stuxnet*, após a análise dos resultados da pesquisa realizada.

2 O CAMPO DE BATALHA VIRTUAL

O propósito deste capítulo é explicar os efeitos da revolução da informação na GC nos dias atuais e a necessidade do domínio do conhecimento para dispersar a "névoa da guerra" e descrever, de forma breve, a relação existente entre a GC e a Trindade de Clausewitz.

A industrialização levou à guerra de desgaste com enormes exércitos na Primeira Guerra Mundial (1914-1918); a mecanização levou à guerra de manobra, em que predominou o uso de tanques na Segunda Guerra Mundial (1939-1945); e a revolução da informação implicou no surgimento da GC. Quem obtiver o domínio da informação poderá dispersar a "névoa da guerra", desfrutando assim, de vantagens decisivas. Nesse contexto, as comunicações e a inteligência sempre foram importantes e crescerão ainda mais, sendo coadjuvantes para a estratégia militar global.[8]

A guerra já não é essencialmente uma função de quem aplica a maior parte dos recursos e tecnologia no "campo de batalha", mas sim de quem tem a melhor informação sobre ela. Atualmente, o que distingue os vencedores é a sua compreensão da informação, não só do ponto de vista de como dominar o inimigo, mas também em termos doutrinários.[9]

A inspiração veio dos mongóis, no século XIII. Sua horda[10] era quase sempre superada em número pelos seus oponentes, mas conquistaram, por mais de um século, o maior império continental já visto.

A chave para o sucesso mongol foi o domínio absoluto das informações no "campo de batalha". Gengis Khan estava a par da evolução de seu exército, mesmo à distância, utilizando-se de seus mensageiros, conhecidos como *arrows riders.*[11]

---

[8] ARQUILLA; RONFELDT, 1997, p. 23 *et seq*.
[9] *Ibidem*, p.23.
[10] A horda mongol era uma massa de incansáveis cavaleiros nômades asiáticos de pequena estatura e com cabelos compridos, empunhando lanças curtas, espada pequena e escudo, galopando pôneis castanhos ou pretos, protegidos por chuvas de flechas. Disponível em: <http://boingboing.net/2012/04/19/win-a-signed-galley-copy-of-gr.html>. Acesso em: 29 jun. 2015.
[11] *ARQUILLA; RONFELDT, op. cit.,* p. 24.

Ao longo da história, a doutrina e a estratégia militar têm sofrido profundas alterações. Weigley (1989), notório historiador militar estadunidense, advertiu que a tecnologia permeia a guerra, mas não pode governá-lo, pois não pode ser a tecnologia *per si*, mas sim a organização da tecnologia, no sentido *lato*, que é importante:

> [...] *the technology of war does not consist only of instruments intended primarily for the waging of war. A society's ability to wage war depends on every facet of its technology* [...] *its methods of organizing its technology* [...] *behind military hardware there is hardware in general, and behind that there is technology as a certain kind of know-how* [...] (p. 196)

Portanto, a mudança tecnológica que corresponde a essa visão ampla é a revolução da informação. Isso é o que vai trazer a próxima grande mudança na natureza dos conflitos e da guerra. Considerando que a GC se refere a conflitos relacionados com o conhecimento a nível militar, esse conceito implica que os futuros conflitos serão travados mais por "redes e quem dominar a "rede" terá grandes vantagens.

A seguir, na próxima seção, serão explicados os efeitos da revolução da informação, nos dias atuais, e a necessidade do domínio do conhecimento para dispersar a "névoa da guerra" dentro do novo "campo de batalha", agora virtual.

2.1 Os efeitos da revolução da informação

A revolução da informação reflete o avanço da informatização da informação e tecnologias de comunicação e suas inovações dentro das organizações. Mudanças estão ocorrendo na forma como as informações são coletadas, armazenadas, processadas e apresentadas e como as organizações são projetadas para tirar proveito do seu respectivo fluxo. Portanto, a informação vem se tornando um recurso estratégico tão valioso e influente na era pós-revolução industrial, como o capital e o trabalho foram na era da "sociedade industrial" (1750-1950) (ARQUILLA, RONFELDT, 1997).

Ela põe em movimento forças que desafiam a concepção de muitas instituições. Interrompe e corrói as hierarquias em torno do que as instituições são normalmente concebidas. Difunde e redistribui o poder, por vezes para o benefício dos Estados mais fracos, atravessando fronteiras. Esses pontos podem conduzir diretamente o futuro dos conflitos e da guerra.[12]

Daniel Bell (1919-2011), prestigiado sociólogo estadunidense, trouxe a "era da informação" para a atenção de cientistas sociais estadunidenses e europeus. Para ele, o princípio axial da sociedade pós-industrial é a centralidade de conhecimentos teóricos e seu novo papel, quando codificados, como o diretor de mudança social, introduzindo o conceito do termo "sociedade da informação" (BELL, 1973).

Nesse contexto, a GC significa uma transformação na natureza da guerra, e isso implica no desenvolvimento de novas doutrinas e que tipos de forças são necessárias para travá-la, podendo ser aplicável tanto em conflitos convencionais e ambientes não convencionais, tanto para fins defensivos ou ofensivos.[13]

Enfim, com a inovação na guerra, podemos dizer que a GC está para o século XXI, assim como a *blitzkrieg*[14] foi para o século XX. Isso representa uma extensão da importância tradicional de obtenção de informações na guerra e de tentar localizar, observar, surpreender e enganar o inimigo antes que ele faça o mesmo com você.[15]

A seguir, na próxima seção, será descrito, de forma breve, a relação existente entre a GC e a Trindade de Clausewitz, em que um ciberataque simultâneo direcionado aos elementos basilares da Trindade, conforme o conceito de "guerra em paralelo", pode ocasionar a "paralisia estratégica" de um Estado, como sistema, e entrar em colapso, causando o caos e a desordem.

---

[12] *Ibidem*, p. 26.
[13] *Ibidem*, p. 43.
[14] *Blitzkrieg* (termo alemão para "guerra-relâmpago") foi uma doutrina militar em nível operacional que consistia em utilizar forças móveis em ataques rápidos e de surpresa, com o intuito de evitar que as forças inimigas tivessem tempo de organizar a defesa. Baseia-se no efeito-surpresa, na rapidez da manobra e na brutalidade do ataque. Disponível em: <http://veja.abril.com.br/especiais_online/segunda_guerra/infos/guerra_relampago/info.html>. Acesso em: 15 jun. 2015
[15] ARQUILLA; RONFELDT, *loc*. *cit*.

2.2 A Guerra Cibernética e sua relação com a Teoria de Clausewitz

Como já foi dito anteriormente, ao longo do tempo a GC vem proporcionando uma gradual mudança de paradigma referente às estratégias militares, dando mais ênfase aos ciberataques e suas contramedidas, resultando na noção de que a GC é um potencial multiplicador de força e um aperfeiçoamento das operações tradicionais (SHARMA, 2010).

A seguir, serão abordados os conceitos da Trindade de Clausewitz, os quais servirão de base para discussões sobre a mudança ou não da natureza da guerra, bem como se a teoria da guerra permanece vigente e aplicável nos conflitos atuais, como a GC.

Para Clausewitz, "a guerra é um ato de força para obrigar o nosso inimigo a fazer a nossa vontade".[16] Por meio dessa frase, ele estabelece uma importante relação, explicando que a guerra, por não ser autônoma, é a extensão da política, que, por sua vez, determina o seu "caráter" e ao estabelecer as condições de como ela será travada, a GC é capaz de compelir o inimigo a sua vontade, induzindo-o à "paralisia estratégica" (meio) com o propósito de atingir os objetivos desejados (fim), sem emprego do uso da força convencional.

Nesse contexto, faz-se mister citar que "a guerra é meramente a continuação da política por outros meios"[17], e desse modo, o estrategista militar prussiano deixa clara sua ideia de que a guerra é vista como ato ou instrumento da política, partindo da premissa de que todas as guerras têm a mesma natureza, ensina que "a guerra é mais do que um verdadeiro camaleão, que adapta um pouco as suas características a uma determinada situação".[18]

Fica evidente que a natureza da guerra é única e imutável, ao passo que suas características podem se alterar por conta de ideias, tecnologias ou influências, tanto do tempo quanto do espaço.

---

16 CLAUSEWITZ, 1984, p. 75.
17 *Ibidem*, p. 91.
18 *Ibidem*, p. 92.

Outro aspecto de relevância diz respeito aos três elementos que compõem a denominada Trindade Clausewitziana: a violência, o ódio e a inimizade; o acaso e a probabilidade; e a razão e a política, que se relacionam com possíveis atores. O primeiro deles foi associado às pessoas; o segundo, às Forças Armadas; o terceiro, ao governo. Todos os três elementos formam o núcleo de um Estado e interagem entre si (CLAUSEWITZ, 1984).

Segundo Amit Sharma, membro da Organização de Desenvolvimento e Pesquisa de Defesa (DRDO) da Índia, os elementos da Trindade quando atacados por ciberataques, de forma simultanea, criam o conceito de "guerra em paralelo", gerando um efeito cascata e induzindo uma "paralisia estratégica" do Estado, que como sistema, desmoronará e será dominado rapidamente, criando o conceito da "Trindade Cibernética" (ANEXO).

Atualmente, os países desenvolvidos têm dependência tecnológica dos ativos de informação, em que todos os três elementos de Clauzewitz estão interligados no ciberespaço, tais como sistemas de C², sistemas de posicionamento global e infraestruturas críticas.[19]

As vantagens tecnológicas em relação ao acesso a serviços essenciais de um Estado, como as instituições finaceiras, sistemas bancários e de transporte, não só facilitaram a vida das pessoas, mas também a fizeram vulneráveis, tornando-as dependentes, porém vivendo em uma sociedade em que as pessoas são socialmente desconectadas, individualistas e politicamente desengajadas, o que pode gerar resultados catastróficos no futuro, quando o caos poderá prevalecer, causando destruição total de um Estado.[20]

No próximo capítulo, será abordado o ciberataque, como foi utilizado a "arma cibernética" *Stuxnet* ao longo da Operação *Olympic Games*, comandados pelos norte-americanos, às facilidades nucleares do Irã, criando assim, um novo paradigma dentro da GC.

---

19 SHARMA, 2010, p. 4.
20 *Ibidem*, p. 5.

3 *STUXNET*: UM NOVO PARADIGMA NA GUERRA CIBERNÉTICA

> *President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to conter* (WHITE HOUSE, 2009, p. 1)

Em 2010, um pronunciamento do Presidente Barack Obama após a descoberta do S*tuxnet* causou drásticas mudanças na comunidade cibernética do mundo inteiro. Ele não só mostrou a que ponto os Estados são vulneráveis frente à ciberataques, mas identificou que a segurança cibernética é vista como um sério desafio econômico e de segurança nacional e deve ser enfrentado, porém os Estados não estão prontos para enfrentá-los, até mesmo os EUA (tradução nossa).

O *Stuxnet* foi uma demonstração tanto para os Estados que estavam planejando investir em GC, como para aqueles que não investiam, além de realçar que a GC, em grande parte, carece de aportes financeiros elevados, geralmente associados com a guerra tradicional. Para aqueles Estados que não estavam investindo, a ameaça de perdas catastróficas veio à tona após o ciberataque às facilidades nucleares iranianas (LEE, 2011).

Após o evento *Stuxnet*, houve um impacto sobre a política e o orçamento norte-americanos destinados à GC. Segundo dados da Agência de Projetos de Pesquisa Avançados de Defesa do Pentágono (DARPA), responsável por desenvolver novas tecnologias para uso militar, serão alocados para aquela agência US$ 1,5 bilhão, no período de 2013 a 2017, com o objetivo específico de aumentar as suas capacidades de ciberataque e isso foi usado como inspiração e justificativa para controlar a Internet. Além disso, inspirou outros governos e grupos a desenvolver suas próprias armas cibernéticas (PAGANINI, 2012).

Devido ao poder desse *worm*, que foi concebido para penetrar numa instalação nuclear com medidas de segurança extremas, ele poderia ser projetado para acessar sistemas financeiros e bancários ou até mesmo roubar facilmente as informações pessoais de milhões de pessoas em todo o mundo, deixando-os vulneráveis (LEE, 2011).

Nesse cenário, surgem algumas questões, tais como: os atores não estatais serão vistos no ciberespaço? Se o *Stuxnet* fosse lançado a partir de um ator não estatal, por exemplo, uma corporação, que implicações isso teria para o Estado do ator não estatal e como é que o Irã reagiria? Se um ator não estatal lança um ciberataque da magnitude do *Stuxnet*, com efeitos mais nocivos, o Estado sob ataque consideraria um "ato de guerra"? Será que o ator não estatal seria responsabilizado pelo seu país de origem?

Essas questões não são fáceis de responder e este trabalho irá abordar alguns aspectos que envolvem esse tema à luz do DICA.

Enfim, o *Stuxnet* surge como um novo paradigma da GC e causou uma mudança na forma como os Estados, corporações e os cidadãos visualizam a GC. Esse é apenas o começo de uma nova era da guerra, que se tornará ainda mais invasiva.

Para alguns, foi considerado a primeira arma cibernética a ser utilizada na história[21], mas sua origem e efeitos ainda são desconhecidos.

A seguir, abordaremos como os norte-americanos começaram a planejar e ampliar o uso de armas cibernéticas, tendo o próximo alvo o Irã, por meio da Operação denominada *Olympic Games.*

3.1 Operação *Olympic Games*

Em 2009, nos seus primeiros meses no cargo, após ter sido empossado como presidente dos EUA, Barack Obama ordenou, secretamente, ataques cada vez mais sofisticados sobre os sistemas de computadores das principais instalações de enriquecimento nuclear do Irã em Natanz, ampliando significativamente o uso de armas cibernéticas, inclusive com a criação e uso do *Stuxnet* (SANGER, 2012).

[21] http://www.economist.com/node/17147818

Obama decidiu acelerar os ataques, já iniciados no governo Bush (2001-2009) em 2006, deflagrando uma Operação denominada *Olympic Games*. Alguns especialistas em segurança da informação que estudaram o *worm* disseram que o *Stuxnet* poderia ter sido desenvolvido pelos EUA em parceria com Israel, porém sua origem permanece desconhecida até hoje. Nas semanas seguintes, a planta nuclear de Natanz foi atingida por um ciberataque com a versão mais recente do *worm*. A última de uma série de ataques, algumas semanas depois, colocou fora de operação, temporariamente, entre 1.000 e 5.000 centrífugas.[22]

Foi bem-sucedido esse programa de "sabotagem" planejado para retardar o progresso no desenvolvimento da capacidade de construção de artefatos nucleares do Irã. Estimativas da administração de Barack Obama disseram que o esforço foi um retrocesso de 18 meses a dois anos, mas alguns especialistas dentro e fora do governo foram mais céticos e observaram que, naquela época, o Irã possuía a capacidade de produzir combustível nuclear, com um enriquecimento adicional, suficiente para cinco ou mais armas nucleares.[23]

À época, o Irã negou que as suas instalações de enriquecimento haviam sido atingidas pelo *Stuxnet*, mas em seguida, afirmou que tinha sido descoberto e que tinha contido o ataque. O governo norte-americano reconheceu, à época, o desenvolvimento em armas cibernéticas, mas nunca admitiu usá-las, oficialmente.

Mas a Operação *Olympic Games* era sofisticada e completamente diferente. Foi a primeira vez que os EUA usaram uma arma cibernética para paralisar uma infraestrutura física de um outro país, utilizando-se um *software*, o que até então só poderia ser realizado pelos métodos tradicionais de ataque cinéticos. Em 2006, o ex-presidente George W. Bush (1946-) vislumbrou algumas opções para lidar com o Irã que não inspirava confiança e possuia uma retórica inflamada de seus líderes.

---

[22] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0

[23] https://www.foreignaffairs.com/articles/iran/2015-04-05/deal-it

O então Vice-Presidente norte-americano na administração Bush, Dick Cheney (1941-) pediu que Bush considerasse a realização de um ataque militar contra as instalações nucleares iranianas antes que eles pudessem produzir combustível adequado para a fabricação de um artefato nuclear. Porém, concluíram que essa opção inflamaria ainda mais a região do Oriente Médio, podendo ter resultados incertos (SANGER, 2012).

O presidente Obama, após a sua assunção em 2009, estava ciente de que Bush estava abrindo um novo caminho para definir algumas regras na GC. Segundo Sanger (2012), considerando o ciberataque ao Irã de grande vulto e que causou uma destruição física às suas instalações, isso pôs em cheque a autoridade constitucional dos EUA para lançar ciberataques contra o Irã, ainda mas sem a autorização prévia do Congresso norte-americano:

> [...] de acordo com os participantes nas muitas reuniões realizadas sobre a Operação *Olympic Games*, ele tinha plena consciência de que, que a cada ataque ele estava empurrando os Estados Unidos em um novo território, tanto quanto seus antecessores tiveram com o primeiro uso de armas atômicas na década de 40, de mísseis intercontinentais na década de 50 e de drones na última década. Ele expressou repetidamente preocupação de que o conhecimento americano de que ele estava usando armas cibernéticas [...] (p. A1, tradução nossa).

Se a Operação falhasse, não haveria tempo para sanções e diplomacia com o Irã e Israel poderia realizar um ataque militar convencional, o que levaria a um conflito que poderia espalhar-se por toda a região. Há indícios de que também houve uma colaboração significativa de Israel, com a participação de suas Forças Armada, que detinha conhecimentos técnicos que rivalizavam com a *National Security Agency* (NSA) (SANGER, 2012).

3.2 O ataque às centrífugas de enriquecimento de urânio do Irã

O *Stuxnet* chamou a atenção dos especialistas pelo seu nível de sofisticação. Demonstrou possuir certos requisitos técnicos interessantes, incluindo um vetor de ataque específico que foi limitada a determinados computadores que operam de forma bastante singular.

Enquanto o *worm* propagou-se rapidamente pelo mundo, infectando dezenas de milhares de computadores, seu propósito permaneceu um mistério. Relatos iniciais sugeriram

que este *worm* destinava-se a perturbar telecomunicações por satélite e controlar os sistemas de infraestrutura industriais, porém nada foi comprovado nesse sentido.[24]

No entanto, depois de vários meses, tornou-se evidente que ele possuía um alvo geográfico específico: o Irã. Um número desproporcional de sistemas de computadores infectados foram localizados naquele país. Dados publicados pela empresa Symantec, líder mundial no fornecimento de soluções de segurança, mostraram que cerca das 100.000 máquinas infectadas no mundo, cerca de 60.000 eram localizadas no Irã.[25]

O *Stuxnet* foi descoberto originalmente em 2010 por uma empresa que vende *software* antivírus chamada *VirusBlokAda*, localizada na Bielorrússia, que verificou a infecção, em escala, de sistemas de controle industriais do mundo todo fabricados pela empresa alemã Siemens. Segundo aquela empresa, o *worm* foi introduzido nos sistemas para monitorar as plantas industriais automatizadas, denominado SCADA (*Supervisory Control And Data Acquisition*) que não estão conectados à Internet e possuem portas USB, que por meio de um *pen drive* infectado podia controlá-los e explorar suas vulnerabilidades no Sistema Operacional denominado *WinCC-7.*[26]

De acordo com a Symantec, o *Stuxnet* foi programado para contaminar os *Programmable Logic Controller* (PLC)[27], envolvendo quatro ataques *zero-day*[28] diferentes, tornando-o complexo e tendo como alvo específico as unidades conversoras de frequência, que são usadas para controlar a velocidade de um motor.[29]

---

[24] LANGNER, 2013. p. 18.
[25] SYMANTEC, 2011, p. 5.
[26] LANGNER, *op. cit*., p. 12.
[27] *Programmable Logic Controller* (PLC) significa Controlador Lógico Programável é um sistema de controle de computador industrial que monitora continuamente o estado de dispositivos de entrada e toma decisões com base em um programa personalizado para controlar o estado dos dispositivos de saída. Disponível em: <http://www.amci.com/tutorials/tutorials-what-is-programmable-logic-controller.asp>. Acesso em: 30 jun. 2015.
[28] Ataque *zero-day*, é um ciberataque que ocorre no mesmo dia em que um ponto fraco, antes inexistente, for descoberto no software por indivíduos mal-intencionados. Nesse momento ele é explorado antes que uma atualização do software seja disponibilizada pelo seu desenvolvedor. Disponível em: < http://www.kaspersky.com/pt/internet-security-center/definitions/zero-day-exploit>. Acesso em: 29 jun. 2015.
[29] SYMANTEC, *op. cit*., p. 3.

Isso fez com que os motores elétricos oscilassem, descontroladamente, em velocidades supersônicas, de forma que quebrassem quase 1.000 centrífugas, que eram interligadas (CLARKE; KNAKE, 2015).

As tais unidades conversoras de frequência eram fabricados pela empresa iraniana chamada Fararo Paya, localizada em Teerã ou pela empresa finlandesa Vacon, e foram projetados para receber comandos do *software* da Siemens que foram alterados pelo *worm*.

Os iranianos ficaram confusos, em parte, porque o *worm* ficou adormecido na planta de Natanz por semanas, gravando as operações normais. Quando ficou ativo e realizou o ataque, enviou sinais para sala de controle em que ficavam os operadores, indicando que tudo estava operando normalmente, sendo essa a sua característica mais sofisticada (LANGNER, 2013).

Os pesquisadores passaram meses realizando a engenharia reversa do *Stuxnet* e disseram que o seu nível de sofisticação e por ser pontual sugeriria que um Estado estava por trás do ataque. A análise do código deixa claro que o *Stuxnet* tinha a intenção de destruir seu alvo com determinação tipicamente militar (BROAD; MARKOF; SANGER, 2011).

O *Stuxnet* causou a destruição de um equipamento sensível e integrante da infraestrutura nuclear e crítica do Irã, além de atrasar o seu programa nuclear por algum tempo.

Mas os *hackers*[30] conseguiram capturar o *worm* e decifrá-lo, percebendo que novos ataques poderiam ser realizados no sistema SCADA de empresas norte-americanas, possibilitando assim ataques a outros objetos, tais como geradores ou transformadores elétricos. (CLARKE; KNAKE, 2015).

No próximo capítulo, serão tecidas algumas considerações sobre os aspectos do DICA, seu surgimento e a descrição de seus princípios fundamentais.

---

[30] *Hacker* é um criminoso que usa suas habilidades com computadores para seu próprio proveito, violando a segurança de sistemas de forma ilegal. Disponível em: <https://wikileaks.org/gifiles/attach/172/172124.pdf>. Acesso em: 01 jul. 2015.

4 DIREITO INTERNACIONAL DOS CONFLITOS ARMADOS (DICA)

Ao se discorrer sobre a história da humanidade é possível perceber que sobre ela está a constante presença dos conflitos armados, pois, mesmo nas antigas civilizações sempre houve, mesmo que em pequena escala, a preocupação de se estabelecerem normas a fim de minimizar a conduta dos beligerantes e proteger certos grupos de pessoas.

É diante dessa realidade que o DICA tenta engendrar-se, uma vez que é nítida a noção do que a guerra representa. O que se objetiva é minimizar os efeitos avassaladores criados pela guerra por meio de restrições jurídicas que são responsáveis por atenuar alguns efeitos gravíssimos proporcionados pelos conflitos armados.

O DICA também conhecido como Direito da Guerra (DG) ou Direito Internacional Humanitário (DIH) é um ramo do Direito Internacional Público (DIP) constituído por todas as normas convencionais ou de origem consuetudinária especificamente destinadas a regulamentar os problemas que surgem em período de conflito armado.

O Comitê Internacional da Cruz Vermelha (CICV) define conflito armado como "um conjunto de normas que busca limitar os efeitos dos conflitos armados, que protege as pessoas que não participam ou que deixaram de participar das hostilidades e restringe os meios e métodos de guerra"[31]. O DICA possui três vertentes:

a) **Direito de Genebra**: constituído pelas quatro Convenções de Genebra de 1949, cujo objetivo principal é a proteção das vítimas da guerra;
b) **Direito de Haia**: suas regras estão contidas nas Convenções de Haia de 1899, revistas em 1907 e determina os direitos e deveres dos beligerantes na condução das operações militares e a limitação da escolha dos meios para prejudicar o inimigo.

[31] https://www.icrc.org/pt/guerra-e-o-direito>. Acesso em: 12 jul. 2015.

As duas vertentes citadas foram reunidas por meio dos Protocolos Adicionais de 1977. Essas regras têm vista a necessidade de ter em conta necessidades militares das partes em conflito, nunca esquecendo dos princípios de humanidade; e o

c) **Direito de Nova Iorque**: se preocupa com a proteção dos direitos humanos em período de conflito armado em matéria de desarmamento e limitação da proliferação de armas. Em 1968, a Assembleia Geral das Nações Unidas adotou a resolução 2444, com o título "Respeito dos direitos humanos em período de conflito armado", o que constitui um marco da mudança de atitude daquela organização no que diz respeito ao Direito Humanitário, porém, esse ramo do DICA não será abordado neste trabalho[32].

Esse ramo do DI, surge entre os Estados retornando ao passado e sendo emanando pelos conflitos atuais, com o propósito de constituir regras de conduta entre seus atores.

Nas próximas duas seções, serão abordados o advento do DICA e seus princípios fundamentais, respectivamente.

4.1 O advento do DICA

As concepções e o conteúdo do DICA como atualmente é concebido (universal e em grande parte codificado) são fenômenos recentes, datados do século XIX. Seus principais precursores são Francis Lieber e Henry Dunant (GUERRA, 2011).

Francis Lieber (1800-1872), um jurista e imigrante alemão radicado nos EUA, foi o responsável por criar, a pedido do Presidente Lincoln (1809-1895), um sistema normativo de regras de condutas com a finalidade de serem aplicadas durante a Guerra da Secessão (1861-1865). Tal sistema é conhecido como “Código de Lieber”, o qual teve como escopo evitar sofrimentos desnecessários e limitar o número de vítimas em um conflito (GUERRA, 2011).

[32] Disponível em: <http://direitoshumanos.gddc.pt/Textos/sobre-dih.htm>. Acesso em: 15 jun. 2015

Jean Henri Dunant (1828-1910) foi um grande empresário suíço. Em 1859, fez uma viagem de negócios ao norte da Itália para tratar com Napoleão III (1808 – 1873). Nessa ocasião, acabou testemunhando a Batalha de Solferino[33] (1859) e, ao verificar aquele caos, se sensibilizou e passou a mobilizar voluntários e improvisar atendimento médico em uma das igrejas de Castiglioni. Entretanto, apesar de todo seu esforço, muitos feridos que poderiam ser salvos acabaram morrendo por falta de assistência médica.[34]

De volta à Genebra, em 1862, Dunant registrou suas experiências em um livro intitulado "Lembranças de Solferino" e desencadeou um movimento internacional, como o objetivo de suprir deficiências dos serviços sanitários nos campos de batalha (REZEK,2006).

Com isso, Dunant buscou a conscientização humana sugerindo duas ações para amenizar futuras situações desse tipo: a criação de uma sociedade de socorro privada, que atuaria em conflitos, de forma incondicional e a assinatura de um tratado para permitir essa atuação (BORGES, 2006).

Junto com outras quatro pessoas fundou, em 1863, o Comitê Internacional de Socorro aos Militares Feridos, que conseguiu convocar, no ano seguinte, uma conferência diplomática com a participação de 16 Estados. Mais tarde passou a se chamar Comitê Internacional da Cruz Vermelha (CICV, 1949).

Em 1864, a primeira Convenção de Genebra criava normas escritas de proteção às vítimas de guerra, quais sejam os militares feridos em campanha ou doentes sem discriminação.

Em 1906, a segunda Convenção de Genebra estende o alcance daquelas normas para as forças navais.[35]

---

[33] Ocorrida em 24 de junho de 1859, no norte da Itália, foi um combate decisivo da Segunda Guerra de Independência Italiana, resultante da invasão do Piemonte-Sardenha pelos austríacos em 1859. Essa batalha resultou na vitória das tropas francesas de Napoleão III e Sardo-Piemontesas de Vítor Emanuel II sobre o exército austríaco comandado pelo imperador Francisco José I da Áustria (Franz Joseph). Disponível em: <https://www.icrc.org/por/resources/documents/feature/solferino-feature-240609.htm>. Acesso em: 04 jul. 15.

[34] GUERRA, 2011, p. 34.

[35] *Ibidem*, p. 35.

A terceira Convenção de Genebra de 1929, basicamente abordava a proteção aos prisioneiros de guerra, para que fossem tratados humanamente; definia qual o entendimento sobre quem era considerado como tal; obrigava o respeito a sua religião e também discorria sobre as obrigações sanitárias de higiene e alimentação.[36]

A quarta e última Convenção de Genebra de 1949, de uma forma ampla, defende a proteção aos civis em temo de guerra para que não fossem utilizados como escudo humano e não sofressem punições indevidas. Além das quatro convenções acima mencionadas, complementam o Direito de Genebra os Protocolos Adicionais, ambos criados em 1977, sendo os mais importantes: o Protocolo I (PA I), relativo à proteção às vítimas dos conflitos internacionais e o Protocolo II (PA II), relativo à proteção às vítimas dos conflitos não internacionais.[37]

No caso de conflitos armados internacionais, existe uma grande dificuldade em determinar, conforme o caso, qual Estado é o culpado pela violação da Carta das Nações Unidas; em virtude disso, o *jus in bello* segue independente do *jus ad bellum*, pois sua finalidade é garantir a proteção das vítimas da guerra e seus direitos fundamentais, seja qual for a parte a que pertençam, a partir do momento do início do conflito armado. Pós-Segunda Guerra Mundial, a utilização da força para a solução de controvérsias entre Estados passou a ser proibida. A partir daquele momento a guerra era ilícita (BRASIL, 2009).

A proteção fornecida por essas normas internacionais humanitárias é de interesse global e são regidas por princípios que regulam a violência e preservam a vida humana.

Assim, o surgimento do DICA, cujo cerne reside na valoração do ser humano e sua preservação e tem por finalidade precípua a de enunciar as regras aplicáveis durante os conflitos armados, sejam eles internacionais ou nacionais, de maneira a restringir os direitos dos comba-

---

36 GUERRA, 2011, p. 36.
37 *Ibidem*, p. 37.

tentes, por meio da limitação de condutas nas hostilidades, e proteger os direitos dos não combatentes – tanto os civis, quanto os militares fora de combate – enunciando os mecanismos de proteção das pessoas que caíram no poder do inimigo, além de ter angariado o respeito e a submissão de todos os Estados para o seu cumprimento.

4.2 Princípios fundamentais do DICA

O DICA possui um conjunto de princípios claramente definidos. Esses princípios são práticos, refletem a realidade do conflito e consistem em limitar e aliviar, tanto quanto possível, as calamidades da guerra, mediante a conciliação das necessidades militares, impostas pela situação tática e o cumprimento da missão, com as exigências impostas por princípios de caráter humanitário. Ademais das convenções, normas e costumes, o DICA tem como princípios fundamentais a distinção, a proporcionalidade, a necessidade militar, a limitação e a humanidade que norteiam a aplicação desse ramo do Direito (BRASIL, 2009).

O princípio da distinção**,** como rege o artigo 48 do PA I, a distinção deve ser feita de maneira clara e objetiva sempre deve distinguir claramente o combatente do não combatente (CICV, 1949). O combatente pode ser atacado, a menos que ele esteja fora de combate. O não combatente é protegido contra os ataques, porém podem perder essa proteção sempre que eles participem diretamente das hostilidades.

Deve-se distinguir bens de caráter civil e objetivos militares. Os bens de caráter civil, públicos ou privados, não devem ser objetos de ataques ou represálias e devem ser respeitados e protegidos. Ele regula as questões de quem e o que pode ser atacado (BRASIL, 2009). O Manual de DI aplicado às Operações Navais da Marinha do Brasil (MB) diz:

> Tal princípio rege a escolha de objetivos durante a ação militar e sua estrita observância tem como decorrência evitar a condução de ataques indiscriminados que são proibidos [...] e que não se dirijam contra um objetivo militar determinado, ou que, devido aos métodos e meios empregados, podem atingir indistintamente objetivos militares e bens de caráter civil ou civis (BRASIL, 2009, p. 6-3).

No contexto da GC, no entanto, é um desafio para a nossa capacidade para distinguir, adequadamente, combatentes e não combatentes e a escolha de alvos, como a proibição de ataque à objetos civis, e assim, aderir a esse princípio fundamental.

Além disso, a natureza da GC não se encaixa perfeitamente ao paradigma das hostilidades em torno do qual o DICA é construído, já que não podemos definir qual seria o limite de dano que um ciberataque teria em relação a um ataque armado à luz do DICA, com relação à destruição de dados e informações, sem danos físicos aparentes ou em relação às consequências de um ciberataque em outros objetos não antes intencionados. O artigo 51 do PA I diz que os ataques indiscriminados são proibidos, portanto podendo ser aplicáveis à GC (CICV, 1977).

No princípio da proporcionalidade, como está explicado no artigo 57 do PA I, será aplicado quando for possível que seja feita a escolha entre vários alvos militares para obter uma vantagem militar equivalente, o objetivo deverá ser escolhido entre aquele cujo ataque resulte em um menor dano e perigo para as pessoas e objetos civis (CICV, 1977). Também é definido como a relação proporcional entre o uso da força para alcançar o objetivo militar, que quando atacados, civis e alvos civis devem ser poupados. A utilização dos meios e métodos de guerra deve ser proporcional à vantagem militar concreta e direta. Nenhum alvo, mesmo que militar, deve ser atacado se os prejuízos e sofrimento forem maiores que os ganhos militares que se espera da ação. O uso excessivo da força viola, claramente, o DICA (BRASIL, 2011).

Há controvérsias que giram em torno da sua aplicação para um ciberataque específico. O princípio da proporcionalidade só se aplica a essas operações cibernéticas que equivalem a um "ataque". Apesar de ciberataques, inevitavelmente, possuírem a capacidade de matar ou ferir civis, a grande maioria deles resultaram somente em danos materiais.

Além disso, vale ressaltar que é fundamental que o dano em objetos civis seja entendido em sentido *lato*. Os servidores e roteadores das “redes” na Internet ou segregadas dela podem ser objetos civis, pois são de propriedade, operados e mantidos por civis, em sua maioria.

Podemos dizer que quaisquer danos a esses elementos de infraestrutura podem ser considerados como objeto civil para efeitos de análise da proporcionalidade.

O princípio da necessidade militar é a limitação de uma incursão militar a determinado alvo e objetivo, sob a natureza do ataque de caráter totalmente e exclusivamente militar, sem a ocorrência de eventos prejudiciais ao bem-estar humano não envolvido diretamente com o conflito armado. O uso da força deve corresponder à vantagem militar que se pretende obter. As necessidades militares não justificam condutas desumanas, tampouco atividades que sejam proibidas pelo DICA. (BRASIL, 2011).

Embora os objetos sejam de caráter militar, um impasse que encontramos nos conflitos contemporâneos, como a GC, é a dificuldade do reconhecimento exato de que é um alvo militar (BRASIL, 2011).

Mas para um esclarecimento acerca do que seriam os alvos militares, aqueles cabíveis de um possível ataque, o artigo 52 do PA I, reconhece que os ataques devem ser estritamente limitados aos objetos militares.

No que diz respeito aos bens, os objetos militares são aqueles que, pela sua natureza, localização, destino ou utilização contribuam efetivamente para a ação militar e cuja destruição total ou parcial, captura ou neutralização ofereça, na ocorrência, uma vantagem militar precisa (CICV, 1977).

O princípio da limitação se baseia no artigo 35 do PA I. Em qualquer conflito armado, o direito das partes envolvidas para escolher métodos e meios de guerra e causar danos ao inimigo não é ilimitado, ou seja, é imperiosa a exclusão de meios e métodos que levem ao sofrimento desnecessário e a danos supérfluos (CICV, 1977).

A principal função da proibição ou restrição ao uso de determinadas armas em conflitos, é a de minimizar os sofrimentos gerados por elas, somada ao agravamento dos ferimentos, muitas vezes causando sofrimento desnecessário aos combatentes (BRASIL, 2011).

Por fim, o princípio da humanidade tem como papel principal o de manter as condições básicas de bem-estar e individualidade dos seres humanos em conflitos, com o propósito de evitar e aliviar o sofrimento e as adversidades causadas, por meio da proteção à vida, saúde e pelo respeito ao ser humano em sua totalidade. Por isso, são proibidos ataques exclusivamente contra civis, o que não impede que, ocasionalmente, algumas vítimas civis sofram danos; mas todas as precauções devem ser tomadas para mitigá-los (BRASIL, 2009).

A dignidade humana e o princípio máximo do respeito à humanidade são considerados os pilares do Direito Humanitário. O artigo 27 da quarta Convenção de Genebra determina que todas as pessoas protegidas têm direito, em todas as circunstâncias, ao respeito a sua pessoa, sua honra, seus direitos de família, convicções e práticas religiosas, hábitos e costumes. Serão sempre tratadas com humanidade e particularmente protegidas contra qualquer ato de violência ou de intimidação, contra os insultos e a curiosidade pública (CICV, 1949).

Vimos que o DICA claramente prescreve a obrigação dos Estados para avaliar novas armas, incluindo armas cibernéticas, e se seu emprego completamente ou parcialmente infringiria algumas das normas estabelecidas. Instalações médicas, por exemplo, não devem ser atacadas e devem ser sempre protegidas contra as devastações da guerra.

Consequentemente, ataques a computadores que podem desligar o sistema de geração de eletricidade usada por um hospital ou corromper a base de dados médica são atos de violação dessa proteção. Outros objetos que não devem ser considerados objetos militares são diques, barragens e estações de geração elétrica nuclear, porque um eventual ciberataque que manipule seus sistemas de controle pode provocar severas perdas entre a população civil.

A seguir, no próximo capítulo, falaremos sobre os principais aspectos do DICA aplicados na GC presentes no ciberataque do *Stuxnet* e seus impactos normativos. Além disso, será apresentado, de maneira breve, o conteúdo do Manual *Tallinn*, que é um esforço da OTAN a respeito dos principais aspectos jurídicos relacionados a GC.

5 ASPECTOS DO DICA APLICADOS AO EVENTO *STUXNET*

Dois conceitos dos DI se aplicam à GC: *jus ad bellum* - as leis que regem a decisão de recorrer ao uso da força e *jus in bello* - as leis que regem a condução das hostilidades.

Decorrente do vertiginoso progresso tecnológico atual, torna-se indispensável a aplicabilidade do DICA à realidade da GC para que o ele possa continuar tutelando adequadamente as pessoas humanas em situações de conflito, o que é seu objetivo primordial. A GC trouxe, todavia, um paradoxo que deve ser enfrentado: ao mesmo tempo em que ela reduz o número de baixas civis, ela aumenta o potencial de violação aos princípios do DICA.

Nesse contexto, alguns especialistas em segurança cibernética declaram que a GC cibernética é iminente e já está acontecendo. No entanto, ainda não está claro em que uma GC se encaixa na definição do DI. A questão é como o DICA pode ser aplicado e se os ciberataques podem alterar o *status quo* de seus princípios. É o que veremos nas duas próximas seções.

5.1 *JUS AD BELLUM* e *JUS IN BELLO*

As regras do *jus ad bellum* orientam a decisão de um Estado quanto a saber se um incidente justifica engajar-se em um conflito armado ou desencadeia as disposições da Carta das Nações Unidas sobre o direito do uso da força em legítima defesa, sendo o atacante um ator estatal ou não estatal (LEWIS, 2010).

Segundo Dunlap (2011), professor de práticas do Centro de Direito, Ética e Segurança Nacional da *Duke Law Scholl*, a questão abordada na introdução deste capítulo, é agravada pelos desafios enfrentados pelos juristas e especialistas em tecnologia que estão lutando com questões dentro do contexto de *jus ad bellum* e, em particular, sobre a atribuição de ataques a certos atores estatais avançados tecnologicamente que desenvolvem ferramentas cibernéticas, atrelados à preocupações concernentes à segurança nacional (DUNLAP, 2011).

Com a descoberta do *Stuxnet,* sugere-se que o primeiro “tiro cibernético” de fato tenha sido disparado. Por ocasião da sua decodificação, ficou claro que as armas cibernéticas podem ser incrivelmente destrutivas, equiparadas a armas cinéticas existentes e efetivamente precisas (DUNLAP, 2011).

Assim, será que podemos sugerir que o ataque às facilidades de enriquecimento de urânio do Irã em Natanz foi um ataque que escalou para nível de um ataque armado? Para isso é necessária uma análise mais cuidadosa para determinar se ele se enquadra no DICA.

Pode ser difícil avaliar as consequências de ciberataques para determinar sua semelhança a um ataque armado, pois seus efeitos podem ser distorcidos. O artigo 49 do PA I, define um ataque armado como "atos de violência” contra o adversário, seja no ataque ou na defesa" (CICV, 1977).

Segundo Michael Schmitt, professor da *U.S. Naval War College* e da *Harvard Law School,* o termo "violência" deve ser considerado no sentido de consequências violentas, em vez de atos violentos, pois gera uma “angústia mental” que pode ser incluída no conceito de sofrimento humano; como a perda de ativos, tais como investimentos, poupança e bens, podem ser incluídos como dano ou destruição (SCHMITT, 2002).

Os princípios do DICA podem ser aplicados à GC quando um ataque cibernético é atribuído a um Estado com a intenção de causar sofrimento, dano ou destruição. Na concepção do DICA, o fato de elevar o nível de um ciberataque para ataque armado é um passo importante no contexto da GC, já que quando um Estado alvo estiver sob um ciberataque, este pode ser interrompido de maneira repentina, cessando assim o ataque e, portanto, não sendo aplicável o direito de legítima defesa (SCHMITT, 2002)

Já Graham (2010), membro do *The Judge Advocate General's Legal Center and School* da *U.S. Army,* considera que os critérios de uso da força propostos por Jean Pictet, notório jurista suíço, são parâmetros determinantes por considerar um ataque armado quando a

força aplicada tem escopo, duração e intensidade suficientes, onde reside o conceito de ("*Use of force Continuum"*) e aplicando-os em formas não convencionais do uso da força, como ciberataques. Segundo Graham, Pictet adotou esses critérios baseados em três modelos (GRAHAM, 2010):

a) O primeiro modelo pode ser designado como baseado numa abordagem instrumental (*instrument-based approach*). Usando esse modelo uma avaliação será efetuada com o intuito de saber se o dano provocado por um ciberataque poderia, previamente, ser apenas causado por um ataque cinético. Por exemplo, usando esse modelo e considerando o uso do *Stuxnet* às facilidades de enriquecimento de urânio iranianas, objeto deste trabalho, um ciberataque conduzido com o objetivo de colocar fora de funcionamento uma instalação nuclear seria considerado um ataque armado;

b) O segundo modelo pode ser designado como uma abordagem baseada nos efeitos (*effects-based approach*), sendo também frequentemente referido como um modelo baseado nas consequências. O critério desse modelo assenta no efeito global provocado pelo ciberataque, no(s) Estado(s) vítima(s) dele. Por exemplo, um ciberataque com interrupção de sistemas de infraestrutura crítica de um Estado, como das instituições financeiras, de energia, de transporte e a manipulação de seus "dados", causaria danos à população daquele Estado, podendo ser considerado semelhante a um ataque armado. Essa análise lida com as complexidades dos ciberataques, avaliando os seus resultados; e

c) O terceiro modelo assenta em uma abordagem baseada na responsabilidade objetiva (*strict liability*). Nessa abordagem, um ciberataque contra qualquer infraestrutura crítica seria, de forma automática, considerado um ataque armado.

Com relação aos eventos na instalação nuclear de Natanz, analisando o caso *Stuxnet*, tanto a partir da abordagem baseada nos efeitos ou da abordagem de responsabilidade objetiva, sugere que um ataque armado de fato ocorreu.

Embora não exista consenso sobre qual dos modelos citados é o mais adequado para resolver o problema, parece existir, na visão estadunidense, em que a reflexão sobre os aspectos legais se encontra mais avançada e aprofundada, a tendência para considerar mais adequada a *effects-based approach*, ou seja, a abordagem baseada nos efeitos.

Conforme já dito anteriormente, o próprio código do *Stuxnet*, o qual foi estudado por especialistas após o ataque em Natanz, revelou que seu objetivo era manipular o funcionamento das centrífugas de enriquecimento de urânio e destruir parte significativa de seus equipamentos (GRAHAM, 2010).

No que se refere à legalidade do uso da força no plano internacional, as disposições mais relevantes encontram-se na Carta das Nações Unidas. Esse documento contém um princípio geral de proibição do recurso à guerra, expressão *jus contra bellum*, ou seja, como tendência da sua proibição como modo de solução de conflitos internacionais, iniciada no pós-Primeira Guerra Mundial. O teor do artigo 2º § 4ºda Carta, diz que:

> Os membros deverão abster-se nas suas relações internacionais de recorrer à ameaça ou ao uso da força, quer que seja contra a integridade territorial ou a independência política de um Estado, quer seja de qualquer outro modo incompatível com os objetivos das Nações Unidas (NAÇÕES UNIDAS, 1945, p.3) (tradução nossa).

Porém, a proibição geral contida no artigo é matizada por duas exceções admitidas pela própria Carta. A primeira exceção está contida no artigo 39, conjugado com os artigos 41 e 42, e se refere às ações autorizadas pelo Conselho de Segurança (CS) da ONU, se necessário, incluir o recurso à força, que diz que:

> O Conselho de Segurança determinará a existência de qualquer ameaça à paz, ruptura da paz ou ato de agressão e fará recomendações ou decidirá que medidas deverão ser tomadas de acordo com os artigos 41º e 42º, a fim de manter ou restabelecer a paz e a segurança internacionais (NAÇÕES UNIDAS, 1945, p. 9) (tradução nossa).

A segunda exceção encontra-se vertida no artigo 51 e se refere à legalidade do direito de legítima defesa, individual ou coletiva:

> 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, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança (NAÇÕES UNIDAS, 1945, p. 10-11) (tradução nossa).

Porém, uma terceira exceção, não prevista na Carta da ONU vem da contribuição da jurisprudência que é relativa às chamadas guerras de libertação nacionais, que surgiram devido ao processo de descolonização africana.

Nela reside a tese de que o direito de legítima defesa existiria como direito inerente tanto sob os auspícios da Carta da ONU, quanto no direito costumeiro que encontra respaldo na decisão da Corte Internacional de Justiça (CIJ), portanto ainda válido, juntamente com as normas convencionais (DINH; DAILLIER; PELLET, 1999).

Em face desse dispositivo, o CS terá poder para autorizar os Estados a recorrerem a ações de GC? É inquestionável que esse órgão da ONU tem competência para autorizar os Estados-Membros a recorrerem ao uso da força ou outras medidas contra outros Estados. Todavia, isso só poderá ser feito, como determina o artigo 39, quando as ações de um Estado constituem uma ameaça ou ruptura da paz ou ato de agressão (GRAHAM, 2010).

Como faz notar David Graham, em seu artigo *Cyber Threats and the Law of War*, a experiência internacional de décadas tem mostrado grandes dificuldades na aplicação do dispositivo desse artigo, pois a maioria das decisões apenas chega após extensas e morosas deliberações e estão sujeitas ao veto de qualquer membro permanente do CS. Assim, dada a natureza nebulosa dos ciberataques e a morosidade do CS, parece válido assumir que um Estado lidará com os ciberataques pelo uso do seu direito de legítima defesa (GRAHAM, 2010).

Dessa forma, após as considerações acima feitas, adicionado a noção de que o "ato de força" não se resume aos atos de força cinética, levariam à clara conclusão de que seriam

aplicáveis os dispositivos do capítulo VII da Carta da ONU, referente ao direito de legítima defesa, aos casos em que a gravidade do ciberataque seja suficiente para tal equivalência.

Porém, a realidade se revela mais complexa. Os ataques podem ser realizados por atores não estatais, que não são contemplados pelos dispositivos supracitados. A atuação desses atores tem sido alvo de intenso debate e ganha relevância na GC.

Os novos atores, como as organizações terroristas, ONG e grandes corporações, fazem intenso uso desses recursos e são cada vez mais ativos. Além disso, existem soluções no quadro jurídico internacional atual. Se estivermos perante um ato de GC, esse poderá, verificando-se certos requisitos, ser considerado similar a um "ato de guerra" cinético, pois parece existir um motivo válido para aplicar as normas de DI ora em vigor.

Como já vimos anteriormente, o artigo 48 do PAI trata diretamente do princípio da distinção, em que são assegurados o respeito e a proteção da população civil e objetos civis. De forma semelhante, o PA II, referente aos conflitos armados não internacionais, em seu artigo 13, afirma que a população civil goza de proteção contra os perigos da guerra (CICV, 1977).

Também conforme abordagem anterior, vimos que são proibidos ataques à infraestrutura puramente civil quando a resultante interrupção ou destruição não produzam vantagem militar significativa. Além disso, esses princípios implicam que o atacante precisaria avaliar o potencial de danos colaterais a alvos civis durante um ciberataques para ser legítimo. Para ser coerente com a "Lei da Guerra", o uso de ciberataques durante um conflito teria que possuir as mesmas limitações que os ataques com a utilização de armas cinéticas (LEWIS, 2010).

Enfim, no contexto *Stuxnet*, surgem algumas indagações, como a questão de saber se o *worm* fez a distinção entre possíveis alvos civis e alvos militares localizados na instalação nuclear em Natanz. Outra questão é sobre se o ciberataque foi realizado de maneira que minimizasse os danos colaterais a objetos civis, por ocasião da inoperância de parte das centrífugas e quais foram os participantes diretos daquelas hostilidades.

Compreende-se, desta breve análise, que na maioria dos casos, as leis existentes para o conflito armado podem ser aplicadas a ciberataques, mas existem ambiguidades envolvendo a violação da soberania de terceiros, bem como a natureza dos danos causados pelos ciberataques que poderiam ser interpretados como um "ato de guerra". Há ainda poucos precedentes para resolver essas ambiguidades.

A seguir, a próxima seção abordará alguns tópicos de relevância sobre o Manual *Tallinn*, publicado recentemente pela OTAN, que tem como propósito estabelecer regras internacionais para a GC, à luz do DI.

5.2 MANUAL *TALLINN*

Diante dos ciberataques ocorridos na Estônia, em 2007, na Geórgia em 2008 e no Irã em 2010, com o evento *Stuxnet*, os Estados se voltaram para a segurança do ciberespaço.

Diante disso, em 2008, a convite do CCDCOE da OTAN e com sede na cidade de *Tallinn*, na Estônia, foi criado um grupo internacional de 20 especialistas em tecnologia e segurança cibernética, com a participação de acadêmicos, juristas e peritos técnicos no assunto e liderados pelo professor Michael Schmitt do *U.S. Naval War College*, na tentativa de estabelecer regras do DI aplicáveis a GC e juntos elaboraram o chamado Manual *Tallinn*[38], publicado em 2013. Nele estão contidas 95 regras comentadas (*black-letter rules*). O referido Manual é uma expressão das opiniões de um grupo de especialistas agindo sobre a premissa de sua própria capacidade intelectual, sem um alicerce legal (MÄLKSOO, 2013).

O principal ponto do Manual *Tallinn* é que as normas jurídicas costumeiras e existentes do DI existentes podem ser aplicadas e interpretadas no contexto de GC entre os Estados. Também diz que os Estados, que realizam operações cibernéticas, devem levar em conta que um ciberataque pode constituir uma violação das cláusulas da Carta da ONU em relação ao uso

[38] Disponível em: < https://ccdcoe.org/research.html >. Acesso em: 5 jun. 2015.

da força, dependendo da dimensão e consequências (perda de vidas, danos a objetos) e que um ato de agressão contra outro Estado, pode ser retaliado utilizando o direito da legítima defesa, inclusive com a utilização de armas convencionais (MÄLKSOO, 2013).

Além disso, trata das normas que regulam as questões de soberania, responsabilidade dos Estados, lei da neutralidade e os meios e métodos de ciberataques. Destacam-se outros pontos tais como, que a espionagem cibernética, roubos e ciberataques em *websites*, que não provoquem prejuízos ao nível estatal, não podem ser considerados como ataques armados. Também faz considerações sobre os ciberataques que podem ser equiparados a armas químicas, biológicas e radiológicas pela força da ação; e as operações cibernéticas destinadas a minar a confiança nas estruturas econômicas e governamentais dos Estados (MÄLKSOO, 2013).

A respeito da discussão sobre a atribuição de responsabilidade em um ciberataque, Sklerov (2009, p. 73-74), oficial do *U.S. Cyber Command* (USCYBERCOM), após realizar sua análise sobre esse tema, considerou que a própria tecnologia impõe limitações, pois pode ajudar a identificar a origem do ciberataque por meio de *softwares* de monitoramento e controle, detectando-o antes deles atingirem o seu ponto culminante. Porém isso é difícil acontecer e passível de erros de avaliação, devido ao fato de que sua condução é feita, normalmente, por outros computadores ou redes, espalhados pelo mundo, de modo a esconder a sua real autoria.

A ideologia do referido Manual é que a GC é regida pelas leis internacionais em vigor, as mesmas regras que regulam o início de um ataque armado (*jus ad bellum)* e as regras que regulam a conduta dos conflitos armados (*jus in bello)* e não se aprofundou na questão de responsabilidade penal, não havendo, portanto, um vazio legal (MÄLKSOO, 2013).

Em 2011, o mesmo grupo de especialistas também contribuiu no desenvolvimento da estratégia internacional estadunidense sobre o ciberespaço, o qual dizia que o desenvolvimento de normas para a conduta do Estado no ciberespaço não exige uma reinvenção do DI (WHITE HOUSE, 2011).

6 CONCLUSÃO

Com a revolução da informação, os conflitos interestatais no século XXI ocorrerão no ciberespaço, onde a Internet, as redes de comunicações, os sistemas de controle das infraestruturas críticas e seus serviços essenciais dos Estados estão totalmente interligados, tornando a informação com um considerável importância estratégica, cuja essência apoia-se na Teoria da Trindade de Clausewitz, pois é capaz de obrigar o inimigo a fazer a sua vontade pela da indução de "paralisia estratégica" para atingir fins desejados sem a aplicação de força física.

Assim, a GC se utiliza desses sistemas de informação para negar, corromper ou destruir essas mesmas infraestruturas de informação, mas agora do inimigo. O ciberataque com o *Stuxnet*, ocorrido em 2010, atraiu a atenção do público mundial, devido à crescente importância dessa temática para a sociedade global. Opiniões dos acontecimentos em torno dele, não trataram, adequadamente, as questões jurídicas envolvidas, pois ainda não há um consenso internacional e integrado, totalmente, dentro de um contexto jurídico do DI. Portanto não estamos perante um vazio jurídico.

Não obstante as dificuldades apresentadas, a comunidade internacional faz uso de uma interpretação analógica dos dispositivos do capítulo VII, e, em especial, do artigo 51 da Carta da ONU, que trata do direito de legítima defesa, conforme abordado no capítulo quatro, sendo a legitimação do uso da força por um Estado contra outro, quando da ocorrência de um ataque armado. Uma interpretação extensiva desse dispositivo poderia nos fazer pensar que os ciberataques seriam uma extensão dos ataques armados cinéticos, se estes ameaçam a paz e a segurança internacionais, em que estaria legitimado o uso da força para coibir tais ataques.

Contudo, levando-se em consideração a jurisprudência sobre a aplicação do DICA e conforme os modelos propostos por Jean Pictet para a adoção de critérios para o uso da força, há uma tendência a adotar a abordagem baseada nos efeitos (*effects-based approach*).

Após a rápida análise dos fatos baseados nos alicerces jurídicos que norteiam o DICA, realizada ao longo deste trabalho, podemos crer que os acontecimentos em torno do ataque às facilidades de enriquecimento de urânio em Natanz constituiu-se um ataque armado, na concepção do DICA. Os danos e a destruição necessários estão evidenciados pelo dano físico às suas centrífugas, sendo um ataque preciso e possivelmente usado para fins militares.

Embora distribuídos em uma rede ampla de computador em muitos países, o *Stuxnet* não provocou quaisquer danos colaterais e por essa razão, o ciberataque aderiu aos princípios de distinção e proporcionalidade, tendo como alvo o seu objetivo com precisão e praticamente sem danos colaterais.

A aplicação do DICA no campo de batalha virtual pode ser a chave para a busca de uma legitimação da GC, como conflito armado, não provocando um impacto normativo em seu arcabouço jurídico, mas sim tornando suas medidas de execução e controle mais difíceis, porém com possibilidades de êxito mediante a vontade política dos organismos internacionais.

A inexistência de uma legislação específica sobre a GC, baseada no DICA, tem efeitos práticos mais danosos que a mera dúvida doutrinária. Diante da impossibilidade de se conceituar adequadamente os “atos de força” cibernéticos, os atores, e especialmente aqueles que, por fazer extensivo uso de tecnologias digitais, são mais sensíveis a esses ataques, poderão fazer uso de uma leitura unilateral do uso da força e lançarem mão de seus direitos inerentes de legítima defesa individual ou coletiva para atos que dificilmente seriam caracterizados como tal pela doutrina jurídica atual.

Nesse contexto, a discussão e regulamentação multilateral tem o duplo papel de garantir a maior participação de atores que outrora dispunham de menor relevância, assim como evitar que ocorram excessos nas respostas ao uso da força, logo a construção de um documento normativo a partir do diálogo da comunidade internacional se mostra imprescindível.

Nesse sentido o Manual *Tallinn* apresenta os compromissos necessários, os benefícios para sua implementação, os próximos passos e medidas de sucesso para que isso aconteça.

Após a análise criteriosa realizada pelos especialistas que elaboraram aquele Manual, explorando a aplicação dos princípios fundamentais das Convenções, citadas ao longo do trabalho, só que agora para o ciberespaço e visa abrir o diálogo, construir uma confiança sustentável e ter um impacto positivo sobre a segurança cibernética.

Cada uma das recomendações focou em algumas questões cruciais: Podemos proteger infraestruturas críticas de entidades humanitárias de infraestruturas não protegidas no ciberespaço? Assim como a Cruz Vermelha designa uma entidade protegida no mundo físico, é viável a utilização de marcadores especiais para designar zonas protegidas no ciberespaço? Será que devemos reinterpretar os princípios das Convenções, levando-se em consideração que os "guerreiros" cibernéticos são muitas vezes atores não estatais? As armas cibernéticas possuem características análogas às armas proibidas pelo Protocolo de Genebra?

As normas do DI adotadas no referido Manual servem como um aviso para os Estados, e elas só serão obedecidas, se os Estados considerados como líderes mundiais e grandes potências derem um exemplo positivo.

A crescente participação dos atores não estatais nos conflitos internacionais desafia as antigas concepções do DI. O exemplo das organizações terroristas transfronteiriças é agravado no ciberespaço, que faz poucas distinções entre fronteira, levantando a inevitável questão da responsabilidade dos Estados perante as ações dos atores não estatais.

Para concluir, é certo que, com o crescimento exponencial da sofisticação tecnológica aplicada aos computadores e suas redes, as armas cibernéticas e novos métodos de ataque serão as novas ferramentas dentro do mundo cibernético. É um desafio para o DICA limitar danos a pessoas inocentes e restringir os combatentes no ciberespaço.

REFERÊNCIAS

ARQUILLA, John; RONFELDT, David (eds.). Cyberwar is coming. In Athena's Camp: Preparing for Conflict in the Information Age, First Edition, National Defense Research Institute, Chapter Two, 1997. Disponível em: <http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf>. Acesso em: 18 jun. 2015. Tradução nossa.

BELL, D. The Coming of Post-Industrial Society: A Venture in Social Forecasting, The Intercollegiate Studies Institute, New York, 1973. Disponível em: < http://www.mmisi.org/pr/09_01/ferkiss.pdf>. Acesso em: 30 jun. 2015. Tradução nossa.

BORGES, Leonardo Estrela. O Direito Internacional Humanitário: A proteção do indivíduo em tempo de guerra, Belo Horizonte: Editora Del Rey, 2006, p. 10.

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

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

BROAD, William J.; MARKOFF John; SANGER David E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay, Middle East, January 2011. Disponível em: <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>. Acesso em: 14 jun. 2015. Tradução nossa.

CCDCOE. Cyber Definitions. NATO Cooperative Cyber Defence Centre of Ecellence, Estônia, 2009. Disponível em: <https://ccdcoe.org/cyber-definitions.html>. Acesso em: 23 jun. 2015. Tradução nossa.

CLARKE, Richard A.; KNAKE Robert K. Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro, Brasport, 2015.

CLAUSEWITZ, Carl Von. DA GUERRA. 3 v. Tradução do original para o inglês por Michael Howard e Peter Paret. Tradução do inglês para o português por Luiz Carlos Nascimento e Silva do Valle. 1984. Versão em português disponível em: <https://www.egn.mar.mil.br/arquivos/cepe/DAGUERRA.pdf>. Acesso em: 16 jun. 2015.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA (CICV). Convenções de Genebra de 12 agosto de 1949. Disponível em: < https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions>. Acesso em: 06 jul. 2015.

_____. Os Protocolos Adicionais das Convenções de Genebra de 12 de agosto de 1949. Disponível em: <http://www.icrc.org/por/war-and-law/treaties-customary-law/genevaconventions/>.Acesso em: 06 jul. 2015.

_____. Resumo das Convenções de Genebra de 12 de agosto de 1949 e dos seus Protocolos Adicionais. Disponível em: <http://www.icrc.org/por/assets/files/publications/0368.007_resumo-das-convenções.pdf>. Acesso em: 06 jul. 2015.

CONVENÇÃO DE GENEBRA DE 1949. Convenção I de Genebra para a melhoria da sorte dos militares feridos e enfermos dos exércitos em campanha, de 12 de agosto de 1949. Genebra, 1949.

_____. Convenção II de Genebra relativa à melhoria da sorte dos feridos, enfermos e náufragos das forças armadas no mar, de 12 de agosto de 1949. Genebra, 1949.

_____. Convenção III de Genebra relativa ao tratamento dos Prisioneiros de Guerra, de 12 de agosto de 1949. Genebra, 1949.

_____. Convenção IV de Genebra relativa à proteção das pessoas civis em tempo de guerra, de 12 de agosto de 1949. Genebra, 1949.

DINH, Nguyen Qouc; DAILLIER, Patrick; PELLET, Alain. Direito Internacional Público, Lisboa, Fundação Galouste Gulberkian, 1999.

DTIC. JP 3-12(R) Cyberspace Operations, Joint Eletronic Library, February 2013. Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf>. Acesso em: 22 jun. 2015. Tradução nossa.

_____. DoD Instruction nº 8500.01(CYBERSECURITY), The Official Departament of Defense Website for DoD Issuances, march 2014. Disponível em: <http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf>. Acesso em: 21 jun. 2015. Tradução nossa.

DUNLAP Charles J. Perspectives for Cyber Strategists on Law for Cyberwar, Strategic Studies Quarterly (SSQ), v. 5, p. 81-99, 2011. Disponível em: <http://scholarship.law.duke.edu/faculty_scholarship/2368>. Acesso em: 25 jun. 2015. Tradução nossa.

GUERRA, Sidney. Direito Internacional dos Direitos Humanos, São Paulo: Editora Saraiva, 2011, p. 34 -37.

GRAHAM, David. Cyber threats and the law of war. Journal of National Security Law and Policy, v. 4, n. 1, 2010. Disponível em: http://www.jnslp.com/wp-content/uploads/2010/08/07Graham.pdf . Acesso em : 28 jun. 2015. Tradução nossa.

LANGNER, Ralph. To Kill a Centrifuge: A Technical Analysis of What Stuxnet´s creators Tried to Achieve, November 2013. Disponível em: <http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>. Acesso em: 21 jun. 2015. Tradução nossa.

LEE Robert M. Stuxnet and the Paradigm Shift in Cyber Warfare - A Brief History of the Stuxnet Worm Including Its Targets, Possible Creators of the Worm and Its Effects, 2011. Disponível em: < http://www.controlglobal.com/articles/2011/stuxnet-paradigm-shift-in-cyber-warfare/?start=0 >. Acesso em: 08 jun. 2015. Tradução nossa.

LEWIS, James A. A note on the laws of war in cyberspace, Center for Strategic & Internacional Studies, April 2010. Disponível em: <http://csis.org/publication/note-laws-war-cyberspace>. Acesso em: 03 jun. 2015. Tradução nossa.

MÄLKSOO Lauri. The Tallinn Manual as an international event, Diplomaatia, nº 120, Book Review, 2013. Disponível em: < http://www.diplomaatia.ee/en/article/the-tallinn-manual-as-an-international-event/ >. Acesso em: 12 jul. 2015. Tradução nossa.

NAÇÕES UNIDAS Carta. Charter of the United Nations and Statute of the Internacional Court of Justice, San Francisco, 1945. Disponível em: < https://treaties.un.org/doc/publication/ctc/uncharter.pdf>. Acesso em: 14 jun. 2015. Tradução nossa.

NCSC. CNSS Instruction nº4009 (National Information Assurance Glossary), Committee on National Security Systems, April 2010. Disponível em: <http://www.ncsc.gov/publications/policy/additional_interest.php>. Acesso em: 27 jun. 2015. Tradução nossa.

SCHILLING Voltaire. A história da Guerra: a horda mongol. Disponível em: < http://educaterra.terra.com.br/voltaire/mundo/2003/09/08/.htm>. Acesso em: 29 jun. 2015.

PAGANINI P. Plan X, new lymph to US cyber warfare capabilities, Security Affairs, June 2012. Disponível em: <http://securityaffairs.co/wordpress/6074/intelligence/plan-x-new-lymph-to-us-cyber-warfare-capabilities.html>. Acesso em: 20 jul. 2015. Tradução nossa.

PROTOCOLO ADICIONAL ÀS CONVENÇÕES DE GENEBRA. Protocolo I, de 8 junho de 1977. Dispõe sobre a proteção das vítimas dos conflitos armados de caráter internacional. Genebra, 1977.

_____. Protocolo II, de 8 junho de 1977. Dispõe sobre a proteção das vítimas dos conflitos armados caráter não-internacional. Genebra, 1977.

_____. Protocolo III, de 8 dezembro de 2005. Dispõe sobre a adoção de um emblema distintivo adicional. Genebra, 2005.

REZEK, Francisco. Direito Internacional Público, 10. ed. São Paulo: Editora Saraiva, 2006, p. 417.

SAMORE, Gary. Deal With It: How to Turn the Framework Agreement into a Comprehensive Nuclear Deal. FOREIGN AFFAIRS The Magazine Online, April 2015. Disponível em: <https://www.foreignaffairs.com/articles/iran/2015-04-05/deal-it>. Acesso em: 13 jun. 2015. Tradução nossa.

SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times, Middle East, June 2012. Disponível em: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>. Acesso em: 20 jun. 2015. Tradução nossa.

SCHMITT, Michael N. (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013. Disponível em: < https://ccdcoe.org/research.html >. Acesso em: 5 jun. 2015.

_____. Wired warfare: Computer network attack and jus in bello, International Review of the Red Cross, 2002. Disponível em: <https://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf>. Acesso em: 08 jul. 2015.

SKLEROV, Matthew J. To cyberattacks: a justification for the use of active defenses against states who neglet their duty prevent, p. 73 e74, 2009. Disponível em: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA517821> Acesso em: 10 jul. 2015.

SHARMA, A. Cyber Wars: A Paradigm Shift from Means to Ends, 2010. Disponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/01_SHARMA_Cyber_Wars.pdf>. Acesso em: 17 jun. 2015. Tradução nossa.

SYMANTEC. W32.Stuxnet Dossier, v. 1.4, February 2011. Disponível em: <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>. Acesso em: 22 jun. 2015.

THE ECONOMIST. The Stuxnet outbreak: A worm in the centrifuge, The Economist site, September 2010. Disponível em: <http://www.economist.com/node/17147818>. Acesso em 15 jun. 2015. Tradução nossa.

WEIGLEY Russell. Review: War and the Paradox of Technology, The MIT Press, v. 14, n. 2, 1989, p. 196. Disponível em: <http://www.jstor.org/stable/2538859>. Acesso em: 19 jun. 2015. Tradução nossa.

WHITE HOUSE. International Strategy for Cyberspace, 2011. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em: 07 jul. 2015. Tradução nossa.

_____. The Comprehensive National Cybersecurity Initiative, 2009. The WHITE HOUSE Foreign Policy. Disponível em: < https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>. Acesso em: 15 jul. 2015.

William J. Lynn III, Defending a New Domain: The Pentagon's Cyberstrategy, FOREIGNAFFAIRS The Magazine, v. 89. n. 5, September/October 2010. Disponível em: <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>. Acesso em 25 jun. 2015. Tradução nossa.

ANEXO

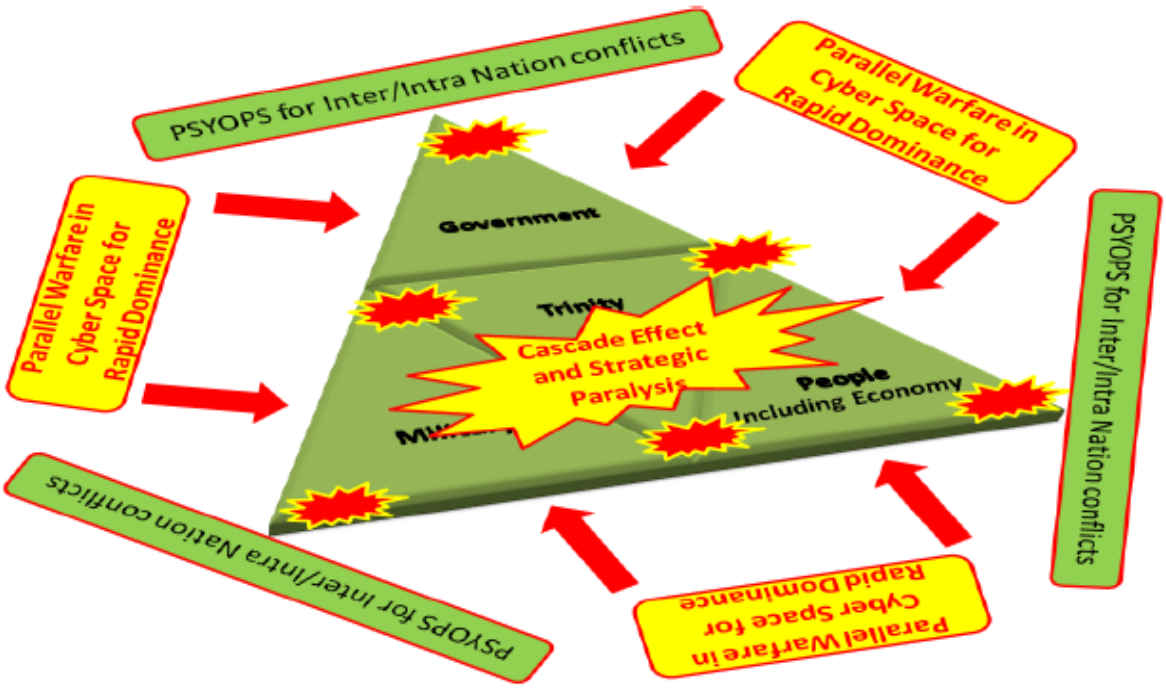

FIGURA 1 – Trindade Cibernética baseada em ciberataques paralelos para induzir um efeito de "paralisação estratégica" de um Estado.
Fonte: SHARMA, 2010, p. 7.