ESCOLA DE GUERRA NAVAL

CC LUCIANO MORAES DE OLIVEIRA

A CARTA DA ONU APLICADA À GUERRA CIBERNÉTICA:
uma análise do caso STUXNET

Rio de Janeiro

2014

CC LUCIANO MORAES DE OLIVEIRA

A CARTA DA ONU APLICADA À GUERRA CIBERNÉTICA:

uma análise do caso 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 L. Lima Martins

Rio de Janeiro

Escola de Guerra Naval

2014

RESUMO

O assunto desta monografia é a guerra cibernética e suas implicações, como uma nova modalidade de guerra, para o Direito Internacional. A metodologia utilizada para esta pesquisa foi o estudo de caso. O objetivo do trabalho foi verificar quais as implicações jurídicas podem ocorrer a partir da guerra travada neste novo campo de batalha: o espaço cibernético. A partir de um breve histórico da criação da Internet e, como consequência da sua criação, do surgimento do ciberespaço, mostra-se a utilização deste terreno virtual como um novo campo de batalha. Por meio do estudo do ataque cibernético perpetrado pelos EUA e Israel, com o vírus Stuxnet, ao Irã, foi possível verificar que, apesar de não haver ainda um ordenamento específico do Direito Internacional, é possível a aplicação das normas e tratados atualmente vigentes para que se regule a guerra cibernética e que o Manual de Tallinn, a despeito de ser apenas um guia para aplicação do DI, é o primeiro passo para a sua regulamentação.

Palavras-chave: Carta da ONU. Direito Internacional. EUA. Guerra cibernética. Irã. Israel. Manual de Tallinn. Stuxnet.

Sumário

1 INTRODUÇÃO

A guerra se refere, entre outras coisas, a conflitos entre sociedades e contendas políticas entre nações. Ela vem a mente como um confronto entre forças armadas, com bombas, artilharia, navios e tanques, onde um oponente deseja submeter o outro a sua vontade através da violência física evidente. Contudo, do final do século XX até o momento, depara-se com a possibilidade de a guerra não requerer mais o uso da violência.

A despeito disso não deve-se abolir as definições clássicas da guerra, mas, sobretudo, considerar novas definições, ou melhor, definições alternativas para a guerra. É importante cogitar a existência da guerra mesmo sem o uso convencional de armas. Conquanto a guerra seja "um ato de força para obrigar nosso inimigo a fazer nossa vontade"[1] não significa que a força seja manifestada claramente, como no lançamento de um artefato nuclear. Há uma enorme variedade de meios que podem persuadir, compelir ou coagir o inimigo. Tais meios podem não resultar, necessariamente, em destruição física de objetivos, mas podem levar o inimigo à rendição.

A arte da guerra sempre sofreu mudanças devido às revoluções tecnológicas. O surgimento da Internet criou uma nova maneira de se fazer a guerra, que não vale-se, necessariamente, da violência: a guerra cibernética. É necessário, então, pensar nas consequências jurídicas decorrentes da adoção desta nova modalidade de combate.

Esta nova realidade suscita as seguintes questões: é necessário adequar o ordenamento jurídico vigente à nova modalidade de guerra? Um ataque cibernético pode atentar contra a integridade e a soberania de um Estado? Há o direito de responder a um ataque cibernético, invocando a legítima defesa, com um ataque convencional?

---

[1] CLAUSEWITZ, *Da Guerra,* Tradução de CMG (RM1) Luiz Carlos N. S. do Valle, p. 75.

Para chegar às respostas dos questionamentos acima será estudado o caso Stuxnet, o ataque cibernético sofrido pelo Irã, nas usinas de enriquecimento de urânio de Natanz, e perpetrado pelos Estados Unidos da América (EUA) unido a Israel, apresentando as implicações jurídicas desta nova modalidade de guerra.

Para tanto na primeira seção de texto será abordado o aparecimento da Internet, o surgimento do ciberespaço e a sua definição e como os militares tiram proveito deste novo campo de batalha. Para isto discutir-se-á alguns casos em que se realizaram ataques cibernéticos e serão apresentados algumas armas cibernéticas e como elas poderão ser usadas.

No bloco seguinte será mostrado que todo sistema necessita de regras para que funcione e o Direito Internacional (DI), como um sistema que regula as relações internacionais entre os Estados, não seria diferente. Então, apresentar-se-á numa breve noção do DI. O tratado será relacionado como a principal fonte do DI e serão mostrados dois tipos de tratado, a Carta e a Convenção. Definir-se-á o que é agressão de acordo com a Resolução n.º 3.314 da Assembleia Geral (AG) da Organização das nações Unidas (ONU) e como a Carta da ONU regula a proibição ao recurso da força para as relações internacionais entre os Estados e o direito que eles têm de recorrerem ao uso da força, como legítima defesa, no caso de serem agredidos por um outro Estado.

Na terceira seção de texto será estudado o caso Stuxnet, como foi implantado o vírus no sistema que controla as centrífugas de enriquecimento de urânio e como foi descoberto que o Irã sofreu um ataque cibernético. Em seguida tratar-se-á das implicações jurídicas do referido caso.

Nesta monografia espera-se concluir que, baseado na Carta da ONU, o ataque às instalações de enriquecimento de urânio iranianas foi ilegal, e, fundamentado ainda na mesma Carta, questionar se o Irã possuiria o direito de agir em legítima defesa contra seus agressores.

2 A CRIAÇÃO DA INTERNET

Na década de 1960, em plena Guerra Fria, o Departamento de Defesa (DoD)[2] dos EUA planejou uma rede de troca e armazenamento de informações, que era descentralizada a fim de mitigar os riscos de comprometimento ou perda de conhecimento sigiloso no caso de um ataque pela União das Repúblicas Socialistas Soviéticas (URSS). A ARPA[3], Agência de Projetos de Pesquisa Avançadas do Departamento de Defesa estadunidense, criou assim uma rede chamada ARPANET[4]. O ataque esperado nunca ocorreu e tampouco os criadores de tal arquitetura imaginavam estar diante de um dos mais espetaculares fenômenos de comunicação. Na década seguinte, com a diminuição da tensão entre EUA e URSS, a ARPANET foi dividida em MILNET[5] e ARPANET, a primeira com os dados militares e a segunda, inicialmente usada no meio acadêmico, deu origem ao que conhecemos hoje como Internet[6] e aonde ela reside, o ciberespaço.

2.1 O Ciberespaço

Atribui-se o termo ciberespaço à William Gibson[7] que o usou em seu romance de ficção científica *NEUROMANCER*[8]. No livro o autor define o espaço cibernético como:

> Uma alucinação consensual, vivida diariamente por bilhões de operadores legítimos, em todas as nações,… Uma representação gráfica abstraída dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. (GIBSON, 1984, p.53).

---

2 Sigla para *Department of Defense*.
3 Sigla para *Advanced Research Projects Agency.*
4 Sigla para *ARPA Network.*
5 Sigla para *Military Network.*
6 O termo Internet significa *Interconnected Networks.*
7 Escritor norte-americano, ficou conhecido como "profeta *noir"* do *cyberpunk*, subgênero da ficção científica.
8 Esta obra de ficção foi publicada em 1984, em Nova Iorque, e inspirou a trilogia *THE MATRIX.*

Para o filósofo francês Pierre Lèvy[9] o ciberespaço designa:

> […] o universo das redes digitais como lugar de encontros e aventuras, **terreno de conflitos mundiais**, nova fronteira econômica e cultural. […] O ciberespaço designa menos os novos suportes de informação do que os modos originais de criação, de navegação no conhecimento e de relação social por ele propiciados (LÈVY, 1999, p.104, grifo nosso).

O espaço cibernético não é somente a Internet, e sim todas as redes de computadores e tudo o que a elas está conectado. A Internet é um sistema aberto de diversas destas redes, isto significa que de qualquer ponto de conexão quem quer que seja poderá acessar qualquer outro computador na Internet. O ciberespaço inclui ainda os demais sistemas que supostamente não são acessíveis através da Internet. Alguns destes sistemas são privados e, ao menos teoricamente, separados dos demais que são abertos. Há ainda outros sistemas como os que trafegam dados bancários, os de transações de crédito ou do mercado de ações e, ainda, os sistemas de controle que permitem que determinados equipamentos se comuniquem entre si, tais como, painéis de controle de geração de energia, elevadores, controles de tráfego aéreo e sistemas de comunicação. Sistemas como os mencionados poderiam despertar o interesse militar.

Qual seria, então, o interesse militar no espaço cibernético como um campo de batalha? Clarke e Knake dizem o seguinte:

> Se eles conseguirem uma rede, guerreiros cibernéticos poderiam roubar todas as suas informações ou enviar instruções que transfeririam seu dinheiro, causariam derramamento de óleo, vazamento de gás, explosão de geradores, descarrilamento de trens, incidente aéreo, enviar um pelotão para uma emboscada ou fazer com que um míssil detonasse em um alvo errado. […] Isto não é hipotético. Coisas assim já aconteceram, às vezes experimentalmente, às vezes por engano e às vezes como resultado de crimes cibernéticos ou guerra cibernética. (CLARKE; KNAKE, 2010, p.70-71. Tradução nossa).[10]

---

[9] Pierre Lévy é filósofo francês da cultura virtual contemporânea.

[10] If they take over a network, cyber warriors could steal all of its informations or send instructions that move money, spill oil, vent gas, blow up generators, derail trains, crash airplanes, send a platoon into a ambush, or cause a missile to detonate in the wrong place. […] These are not hypoteticlas. Things like this have already happened, sometimes e experimentally, sometimes by mistake, and sometimes as a result of cyber crime or cyber war.

Ter essa noção do espaço cibernético, entendendo-o como um campo de batalha sem fronteiras definidas, é relevante para que se entenda como são utilizadas as armas de ataque e defesa neste espaço e como se dá a guerra cibernética.

2.2 Uma conceituação da Guerra Cibernética

Será apresentado em seguida alguns fatos ocorridos desde o início deste século, a fim de se conduzir a alguns conceitos.

Em setembro de 2007 caças israelenses atacaram, no leste da Síria, uma fábrica que estava sendo construída em conjunto com a Coreia do Norte, pelo governo sírio. Esta fábrica, supostamente, produziria armas de destruição em massa. O ataque foi efetuado por caças F-15 Eagles e F-16, a partir da Turquia, sem que o sistema de defesa aérea sírio os detectasse. Esses aviões não possuíam a tecnologia *STEALTH*[11], então, o que possibilitou este ataque? A resposta é simples; foi uma ação de guerra cibernética que controlou aquilo que os radares sírios "enxergavam".

Foram aventadas três possibilidades para o ataque cibernético efetuado contra o sistema de defesa sírio. A primeira delas é que um VANT[12] israelense com tecnologia *STEALTH* tenha emitido sinais[13] que causaram mal funcionamento do sistema de defesa aérea sírio. A segunda é a possibilidade de que o código russo que controla o sistema de defesa aéreo tenha sido comprometido por agentes israelenses por meio de um *malware*[14] conhecido

---

[11] Palavra da língua inglesa que significa camuflagem. Diz-se da tecnologia que permite, por meio de uma seção reta radar reduzida ou de material que absorva a emissão eletromagnética dos radares, que aviões permaneçam quase "invisíveis" aos sistemas de detecção radar. (http://www.infoplease.com/encyclopedia/history/stealth-technology.html.).

[12] Veículo aéreo não tripulado.

[13] Os EUA possuem um sistema semelhante de ataque cibernético cujo nome é Senior-Suter. (CLARKE; KNAKE, 2010, p.7).

[14] *Malware* do inglês *malicious software* que significa programa malicioso. Utilizam-se de ferramentas populares de comunicação como e-mail e mensagens instantâneas para disseminar os *Malware.*

como *trapdoor*[15]. A terceira possibilidade é que, possivelmente, algum agente israelense achou um cabo de fibra ótica da rede de defesa aérea síria e por meio dele inseriu um *trapdoor*, permitindo o ataque aos radares sírios

Outro evento interessante ocorreu na Estônia, um dos países mais conectados do mundo[16]. A maioria de estonianos desta pequena nação báltica, após declarar sua independência no início da década de 1990, procurou remover qualquer sinal dos anos de opressão soviéticos. Um desses sinais era uma gigantesca estátua de bronze do soldado desconhecido soviético que se encontrava na principal praça da cidade de Tallinn, capital da Estônia.

Em 27 de abril 2007, depois de protestos, de um lado pelos soviéticos residentes naquele Estado e do outro por nacionalistas estonianos, foi decidido que a estátua e os restos mortais dos soldados russos, que também se encontravam ali, seriam removidos daquela praça para um cemitério das Forças Armadas. Após essa noite conhecida como "Noite de Bronze" (CLARKE e KNAKE, 2010, p. 12) diversos servidores de *webpages* foram inundados com acessos que colapsaram vários sistemas, como de redes bancárias, de sítios do governo, de sítios comerciais e outros.

O que atingiu a Estônia foi um DDoS[17]. Esse tipo de ataque é realizado por milhares, ou mais, computadores escravos[18] que acessam, simultaneamente, determinados sítios da internet. Esses computadores são infectados por meio de acessos a sítios com aparência inocente, mas que secretamente os infectam com *malwares* que os tornam

(http://us.norton.com/security_response/malware.jsp).

15 *Trapdoor*, alçapão em inglês, ou Cavalo de Troia são programas maliciosos de computador que executam ações não autorizadas pelo usuário como excluir, bloquear, modificar e copiar dados e atrapalhar o desempenho de computadores e redes. (http://brazil.kaspersky.com/internet-security-center/threats/trojans).

16 A Estônia, considerada uma das nações mais conectadas e tecnologicamente avançadas do mundo, e com altos índices de alfabetização em informática, e conhecida também como "E-stônia". (http://www.embaixada-americana.org.br/HTML/ijse0610p/estonia.htm).

17 Sigla para *Distributed Denial of Service* que significa ataques distribuídos de negação de serviço.

18 Esses computadores escravos são chamados *bootnets (robotic network),* uma rede de computadores zumbis controlados remotamente de forma não autorizada.

"zumbis".

Em 2009, pesquisadores canadenses descobriram um programa de computador altamente sofisticado, ao qual deram o nome de *GhostNet,* que tomou aproximadamente 1300 computadores em várias embaixadas ao redor do mundo. O programa tinha a capacidade de, remotamente, ligar a câmera e o microfone dos computadores infectados sem alertar seus usuários e, então, exportar imagens e sons silenciosamente para servidores na China. O alvo principal do *GhostNet* eram os escritórios de organizações não governamentais (ONGs) que trabalhavam nas questões do Tibet. A operação acontecia há vinte e dois meses até ser descoberta. No mesmo ano a inteligência do governo estadunidense vazou para a mídia que *hackers*[19] chineses haviam penetrado na rede elétrica e deixado mecanismos que poderiam ser usados para pôr aquele sistema em baixo.

Em meados da primeira década do século XXI foi criado o Comando Cibernético dos EUA, uma organização militar que tem como missão usar a tecnologia da informação e a Internet como uma arma. Comandos similares existem na Rússia, China e em um bom número de nações. Estas organizações militares e de inteligência estão preparando o campo de batalha cibernético com o que eles chamam de bombas lógicas[20] e *trapdoors,* colocando "explosivos" virtuais em outras nações em tempos de paz. Dada a natureza única da guerra cibernética, há incentivos para que se ataque primeiro, e os alvos mais prováveis são de natureza civil, como bancos, redes elétricas e sistemas de controle de voo. A velocidade com que milhares de alvos podem ser atacados, em qualquer lugar do mundo e simultaneamente, traz a perspectiva de crises de grande volatilidade e o que evitava a guerra nuclear, a deterrência, não funciona bem no caso de uma guerra cibernética, pois se uma nação expuser

[19] *Hackers* são usuários de software ou hardware extremamente hábeis que podem penetrar em computadores e redes de computadores, sem autorização, e adaptar os sistemas para fazerem coisas para as quais eles não estavam programados para fazer. (CLARKE e KNAKE, 2010, glossário).

[20] Bombas lógicas são aplicativos ou uma série de instruções que colocam um sistema ou rede de computadores em baixo e/ou apagam dados ou um programa de uma rede de computadores. (CLARKE e KNAKE, 2010, glossário).

o seu arsenal cibernético rapidamente ele poderá ser estudado e, facilmente, se tornar sem "poder de fogo". O fenômeno da guerra cibernética está envolto em segredos de estado que faz a guerra fria parecer um período de transparência.

Além destas características a guerra cibernética traz consigo um paradoxo. Quanto mais um Estado é desenvolvido tecnologicamente, mais ele é dependente da tecnologia e também é mais vulnerável a ataques cibernéticos. E aqui reside a lógica da importância do primeiro ataque. Caso uma nação muito poderosa, mas também bastante dependente dos seus sistemas informatizados, sofrer o primeiro ataque em seu *backbone*[21] poderá tornar-se rapidamente indefesa.

Essa mesma fraqueza também faz com que os Estados mais poderosos em termos cibernéticos que sofrem ataques no seu ciberespaço não têm o interesse de divulgar que foram atacados para não expor suas vulnerabilidades e os que atacam não queiram divulgar suas armas. Este fato acarreta não haver a divulgação de ações importantes tão logo elas ocorram.

Baseados nos breves exemplos anteriores, a guerra cibernética poderia ser definida, simplisticamente, como aquela travada no espaço cibernético, mas o que isso quer realmente dizer? Pode-se expressar um conceito de guerra cibernética e para tanto é necessário que se considere o espaço cibernético como uma simulação do espaço físico. Tal simulação está distante de ser ótima, mas possui propriedades suficientes para que se conduza uma guerra em seu próprio espaço.

Clarke e Knake (2010, p.6) definem guerra cibernética como as "[…] ações de um Estado para penetrar em computadores ou redes de outras nações com a finalidade de causar prejuízo ou distúrbios."[22] (Tradução nossa).

---

[21] A tradução literal é espinha dorsal. Refere-se às linhas principais de fibra-ótica, para transmissão de dados, que os Estados mais desenvolvidos possuem e que fluem os principais serviços na Internet.

[22] […] actions by a nation-state to penetrate another nation's computers or networks for the pourposes of causing damage or disruption.

O Departamento de Defesa dos EUA não apresenta uma definição específica para guerra cibernética e sim para operações no ciberespaço. O seu dicionário de termos militares diz que as operações no espaço cibernético são "o emprego das capacidades cibernéticas onde o propósito principal é alcançar objetivos no ciberespaço ou através dele."[23] (Tradução nossa).

Já o Ministério da Defesa (MD) brasileiro formulou o seguinte conceito para guerra cibernética:

> Conjunto de ações para uso defensivo e ofensivo de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informações e rede de computadores. Estas ações são elaboradas para obtenção de vantagens **tanto na área militar como na área civil**.[24] (Grifo nosso).

As potencialidades da guerra cibernética vão além do campo militar, atingindo qualquer área que se utiliza de sistemas informatizados. O uso do ciberespaço pelos Estados, para atingir seus objetivos políticos, diplomáticos ou militares, não é, necessariamente, seguido de um ataque convencional e uma nação pode empreender uma guerra cibernética como parte de ou em conjunção com formas mais tradicionais de condução da guerra. Pode, sobretudo, usar "artefatos cibernéticos" como armas estratégicas, já instaladas em tempo de paz, atingindo, como já mencionado, redes de produção de energia elétrica, sistemas de comunicação, sistemas bancários, etc.

Há muitas razões para se crer que, em um futuro bem próximo, a maioria das guerras convencionais serão precedidas de um ataque cibernético e que, por sua vez, ataques cibernéticos serão conduzidos como atividades isoladas, sem que seja necessário mobilizar os poderes terrestres, aéreos ou navais. Serão estes motivos suficientes para que surja a preocupação com a guerra cibernética? A julgar pelo que tem ocorrido ao redor do mundo nos últimos anos, sim. Além do que, na arte estratégia operacional procura-se como objetivos os

---

[23] The employment of cyberspace capabilities where the primary pourpose is to achieve objectives in or through the cyberspace. http://www.dtic.mil/doctrine/dod_dictionary/.

[24] BRASIL, Ministério da Defesa. MD35-G-01. Glossário das forças armadas. Brasília, 2007. p.123.

centros de gravidade do oponente e estes podem estar concentrados em um campo que não é necessariamente o militar, como, por exemplo, o poder industrial que sustenta uma nação, sendo, talvez, mais facilmente destruídos ou neutralizados por meio da guerra cibernética. E quais os motivos que levam a crer nesta afirmação? Clarke e Knake citam cinco:

> **A guerra cibernética é real.** O que nós temos visto até agora está longe de ser um indicativo do que pode ser feito. Muitas destas, bem conhecidas, escaramuças no espaço cibernético usaram armas cibernéticas primitivas[25] (com a notável exceção das operações de Israel). É uma suposição razoável que os atacantes não queiram revelar suas mais sofisticadas capacidades, ainda. O que os Estados Unidos e outras nações são capazes de fazer em uma guerra cibernética pode devastar uma nação moderna.
> **A guerra cibernética acontece na velocidade da luz.** Como os fótons de um pacote de ataque correndo por um cabo de fibra ótica, o tempo entre o lançamento de um ataque e seu afeito é escassamente mensurável, criando um risco para os tomadores de decisões de crises.
> **A guerra cibernética é global.** Em qualquer conflito, a guerra cibernética rapidamente torna-se global, computadores e servidores são adquiridos e hackeados por todo mundo são postos fora de serviço. Muitas nações são rapidamente atraídas.
> **A guerra cibernética ignora o campo de batalha.** Os sistemas de que as pessoas dependem, tanto bancos a radares de defesa aérea, podem ser acessados pelo ciberespaço e podem ser, rapidamente, tomados ou colocados em baixo sem, primeiro, derrotar as defesas tradicionais de uma nação.
> **A guerra cibernética já começou.** Em antecipação às hostilidades, algumas nações já estão "preparando o campo de batalha." Elas estão invadindo as redes e infraestruturas umas das outras e deixando *trapdoors* e bombas lógicas – agora, em tempo de paz. Esta natureza contínua de guerra cibernética, esta névoa de paz e guerra, traz uma nova dimensão de instabilidade. (CLARKE; KNAKE, 2010, p. 30-31. Tradução nossa, grifos do autor).[26]

---

[25] Quando o livro foi escrito ainda não havia ocorrido o ataque com o vírus Stuxnet, que será objeto de estudo deste trabalho.

[26] **Cyber war is real**: What we have seen so far is far from indicative of what can be done. Most of these well-known skirmishes in cyberspace used only primitive cyber weapons (with the notable exception of the Israeli operation). It is a reasonable guess that the attackers did not want to reveal their more sophisticated capabilities, yet. What the United States and other nations are capable of doing in a cyber war could devastate a modern nation.
Cyber war happens at the speed of light. As the photons of attack packets stream down fiber-optic cable, the time between the launch of an attack and its effect is barely measurable, thus creating risks for crisis decision makers.
Cyber war is global. In any conflict, cyber attacks rapidly go global, as covertly acquired or hacked computers and servers throughout the world are kicked into service. Many nations are quickly drawn in.
Cyber war skips the battlefield. Systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defenses.
Cyber war has begun. In antecipation of hostilities, nations are already "preparing the battlefield." They are hacking into each other's networks and infrastructures, laying in trapdoors and logic bombs – now, in peacetime. This ongoing nature of cyber war, the blurring of peace and war, adds a dangerous new dimension of instability.

Deparando-nos com as afirmações citadas percebemos que, assim como o advento da bomba nuclear suscitou uma nova percepção jurídica da guerra, a guerra cibernética também conduz a determinadas reflexões tais como o uso da força e o direito a legítima defesa no caso de um ataque cibernético. Na próxima seção serão discutidos as fontes do Direito Internacional (DI) e o ordenamento jurídico existente aplicado ao ciberespaço.

3 O DIREITO INTERNACIONAL

Vive-se em sociedade e para que os indivíduos possam bem se relacionar há a necessidade de que certas regras sejam estabelecidas. O jurista Celso de Mello define o Direito Internacional como "o conjunto de normas que regula as relações externas dos atores que compõem a sociedade internacional." (MELLO, 2004, p.77). Os atores internacionais são os Estados, organizações internacionais e os indivíduos. Dentre essas relações será estudada, especificamente, a guerra e as normas do DI afetas a ela.

Todo sistema minimamente organizado depende de regras para que funcione. No DIP[27] não seria diferente. Mello diz que "não pode existir sistemas que não possua normas imperativas. No DIP ocorre fenômeno idêntico." (MELLO, 2004, p.85). Quais seriam as normas imperativas do DI? Verdross, citado por Mello, "apontava como normas imperativas do DI: dever dos Estados proteger os estrangeiros, normas humanitárias e princípios da Carta da ONU regulando o uso da força." (MELLO, *loc. cit.*). A essas regras imperativas se refere como *jus cogens*[28]. O art. 53 da Convenção de Viena sobre os Direitos dos Tratados de 1969 define o que é *jus cogens:*

> […] Para os efeitos da presente Convenção. Uma norma imperativa de direito internacional geral é a que for aceita e reconhecida pela comunidade internacional dos Estados no seu conjunto como norma à qual nenhuma derrogação é permitida e que só pode ser modificada por uma nova norma de direito internacional geral com a mesma natureza. (Convenção de Viena, 1969).

---

[27] DIP – Direito Internacional Público usado aqui com o mesmo significado de Direito Internacional.

[28] *Jus cogens* – expressão latina que significa direito cogente, isto é, a lei que é absoluta e sua aplicação não depende da vontade das partes interessadas.

Para muitos autores as normas de *jus cogens* são aquelas que a sociedade internacional considera como indispensáveis para a sua existência, por isso tais normas não admitem a objeção persistente e criam obrigações internacionais para todos. Para que se possa identificar as normas de *jus cogens* tratar-se-á, a seguir, das fontes do Direito Internacional.

3.1 As fontes do DI

Os tratados são considerados atualmente a fonte mais importante do DI. A Convenção de Viena de 1969 define, em seu art. 1º, os tratados como sendo "um acordo internacional regido pelo direito internacional e celebrado por escrito, entre um ou mais Estados."

Há vários termos que dizem respeito aos tratados e serão citados dois que interessam para este trabalho e foram definidos por Celso de Mello:

> Convenção – é o tratado que cria normais gerais […]
> Carta – é o tratado em que se estabelecem direitos e deveres. É uma forma solene. Utilizado também para os instrumentos constitutivos de organizações internacionais. (Carta da ONU). (MELLO, 2004, p.213).

O tratado mais relevante para esta monografia é a Carta da Organização das Nações Unidas (ONU), assinada em São Francisco nos EUA em 26 de junho de 1945, e, especificamente, é de interesse para nosso estudo os seus art. 2º alínea 4 e o art. 51.

3.2 A Carta da ONU

Desde meados do século XX o DI tem buscado restringir o uso da força para solução dos conflitos nas relações internacionais dos Estados soberanos. Os artigos da Carta

da ONU que foram mencionados anteriormente tratam da proibição do uso da força e do direito à legítima defesa. Neste primeiro momento tratar-se-á do Art. 2º alínea (4), citado em seguida, que frequentemente é visto como uma pedra fundamental para o não emprego da força pelos Estados-membros da ONU para resolver seus conflitos:

> Todos os Membros devem evitar, em suas relações internacionais, a ameaça e o uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou em qualquer maneira inconsistente com os propósitos das Nações Unidas. (Carta da ONU, 1945).

O artigo acima é a regulação legal moderna do uso da força como instrumento de solução dos conflitos nas relações internacionais. Em consequência dele, qualquer uso da força é proibido, a não ser em dois casos: legítima defesa individual ou coletiva, regulado pelo art. 51, como se verá a seguir, ou quando for autorizado pelo Conselho de Segurança da ONU. Trata-se aqui da, quase, extinção do *jus ad bellum*[29]. Celso de Mello a esse respeito nos diz o seguinte:

> Até o século XX o *jus ad bellum* pertenceu ao Estado. O DI regulamentava a guerra entre os Estados. Atualmente, com a renúncia à guerra, os Estados perderam, teoricamente, o *jus ad bellum*. **O uso da força armada** está se tornando o monopólio da ONU e o seu emprego por ela não cria propriamente uma guerra, porque é apenas uma ação de polícia internacional. (MELLO, 2004, p.1504. Grifo nosso).

Há nesta citação um dado importante para a condução deste trabalho e uma consideração a ser feita quanto ao uso da força no que diz respeito à guerra cibernética. Pode-se considerar o uso de um *malware,* ou outro tipo de "artefato" cibernético, como uma arma? E seu uso por um Estado para atingir outro Estado como uso da força armada? A própria Carta da ONU não especifica o uso da força armada e sim "o uso da força contra a integridade territorial e a independência política de qualquer Estado". Neste contexto, poder-se-ia considerar um ataque cibernético um ato de agressão? Para responder estas questões será necessário recorrer à definição de agressão dada pela Resolução nº 3314 da Assembleia Geral

[29] *Jus ad bellum* – Expressão em latim que significa o direito à guerra.

(AG) da ONU, abaixo segue um extrato da referida Resolução:

> Art 1º – Agressão é o uso da força armada de um Estado contra a soberania, a integridade territorial ou a independência política de outro Estado, **ou de qualquer forma incompatível com a Carta das Nações Unidas**, tal como decorre da presente Definição;
> […]
> Art 3º - Qualquer dos seguintes atos, independentemente de uma declaração de guerra, são […] qualificados como atos de agressão;
> […]
> (b) – Bombardeio por força armada de um Estado contra o território de outro Estado ou **o uso de qualquer arma** por um Estado contra o território de outro Estado;
> […]
> Art 5º (1.) – **Nenhuma consideração de qualquer natureza**, mesmo que política, econômica, militar ou qualquer outra, **pode justificar um ato de agressão**.[30](Assembleia Geral da ONU. Tradução nossa, grifo nosso)

Como se pode observar na definição de agressão "o uso de qualquer arma, por um Estado, contra o território de outro Estado" é considerado como um ato de agressão, e, neste caso, considerar-se-ia o uso de armas cibernéticas, contra a soberania ou a integridade territorial de um Estado, como sendo um ato de agressão. De fato a ambiguidade na definição de agressão garante a aplicação do DI a uma vasta variedade de situações.

Uma das dificuldades relativas a um ataque cibernético repousam no fato de que definir o agressor nem sempre é tarefa fácil, visto que, tal tipo de ataque pode ser perpetrado de qualquer lugar do mundo para qualquer outro lugar, sem que seja possível rastrear a origem, propriamente dita, dele. Sendo assim como imputar a culpa de uma agressão desta natureza a determinado Estado.

Outra consideração a fazer é que, por exemplo, um ataque de uma força armada

---

[30] *Art 1º – Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or* ***in any other manner inconsistent with the Charter of United Nations****, as set out in this Definition;*
[...]
Art 3º – Any of the following acts, regardless of a declaration of war, shall […] qualify as an action of aggression:
[...]
(b) Bombardment by an armed force of a State against the territory of another State ***or the use of any weapons*** *by a State against the territory of another State;*
[...]
Art 5º (1.) – ***No considerations of whatever nature****, wether political, economic, military or otherwise,* ***may serve as a justification for aggression.***

convencional, independentemente de seus efeitos, é considerado sempre um ato de agressão. No caso de um ataque cibernético como mensurar seus efeitos a fim de que ele seja definido como um ato de agressão. Essas considerações são, de fato, importantes pois enseja a conjectura sobre o direito de legítima defesa dos Estados, no caso de sofrerem uma agressão. Portanto veja-se o Art. 51 da Carta da ONU.

> Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva se um ataque armado ocorrer contra um Membro das Nações Unidas, até que o Conselho de Segurança tome as medidas necessárias para manter a paz e a segurança internacional. As medidas tomadas por Membros no exercício do seu direito de legitima defesa devem ser comunicadas imediatamente ao Conselho de Segurança e não afeta de forma alguma a autoridade e a responsabilidade do Conselho de Segurança, sob a presente Carta, de tomar, a qualquer momento, as ações que julgar necessário para manter ou restabelecer a paz e a segurança internacional. (Carta da ONU de 1945)

Vê-se então que, na ocorrência de um ato de agressão contra sua soberania ou integridade territorial, um Estado poderá se defender contra este ataque. Celso de Mello diz que "a legítima defesa pressupõe a existência de um prejuízo, bem como a violação de uma obrigação jurídica. Ela é considerada um direito inalienável de um Estado." (MELLO, 2004, p. 454). Isto significa que um Estado não pode clamar o direito de agir em legítima defesa, se não houve prejuízo ou violação jurídica, como um pretexto para a agressão. Embora o direito de agir em legítima defesa possa parecer um pouco confuso, há critérios para que se determine a legalidade de se tomar uma ação em legítima defesa. Os princípios da necessidade e da proporcionalidade proveem estes critérios.

Ambos os conceitos são parte do *jus ad bellum;* são a justificativa moral para que se vá a guerra. Necessidade diz respeito a recorrer a legítima defesa somente como o último recurso. A noção de proporcionalidade implica o quanto da força pode ser utilizada, limitada em magnitude, intensidade e duração necessárias para conter a ação que suscitou a legítima defesa. Sabe-se também que, para que se configure o direito de legítima defesa, o ataque tem

que ser atual, isto é, estar ocorrendo no momento da resposta, pois do contrário seria represália.

Esta é outra dificuldade apresentada em relação a um ataque cibernético, posto que, tais ataques podem ser efetuados tão rapidamente quanto a velocidade da luz e causar efeitos devastadores. Então poderia ser questionado se haveria, ou não, tempo para a reação da vítima de modo que possa ser considerada como legítima defesa.

Reiterando o que já foi dito acima, já não cabe mais se falar em *jus ad bellum,* pois não mais existe um direito à guerra, é admitido, portanto, falar-se em direito à legítima defesa.

Diante de um ataque iminente ou a possibilidade de um ataque há autores que defendem a tese da validade da legítima defesa preventiva. Um determinado Estado ataca antes de ser atacado alegando que o fez para se defender. Contudo a legítima defesa preventiva está sujeita a várias objeções, como a imprecisão e a avaliação errônea da situação. No caso de uma ataque cibernético essa imprecisão é, ainda, mais proeminente, visto que é difícil atribuir a autoria de um ataque quando ele ocorre, mais ainda, seria atribuí-la quando na iminência de ocorrer.

Em 2013, como uma tentativa de que fossem estabelecidas regras básicas de DI para a guerra cibernética, foi publicado o Manual de Tallinn[31]. Este manual foi organizado sob os auspícios da Organização do Tratado do Atlântico Norte (OTAN) e coordenado por Michael Schmitt, membro sênior do *NATO Cooperative Cyber Defence Centre of Excellence*[32]. A confecção do Manual contou com a colaboração de cerca de vinte especialista dentre, acadêmicos, juristas e militares. Esta publicação, entretanto, não é uma norma, mas, sobretudo, uma orientação acadêmica de como o DI, no que diz respeito ao *jus ad bellum* e ao

[31] Manual de Tallinn – Título original *Tallinn Manual on the Internacional Law Applicable to a Cyber Warfare.*

[32] Centro de Excelência de Cooperação de Defesa Cibernética da OTAN.

jus in bellum, pode ser aplicado à guerra cibernética[33].

O referido Manual, na sua regra n.º 11, define que "uma operação cibernética constitui-se em uso da força quando sua dimensão e efeitos são comparáveis a uma operação não cibernética que seja considerada como uso da força."[34] No mesmo texto está definido, na sua regra n.º 13[35], que o direito a legítima defesa somente poderá ser invocado caso se sofra um ataque cibernético que, devido a sua dimensão e seus efeitos, seja considerado um ataque armado.

Na próxima seção apresentaremos o caso Stuxnet, suas relações com o ordenamento jurídico atual e suas implicações para o futuro do DI.

---

[33] <http://en.wikipedia.org/wiki/Tallinn_Manual>.
[34] Manual de Tallinn, 2013, p.47.
[35] Manual de Tallinn, 2013, p.53.

4 O CASO STUXNET E SUAS CONSIDERAÇÕES PARA O DI

O ataque com o vírus Stuxnet perpetrado às usinas de enriquecimento iranianas, localizadas na cidade de Natanz, na região central do território, pode ser considerado como o primeiro ataque cibernético com uma arma sofisticada desenvolvida especialmente para este fim. Em seguida será apresentado este caso e as suas implicações para o DI.

4.1 O caso STUXNET

Em janeiro de 2010 durante uma visita da Agência Internacional de Energia Atômica (AIEA) às fábricas de enriquecimento de urânio iranianas, em Natanz, os inspetores constataram que algo não estava funcionando bem. Normalmente, a taxa de reposição de centrífugas de enriquecimento de urânio era de 10% ao ano, isto é, das 8.700 existentes lá, em torno de oitocentas eram repostas anualmente. Contudo verificou-se que mais de 1000 delas foram substituídas em, apenas, alguns meses. Qual teria sido o motivo para esta discrepância? Os inspetores não tinham conhecimento do que havia de errado e nem tinham autorização para perguntar, pois o motivo de sua visita era ter conhecimento do material radioativo processado nas centrífugas, mas era claro que algo as havia danificado.

Meses antes, em junho de 2009, os computadores que controlavam as centrífugas foram infectados com um *worm*[36] com o intuito de sabotar o programa de enriquecimento de urânio iraniano e prevenir o Presidente Mahmoud Ahmadinejad de suas possíveis intenções de construção de um artefato nuclear.

---

[36] *Worm* palavra em inglês que significa verme. Em informática diz-se do programa malicioso que é autorreplicante e pode executar tarefas destrutivas em um computador ou rede de computadores. (http://www.symantec.com/security_response/glossary/define.jsp?letter=w&word=worm).

Este vírus, na visão de dezenas de estudiosos da segurança de informações digitais, foi um dos mais complexos *malwares* já escritos, tornando-se a primeira arma cibernética real já vista no mundo.

Em junho de 2010 Sergey Ulasen, líder da divisão antivírus de uma pequena empresa bielorrussa de segurança de informações digitais, situada em Minsk, a VirusBlokAda, recebeu em seu escritório um e-mail com o relatório de um cliente no Irã. Os computadores estavam em um *loop* de reinicialização, isto é desligavam e religavam várias vezes, sem o controle dos operadores. Percebeu-se que os computadores estavam infectados por algum tipo de vírus.

O ramo de empresas que atuam na área de segurança da computação tornou-se, nos últimos anos, uma indústria de bilhões de dólares em virtude da quantidade enorme de ataques de *hackers* e de vírus em evolução.

Empresas como Symantec, Macfee e Kaspersky são nomes conhecidos neste ramo de anti-vírus, mas a pouco conhecida VirusBlokAda é uma pequena neste setor.

A equipe de Ulasen examinou os computadores infectados e diagnosticaram que o *malware* explorava o *zero-day*[37], uma vulnerabilidade do sistema. Esses programas são armas muito potentes para os hackers e também muito raras, pois é preciso ter muita habilidade para encontrar essas vulnerabilidades e explorá-las. São mais de 12 milhões de novos vírus achados todos os anos e apenas algumas dezenas são os que exploram o *zero-day*.

O vírus encontrado nos computadores de Natanz foi espalhado, de um computador para outros, por meio de um *pendrive.* A vulnerabilidade estava em um arquivo do Internet Explorer, um programa do sistema operacional do Microsoft Windows. O vírus infectava o

---

[37] *Zero-day* – É o dia que os pesquisadores de segurança anunciam a descobertas de uma nova vulnerabilidade em um sistema. Isso inicia o tempo entre a descoberta da vulnerabilidade e a sua correção, dando a opotunidade de que essa vulnerabilidade seja explorada. (http://www.symantec.com/security_response/glossary/define.jsp?letter=z&word=zero-day).

sistema da seguinte maneira. Um *pendrive* contaminado é inserido no computador, automaticamente o programa Explorer do Microsoft Windows escaneia o conteúdo do *pendrive,* neste momento o código do vírus é copiado para dentro do sistema sem que o usuário perceba. Parte deste código está criptografada no computador. Pode-se associar esse processo ao de combatentes de operações especiais lançados camufladamente no terreno inimigo.

A empresa VirusBlokAda informou a Microsoft da descoberta. O vírus foi apelidado de Stuxnet, combinação dos nomes de dois arquivos encontrados em seu código, stub e mrxnet.sys. Descobriu-se também que o vírus havia sido lançado em junho de 2009 e que já havia sido aperfeiçoado desde a primeira ação até sua descoberta. O Stuxnet utilizava-se de certificados digitais[38] de empresas como Realtek Semicondutores, fabricante de *hardware*, e JMicron Technology, fabricante de circuitos integrados, ambas as empresas sediadas em Taiwan. Estes certificados davam uma aparência confiável ao vírus. Um vírus de computador apresentar esse método para se tornar confiável é extremamente raro, segundo as empresas de segurança digital, devido a isso concluíram que quem implantou o *malware* possuía muitos recursos, tanto técnicos quanto financeiros.

O Stuxnet atuava no sistema SCADA[39] da SIEMENS, empresa com sede na Alemanha que atua na área de automação de sistemas, este sistema controla o funcionamento das centrífugas. Vírus que atuem neste tipo de sistema não são comuns, pois não possuem muito apelo financeiro. Inicialmente o ataque parecia um caso de espionagem industrial para roubar dados de funcionamento do sistema que permitissem a sua fabricação por uma empresa

---

[38] O certificado digital é um código que dá a garantia de que um programa foi realmente produzido por determinada empresa, possuidora da certificação. O certificado da credibilidade ao programa e segurança ao usuário.

[39] SCADA – *Supervisory Control and Data Acquisition* – O sistema de supervisão e controle de aquisição de dados serve para controlar remotamente equipamentos como as centrífugas da fábrica de enriquecimento de urânio de Natanz. É também utilizado em indústrias de alimentos, controladores de gasodutos e estações de tratamento de água, entre outros.

concorrente, mas não foi o caso. O vírus atuava acelerando e desacelerando aleatoriamente as centrífugas e também as ligando e desligando em intervalos muito curtos, acarretando com isso a avaria em grande quantidade de equipamentos.

A Symantec interessou-se, especialmente, por esse vírus por vários motivos. Não era um programa curto, como geralmente são os desse tipo. Em vez dos 15 Kbytes usuais para esse caso o programa possuía 500 Kbytes. Explorava o *zero-day,* já dito acima que é uma raridade. O vírus era muito sofisticado com uma imensa quantidade de comandos e dados bastante eficiente. O código utilizado era complexo demais para ser apenas espionagem.

Os especialistas da Symantec conseguiram mapear os computadores infectados pelo Stuxnet e chegaram ao seguinte padrão. Das 38.000 máquinas infectadas no mundo inteiro, 22.000 localizavam-se no Irã. Outras nações infectadas foram a Indonésia com 6.700 máquinas, a Índia com cerca de 3.700, além de outras, os EUA apareciam com apenas 400 máquinas infectadas. De todas as máquinas infectadas um número menor ainda possuía o sistema que interessava aos criadores do vírus, eram 216 máquinas no Irã e 16 nos EUA.

Devido ao número de infecções tão fora dos padrões vistos até o momento, pareceu muito claro que o centro dos ataques era o Irã. Fato importante de ser citado é que os ataques cessaram antes que se descobrissem os seus autores. A sofisticação do código, os certificados fraudulentos, o custo para fabricar esse tipo de arma e a região central do ataque, a República do Irã, fez os especialistas chegarem a conclusão de que o ataque era obra de um centro de guerra cibernética estatal.

O vírus foi desenvolvido pelos EUA e Israel, como parte da operação *Olympic Games*[40]*,* a fim de atrasar o programa nuclear iraniano. A arma atingiu seu objetivo e retardou o programa de enriquecimento de urânio iraniano em, pelo menos, dois anos. Se o Stuxnet é

[40] A operação *Olympic Games* foi iniciada na administração Bush e o presidente Obama acelerou os ataques logo que assumiu o governo. <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0>.

uma arma cibernética, qual as consequências de sua utilização para o ordenamento jurídico?

4.2 As implicações jurídicas

O Irã manteve-se em silêncio sobre o caso Stuxnet até recentemente, mas o governo pretende levar o caso aos tribunais internacionais. Quais seriam as disposições que este caso poderia suscitar neste processo?

Parece muito claro que os agentes que lançaram o Stuxnet violaram um dos textos mais elementares do DI e cujos termos são aceitos como *jus cogens,* a Carta da ONU.

O Art. 2º (4) da Carta deixa claro que "os Membros devem evitar, em suas relações internacionais, a ameaça e o uso da força contra […] a independência política de qualquer Estado […]." Embora o sentido de força apresentado na Carta seja amplo o suficiente para que se considere ambos os ataques, armados e não armados, como uso da força, a maioria dos juristas ainda considera como força àquela associada à força armada. Contudo, isso não significa que a proibição do uso da força esteja, necessariamente, associada aos ataques cinéticos, nucleares, biológicos ou químicos. Entendendo o uso da força como a coerção de um Estado por outro Estado, podemos caracterizar certos atos que não são força física, mas que envolvem a coerção, como um ataque cibernético, incompatíveis com a Carta da ONU.

A Resolução n.º 3314 da AG da ONU menciona, em seu art. 3º alínea (b), que agressão é "o uso de qualquer tipo de arma por um Estado contra a integridade de outro Estado." Com efeito, parece ser incontestável que um ataque cibernético pode ser abrangido pela proibição do uso da força previsto no artigo 2º (4) da Carta da ONU.

Pode-se dizer que, como depreendido da regra nº 11 do Manual de Tallim, atingir a infraestrutura industrial de um Estado é atingir a sua integridade e soberania. Respeitar a infraestrutura industrial, tanto quanto o território, de outro Estado é um dos princípios básicos do DI. Verifica-se, então, que o ataque cibernético às instalações nucleares iranianas foram, sim, uma ato de força ilegal sob a ótica do que está disposto na Carta da ONU.

Não há dúvida de que se a usina de Natanz fosse atacada por um míssil e, da mesma forma, atrasasse o programa nuclear iraniano destruindo a mesma quantidade de centrífugas destruídas por meio do ataque cibernético com o vírus Stuxnet, não haveria dúvidas em se considerar aquele ato como de força. Contudo o que ocorreu lá pode ser considerado como interferência, promovida pelos EUA e Israel, com o programa de enriquecimento de urânio iraniano, atingindo, desta forma, a soberania e a independência política daquele Estado. Se forem confrontadas as consequências do ataque cibernético com o exemplo dado de lançamento de um míssil o efeito desejado seria o mesmo. O Manual de Tallinn, na alínea (7) da regra n.º 1[41], diz que uma operação cibernética com o intento de coagir um governo se constitui em uma intervenção ou uso da força proibidos. Portanto, perpetrar um ataque cibernético que destrua ou danifique uma indústria de um Estado estrangeiro, com o intuito de interromper ou atrasar um programa estatal, independente da extensão do dano causado a ela, claramente, viola a Carta da ONU. O ataque foi um ato de força ilegal, frente às disposições jurídicas vigentes, o que permite que o Irã tome medidas legais cabíveis.

O outro artigo da Carta da ONU, que foi mencionado acima, se refere ao direito inerente de legítima defesa. No artigo 51 está claro que um Estado tem o direito de agir em legítima defesa quando "um ataque armado ocorrer." A regra n.º 13 do Manual de Tallinn diz que para uma operação cibernética ser considerada um ataque armado dependerá de sua

[41] Manual de Tallinn, 2013, p. 26.

dimensão e de seus efeitos.

A legítima defesa somente poderá ser aplicada ao agressor devidamente definido, coisa que normalmente não é possível em um ataque cibernético. Outro dado importante é que um Estado que sofre uma agressão somente poderá invocar seu direito a legítima defesa, respeitando os princípios da necessidade, da proporcionalidade e da iminência, a fim de interromper o ataque de que está sendo vítima naquele momento, pois caso responda a agressão muito tempo depois o ato seria considerado como retaliação, o que é proibido pelo DI.

Em essência o DI permite que um Estado responda, de maneira convencional, a um ataque cibernético. Na alínea (3) da regra n.º 13 do Manual de Tallim diz que certas operações cibernéticas podem gerar consequências que justifiquem considerá-las com ataque armado, mesmo que elas sejam caracterizadas por sua natureza não cinética, e, sendo assim, poderiam ser respondidos com um ataque armado em legítima defesa.

No caso em lide, o DI não permitiria que o Irã contra-atacasse os EUA ou Israel. Essa proibição seria menos pela natureza do ataque e suas consequências do que pelo tempo ocorrido entre as ações e a conclusão de que elas foram fruto de uma operação cibernética. Conforme já exposto um ataque para interromper um ataque cibernético não pode ser retaliatório; o Stuxnet foi descoberto ainda em 2009 e até 2010, quando o vírus já não era mais efetivo, ainda não havia sido, totalmente, identificado. O ataque já havia terminado quando foi descoberto e, assim, o Irã não poderia retaliar, pois não é permitido pelo DI. Caso a operação fosse descoberta enquanto ocorria poderia ser usado, no seu direito a legítima defesa, um ataque convencional para responder ao ataque cibernético, e eles estariam amparados pelo DI. Portanto o remédio jurídico, neste caso, é o protesto diplomático junto aos órgãos internacionais e a tentativa de reparação, restando ao Irã apenas esta alternativa legal.

Estudando o caso Stuxnet observa-se que, a despeito da ilegalidade da operação *Olympic Games,* perpetrada pelos EUA e Israel, por ter ferido a soberania e a integridade política e econômica do Irã, eles não poderiam agir, a fim de responder, em legítima defesa, em virtude do lapso temporal entre o ataque cibernético e a sua descoberta.

Tanto a Carta das Nações Unidas como os demais tratados e códigos internacionais foram criados numa época em que as agressões e as ameaças de agressão a um determinado Estado, por outro, eram sempre visíveis, como a movimentação de tropas, o ataque armado e a invasão de território. A guerra cibernética surge como uma nova modalidade de conflito, de caráter deveras furtivo.

Não há, ainda, leis internacionais claras e específicas que definam tudo o que diz respeito à guerra no contexto cibernético. A equivalência entre um ataque armado e um ataque cibernético não é consistente em uma interpretação estreita da legislação em vigor. O Manual de Tallinn, promovido pela OTAN, não é um ordenamento jurídico ainda, mas um guia para que se interprete, no contexto cibernético, as normas e os costumes internacionais vigentes.

A dependência e a confiança da sociedade moderna nos sistemas informatizados pressupõe que os ataques cibernéticos são formas não convencionais de fazer guerra que podem causar muito mais danos nas infraestruturas críticas de um Estado, tais como sua rede de distribuição de energia ou seus sistemas de controle de tráfego aéreo, e trazer mais ameaça a eles do que um ataque convencional.

Conforme visto anteriormente não há muitos conflitos ou ações de guerra cibernéticas conhecidas, porque talvez elas não ocorrem tão claramente, para que se crie jurisprudência. A criação de uma legislação que seja específica ao conflito no ciberespaço se reveste de um fator complicador. A capacidade cibernética ofensiva de um Estado traz consigo certa similaridade com um ataque convencional, contudo, ao mesmo tempo, carrega

características únicas e evoluem muito rapidamente e de forma pouco previsível. Por consequência qualquer conceito jurídico mais específico pode se tornar obsoleto muito rapidamente. Neste aspecto parece ser mais interessante que se tenha, ao menos por enquanto, legislação mais genérica e fim de abraçar qualquer uso ilegal da força no ciberespaço e, caso aja, permitir a vítima que responda em legítima defesa.

5 CONCLUSÃO

Este trabalho seguiu o seguinte caminho. Na primeira seção de texto foi apresentado um breve histórico de como surgiu a Internet e, como consequência dela, o ciberespaço. Tratou-se do interesse militar no espaço cibernético como um "terreno" recém-criado para que surgisse uma nova modalidade de guerra. Foram expostos alguns exemplos de como essa nova modalidade de guerra, a guerra cibernética, pode acontecer e quais são os cinco motivos que sustentam a afirmação de que a ciberguerra é uma realidade e deve haver uma preocupação com a sua ocorrência. São eles: a guerra cibernética é real, ela acontece na velocidade da luz, ela é global, a guerra cibernética ignora o campo de batalha e ela já começou. A seção foi encerrada com a ideia de que se deve adequar o DI a esta nova modalidade de conflito.

No segundo segmento de texto foi mostrado que todo sistema minimamente organizado depende de regras que o façam funcionar perfeitamente. No DI essas regras existem, obviamente, e são regras imperativas, as quais se dá o nome de *jus cogens*. Foi mencionado que os tratados são as fontes mais importantes do DI. Também definiu-se dois tipos de tratados: a Carta e a Convenção. Ainda nesta seção foram apresentados dois artigos da Carta da ONU, considerados os mais importantes para esse estudo: o art. 2º (4), que trata da proibição do uso da força nas relações internacionais entre os Estados, e o art. 51, que trata do direito de legítima defesa. No final desta seção relacionou-se o art. 2º (4) com os ataques cibernéticos, apresentou-se a definição de agressão, de acordo com a resolução 3.314 da AG da ONU, e se tratou do direito à legítima defesa, disposto no art. 51, no caso de um Estado sofrer um ataque cibernético. Foi apresentado, também o Manual de Tallinn, orientação acadêmica de aplicação do DI à guerra cibernética.

Nesta seção foi visto que um ataque cibernético poderá, sim, ferir a soberania, a integridade ou a independência política de um Estado. De acordo com o Manual de Tallinn, um ataque cibernético será considerado como uso da força se seus efeitos e sua dimensão se equivalerem ao de um ataque convencional. Um Estado que sofra um ciberataque poderá responder, em legítima defesa, até mesmo com uma operação convencional, desde que cumpra os requisitos da necessidade, da proporcionalidade e da iminência e tenha claramente o seu agressor definido.

Chegou-se a conclusão de que o Irã sofreu um ataque, previsto como agressão, de acordo com a Resolução 3.314 da AG da ONU, ilegal sob a ótica do DI, visto que a interferência em seu programa de enriquecimento de urânio foi um atentado contra a sua independência política e a sua soberania, previsto no art. 2º (4) da Carta da ONU.

A despeito da ilegalidade da ação estadunidense israelense, o governo iraniano não tinha respaldo legal para responder ao ataque cibernético, invocando o art. 51 da Carta da ONU, que trata de legítima defesa, pois houve um lapso temporal demasiado entre o cessamento dos ataques e a descoberta de que esse foi o motivo dos danos causados às centrífugas de Natanz. Caso o Irã atacasse os EUA ou Israel na ocasião da descoberta do vírus essa ação seria considerada como retaliação, o que é ilegal. Restou à República do Irã, apenas, a possibilidade de recorrer, com um protesto diplomático aos órgãos internacionais de justiça, a fim de ter algum tipo de reparação.

Abordou-se, ainda, o paradoxo da guerra cibernética em que quanto mais um Estado é desenvolvido e dependente dos seus sistemas informatizados, mais vulnerável ele é, devido mesmo a sua dependência.

Conclui-se que em virtude da falta de jurisprudência no ambiente da guerra cibernética, não há, até o momento, leis específicas que regulem os conflitos neste terreno, há,

contudo, uma orientação, dada pelo Manual de Tallinn. Também chega-se a conclusão de que devido há velocidade e a imprevisibilidade com que as evoluções ocorrem no ciberespaço um ordenamento jurídico mais específico pode se tornar obsoleto antes mesmo que se tenha a oportunidade de se colocá-lo em prática.

Finalmente, contatou-se que não há, ainda, uma guerra cibernética de larga escala ocorrendo e, por isso, as nações que possuem arsenais cibernéticos ainda não os apresentaram em sua totalidade, não permitindo que se preveja os resultados de um conflito cibernético de grandes proporções. Entretanto é certo que os paradigmas jurídicos do *jus ad bellum,* no ciberespaço, terão que ser transformados.

REFERÊNCIAS

BRASIL, Ministério da Defesa, *Glossário das Forças Armadas MD-34G01,* 4. ed, 2007. 278p. Disponível em: <http://www.hmab.eb.mil.br/downloads/outros/glossario_fa.pdf>. Acesso em: 20 Abr. 2014.

BROAD, William J.; MARKOFF, Jonh; SANGER, Devis E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *The New York Times*, 15 Jan. 2011. Disponível em: <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all& module= Search&mabReward=relbias%3Ar>. Acesso em: 26 Apr. 2014.

BROAD, William J.; SANGER, Devis E. Worm was perfect for sabotaging centrifuges, *The New York Times*, 18 Nov. 2010. Disponível em: <http://www.nytimes.com/2010/11/19/ world/middleeast/19stuxnet.html?pagewanted=all&module=Search&mabReward=relbias%3 Ar > Acesso em: 26 Apr. 2014.

CAN, Murat. Stuxnet and international law: Possible scenarios. *The Turkish Journal*, 15 May 2014. Disponível em: <http://www.turkishweekly.net/op-ed/3185/stuxnet-and-internacional-law-possible-scenarios>. Acessso em: 15 June 2014.

CLARKE, Richard A.; KNAKE, Robert K. *Cyber War*: The next threat to national security and what to do about it. Version 08102012: Harper-Collins e-books, 2010. 279 p.

CLAUSEWITZ, Carl Von. *Da Guerra*. Tradução de CMG (RM1) Luiz Carlos N. S. do Valle, 845 p. Versão inglesa de: Michael Horward e Peter Paret. Original alemão. Disponível em: <http://pensamentosnomadas.files.wordpress.com/2012/11/da-guerra-carl-von-clausewitz.pdf >. Acesso em: 22 Jun. 2014.

COLLER, Kevin. The thin line between cyberattacks and real war. *The Daily Dot.* 22 May 2013. Disponível em: <http://www.dailydot.com/politics/cyber-attack-war-china-sea-law/>. Acesso em: 15 June 2014.

COSTA, Luiz Rosado. *A Aplicação dos Princípios de Direito Internacional Humanitário à Guerra Cibernética*, Trabalho de conclusão de curso (Especialização em Aplicações Complementares às Ciências Militares) – Escola de Formação Complementar do Exército, Salvador, 2011. Disponível em: <http://www.esfcex.ensino.eb.br/revista/producaocientifica/ arquivo/574_Artigo.pdf>. Acesso em: 12 Jun. 2014.

DICENSO, Davis J., *IW Cyberlaw*: The Legal Issues of Information Warfare, Airpower journal, Summer 1999, pp 85-94.

GHOSH, Shona. Is an International Cyberwar Imminent? *AlterNet*, 15 Apr. 2013 Disponível em: <http://www.alternet.org/media/international-cyberwar-imminent>. Acesso em: 23 Mar. 2014.

JACOBSON, Mark R. *War in the Information Age*: International Law, Self-Defense and the Problem of "Non-Armed" Attacks, The Journal of Strategies Studies, Vol 21, N.º 3, 1998, pp. 1-23.

JAYAKUMAR, Kirthi. Cyberwar and International humanitary law: What are the principles of conflict transformation. *Transconflict*. 21 mar. 2013. Disponível em: <http://www.transconflict.com/2013/03/cyber-war-and-international-humanitary-law-213/>. Acesso em: 23 Mar. 2014.

FRANÇA, Junia Lessa; VASCONCELLOS, Ana Cristina. *Manual para normalização de publicações técnico-científicas.*8. ed. Belo Horizonte: Ed. UFMG, 2007. 255 p.

LÉVY, Pierre. *A Inteligência coletiva:* por uma antropologia do ciberespaço. 5. ed. São Paulo: Loyola, 2007. 212 p.

MCMILLAN, Robert. Was Stuxnet built to attack Iran's nuclear program?, *Infoworld*, 21 Sept. 2010. Disponível em: <http://www.infoworld.com/d/security-central/was-stuxnet-built-attack-irans-nuclear-program-110>. Acesso em: 26 May 2014.

MELLO, Celso D de Albuquerque. *Curso de Direito Internacional Público*. 15 ed. Rio de Janeiro: Renovar, 2004. 2v.

MUIR JR, Lawerence J. The Case Against an International Cyber Warfare Convention, *The Wake Forest Law Review*, 9 Dec. 2011. Disponível em: <http://www.wakeforestlawreview.com/the-case-against-an-internacional-cyber-warfare-convention>. Acesso em: 23 Mar. 2014.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Charter of The United Nations, 1945. Disponível em: <http://www.un.org/en/documents/charter/>. Acesso em: 22 Apr. 2014.

_____. Genral Assembly Resolution n.º 3314 (XXIX), 14 Dec. 1974. Disponível em: <http://un.org/ga/search/view_doc.asp?symbol=A/RES/3314(XXIX)>. Acesso em: 22 Apr. 2014.

_____. Vienne Convention on the law of treaties, 23 mai. 1969. Disponível em: <https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf>. Acesso em: 01 Jun. 2014.

PMITTAL. How Digital Detectives Deciphered Stuxnet, The Most Menacing Malware im History. *Wired* 07 Nov. 2011. Disponível em: <http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/>. Acesso em: 21 May 2014.

SANDRONI, Gabriela Araújo. Prevenção da Guerra Espaço Cibernético, Jus Navigandi, Teresina, ano 19, n.º 3975, 20 Mai 2014. Disponível em: <http://jus.com.br/artigos/28660> Acesso em: 12/06/2014.

SCHMITT, Michael N. (Coord.). *Tallinn Manual on the internacional law applicable to cyber warfare.* Cambridge: Cambridge University Press, 2013. 215 p. Disponível em: <http://www.collaboratory.de/images/4/4b/Tallinn-Manual-on-the-International-Law-

Applicable-to-Cyber-Warfare-Draft-.pdf>. Acesso em: 20 Mar. 2014.

SHEKARAUBI, Shahrooz. Iran´s Case against Stuxnet. *International Policy Digest*. 18 Mar. 2014. Disponível em: <http://www.internacionalpolicydigest.org/2014/03/18/irans-case-stuxnet/>. Acsseo em: 05 Apr. 2014.

SWASON, Lesley. The Era of Cyber Warfare: Applying International Humanitary law to the 2008 Russian-Georgian Cyber Conflict, Loy. L.A. Int't & Comp. L., vol. 32. Rev. 303 (2010). Disponível em: <http://digitalcommons.lmu.edu/ilr/vol32/iss2/5>. Acesso em: 20 Mar. 2014.

UNITED STATES OF AMERICA. Departament of Defense. *DOD Dictionary of Military Terms*. Disponível em: <http://www.dtic.mil/doctrine/dod_dictionary/>. Acesso em: 10 June 2014.

WAXMAN, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), *Yale Journal of Internacional Law,* v. 36, issue 2, pp 421-459. 2011. Disponível em: <http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf>. Acesso em: 22 Mar. 2014.