ESCOLA DE GUERRA NAVAL

CC MARCELO DE SOUZA BARBOSA

A EXTRATERRITORIALIDADE NO AMBIENTE DA GUERRA CIBERNÉTICA À LUZ DO DIREITO INTERNACIONAL PÚBLICO.

RIO DE JANEIRO

2017

CC MARCELO DE SOUZA BARBOSA

A EXTRATERRITORIALIDADE NO AMBIENTE DA GUERRA CIBERNÉTICA À LUZ DO DIREITO INTERNACIONAL PÚBLICO.

Dissertação apresentada à banca examinadora da Escola de Guerra Naval, como requisito parcial para conclusão do Curso de Estado-Maior para Oficiais Superiores, sob a orientação do Capitão de Fragata Eugenio Campos Huguenin .

RIO DE JANEIRO
ESCOLA DE GUERRA NAVAL
2017

RESUMO

BARBOSA, Marcelo de S. A extraterritorialidade no ambiente da guerra cibernética à luz do Direito Internacional Público. 2017. 54 f. Dissertação (Curso de Estado-Maior para Oficiais Superiores) – Escola de Guerra Naval, Rio de Janeiro, 2017.

O desfio deste trabalho é analisar a extraterritorialidade no ambiente da guerra cibernética à luz do Direito Internacional Público. Para tal, faz-se mister entender, primeiramente, a problemática do que venha ser a guerra cibernética ou ciberguerra, considerando-a como um novo domínio da guerra, além dos tradicionais; seus princípios ou características peculiares, principalmente, aliado ao seu ambiente que é o ciberespaço que não tem barreiras físicas sem olvidar que a guerra cibernética não somente ocorre no campo virtual e interconectado, mas como também em redes locais estanques ou computadores fora da rede mundial de computadores. Dentro do rumo traçado, discorre-se a regulamentação da guerra cibernética no Direito Internacional Público tratando das iniciativas da comunidade internacional sobre o tema, destacando a mais contundente que é o Manual de Tallinn, e investigando o ordenamento em vigor a fim de verificar a adequação dos atuais paradigmas do *jus in bello* e do *jus ad bellum* para disciplinar os conflitos no espaço cibernético. Foi possível constatar que é possível a aplicação das atuais regras da Carta da Organização das Nações Unidas com critérios técnicos para determinar a autoria e a origem de um ataque, bem como os princípios, usos e costumes do Direito Internacional servem para disciplinar a guerra cibernética. Além disso, o Direito Internacional encara o desafio de aplicar uma resposta coordenada a nível internacional para se adaptar a esse novo domínio, fortalecendo a soberania em detrimento da característica transnacional da ciberguerra, nascendo como tendência a cooperação. Por fim, trata-se da relação de soberania e ciberespaço, perscrutou-se uma possível relativização da mesma devido às características desse novo ambiente da guerra. Ademais, buscou-se abrilhantar o estudo com o caso s*tuxnet*, ocorrido no Irã, e w*annacry* a fim de demonstrar a importância do tema para a sociedade de forma geral.

Palavras-chave: Direito Internacional Público. Guerra Cibernética. Manual de Tallinn. Extraterritorialidade. Soberania.

SUMÁRIO

1 INTRODUÇÃO

O estudo do espaço cibernético e o que nele ocorre revela-se um desafio, seja pela importância do tema para a sociedade humana ou por ser um assunto embrionário no âmbito do Direito Internacional Público (DIP). Uma questão importante nesse estudo reside no "local" em que ocorre o fluxo de dados, talvez pelo fato da sociedade não ter enfrentado anteriormente os desafios advindos da informação e internet.

É inquestionável que o mundo, com modernas tecnologias computacionais e de comunicações, vem sofrendo transformações significativas que estão influenciando a vida da sociedade, tendo a internet[1] um papel fundamental. Com seu surgimento, a sociedade firmou um sistema global, tendo essa como ambiente de interação, permitindo o acesso e troca de informações. É mister ressaltar que a internet é a revolução tecnológica mais poderosa da história da humanidade.

Com as tecnologias disponíveis e o incremento da interligação da rede mundial de computadores e dos sistemas de informação, consequentemente, crescem as vulnerabilidades, podendo, inclusive, comprometer informações de relevância para uma organização, indivíduo ou Estado, que estão cada vez mais conectados e dependentes de programas hospedados em redes de computadores. Assim, além dos quatro domínios já conhecidos (terra, mar, ar e espaço), surge mais um, o espaço cibernético[2].

Chega-se a um ponto crucial: o espaço cibernético ou ciberespaço, que tem levado a mudanças não somente nos domínios, mas no modo de condução da atividade cibernética, seus limites e os conflitos oriundos dele, os quais estão crescendo nos últimos anos em um ritmo acelerado.

---

[1] "A rede mundial das redes destinada a acesso geral para a transmissão de e-mails, compartilhamento de informações em páginas da web e assim por diante." (KNAKE, 2015, p.226)

[2] Inclui a internet, além de várias outras redes, incluindo as transnacionais como as bancárias. (KNAKE, 2015, p. 60-61)

Esse assunto tornou-se tão relevante que os Estados e Organizações Internacionais, preocupados com o que deve ser feito para resolver esse problema, o qual demanda soluções inseridas dentro do contexto da guerra, promoveram iniciativas de forma a tentar firmar um entendimento sobre a guerra cibernética no contexto do DIP, destacando-se o Manual de Tallinn sob a égide da Organização do Tratado do Atlântico Norte (OTAN) que não se constitui em uma fonte formal do direito.

Nesse mundo virtual interligado, estão inseridos os conceitos de espaço cibernético (ECiber), ataques cibernéticos (AC) e guerra cibernética (GC). Ainda neste mundo virtual, o ECiber caracteriza-se por ser um ambiente dinâmico, com alcance global e sem fronteiras delimitadas, estando presente em todas as redes de computadores do mundo e em cada coisa conectada a mesma. Assim sendo, favorece-se a prática de atos ilícitos como invasões à rede ou roubo de informações, que são denominados os ataques cibernéticos, que podem evoluir para um estado de guerra[3], constituindo-se uma guerra cibernética.

José Augusto Sacadura Garcia Marques[4] ensina sobre o caráter transnacional da internet que invoca uma cooperação entre Estados de forma a acordar princípios mínimos; e como o ciberespaço inclui a internet, podemos, inicialmente, estender ao novo domínio: o ECiber. Assim percebe-se que há desafios a serem vencidos pela comunidade internacional.

Miguel-Angel Davara Rodríguez[5] coloca em dúvida a questão da soberania dos Estados em função do desenvolvimento tecnológico, partindo da premissa do desvio de finalidade das normas e tendo como possível solução um regresso à ética clássica e aos princípios gerais do Direito para a concepção de um senso comum.

---

[3] "A existência de um "estado de guerra", entre atores internacionais, não está mais vinculada à lógica centralizadora da guerra somente entre Estados, há o aumento de possibilidades de novos atores promoverem a guerra, mesmos os não identificados como sujeitos do Direito Internacional." (RENATA DE BARROS, 2015, p.92)

[4] Telecomunicações e proteção de dados. *In*: As telecomunicações e o direito na sociedade da informação, p.85.

[5] *La liberalización del mercado de las telecomunicaciones: una perspectiva desde la ética*. *In:* As telecomunicações e o direito na sociedade da informação, p.179.

À consideração do supra exposto, o fundamento deste trabalho consiste na análise da extraterritorialidade da guerra cibernética à luz do DIP em função deste novo ambiente de guerra (virtual) onde não há fronteiras físicas, nem a definição clara de atores e combatentes. Para tal, é necessária uma análise de tratados e convenções internacionais, doutrina, artigos científicos e fonte bibliográfica sobre o assunto, a fim de entender como o DIP está se relacionando com: a questão da extraterritorialidade na GC e a soberania dos Estados; e as iniciativas da comunidade internacional sobre a questão supra e possíveis consequências. Assim, busca-se verificar se há relativização da soberania dos Estados frente ao caráter transnacional da guerra cibernética.

Para perscrutar o alicerce teórico, será utilizada como metodologia a pesquisa documental e bibliográfica. Desse modo, através da leitura de tratados e convenções internacionais, doutrina, artigos científicos e fonte bibliográfica sobre o assunto, espera-se obter o resultado pretendido, aspirando uma produção instigadora de uma postura mais participativa dos Estados.

1.1 DELIMITAÇÃO DO TEMA

O tema sobre a guerra cibernética e o DIP no ordenamento jurídico internacional é amplo e empolgante, visto que é um assunto vital para a comunidade internacional. Destarte, há que se entender todo o contexto e como a transnacionalidade da guerra cibernética veio tomando forma com a globalização e a rede mundial de computadores.

Nesse trabalho, a ideia foi a escolha da extraterritorialidade da guerra cibernética à luz do DIP a fim de não correr o risco de dispersão do tema central, ressaltando que, neste

trabalho, está sendo usado o significado da extraterritorialidade[6] no sentido estrito da palavra e não se tratando do princípio da extraterritorialidade[7] alusivo ao Direito Penal.

Em função de diversos estudos e iniciativas existentes sobre o tema na comunidade internacional, a guerra cibernética mostra-se um tema rico, de forma que o estudo de Tallinn será abordado em função de sua relevância, porém evitando as polêmicas doutrinárias, por não ser o escopo do estudo.

A extraterritorialidade nos leva diretamente a questão da soberania dos Estados, que se limita ao seu território, inicialmente. Entretanto, pode ser que o caráter transnacional do ECiber relativize a soberania dos Estados na guerra cibernética, dentro do Direito Internacional Público, merecendo assim sua investigação.

1.2 CONTEÚDO

No segundo capítulo, aborda-se, primeiramente, as definições da guerra cibernética que se mostra completamente diferente da guerra cinética, verificando o que é, como é travada e em qual domínio. Este, que já pode ser chamado como um novo domínio – espaço cibernético, totalmente diferente dos tradicionais, tem suas peculiaridades em função da realidade virtual que subsiste em uma série de redes e computadores, o anonimato dos respectivos atores e sem limites físicos definidos.

Ademais, ainda são exploradas suas características como rastreabilidade, seus efeitos no mundo real e a possibilidade de uso tanto para ataque como defesa. Para conter essa

---

[6] Segundo o Dicionário Aurélio Eletrônico – século XXI, extraterritorialidade é a qualidade de extraterritorial, ou seja situado fora do território.

[7] Fernando Capez ensina que o princípio da extraterritorialidade consiste na aplicação da lei brasileira aos crimes cometidos fora do Brasil e que o direito internacional concede ampla liberdade aos Estados para julgar, dentro dos seus limites territoriais, qualquer.crime, não importando onde tenha sido cometido, sempre que julgar contrário à ordem pública.

ameaça, as normas terão que se adequar ao ambiente virtual e transnacionalidade, pois um crime ou ataque nunca deixarão de ser considerados crimes ou atitude hostil e deliberada.

Outro ponto que também será abordado são os conflitos no espaço cibernético, que tem formas distintas de combate com relação ao modo tradicional, armas de tecnologias complexas e inovadoras, além de uma pluralidade de atores da comunidade internacional. Ademais, será evidenciada a íntima relação do Estado, como agente desenvolvedor, com os conflitos, visto que se observa uma relação muito próxima entre o ente estatal e a guerra cibernética.

No capítulo 3, segue-se com a regulamentação da guerra cibernética no DIP, abordando seus princípios e costumes, logo tendo por conteúdo a Carta da Organização das Nações Unidas, que foi escrita antes do fenômeno da internet. Assim, a ciberguerra torna-se um desafio, especialmente no que tange ao uso da força com suas definições clássicas e o teatro de operações, que foge do campo físico e evolui para o virtual. Acompanhando essa evolução, cita-se o Manual de Tallinn que é uma tentativa de evoluir na questão, porém sem ter caráter normativo e nem representar a opinião da organização que a solicitou. Ademais, buscou-se abrilhantar nosso estudo com os desafios no âmbito do DIP em função da evolução da internet adquirindo contornos significativos.

No capítulo 4, chega-se a relação entre os Estados e a guerra cibernética, investigando como se comporta a soberania dos Estados, ou seja, nesse novo domínio, como ainda está sendo vista a soberania, se absoluta ou relativa, de forma que o Estado possa combater essa atividade; e para ilustrar traz-se a baila o caso s*tuxnet*, ocorrido no Irã, e *wannacry* em escala mundial.

2 GUERRA CIBERNÉTICA

Mas o que é a guerra cibernética? Segundo Clausewitz (1996), a guerra significa uma violência contra o opositor a fim de que o mesmo se submeta a vontade do atacante.

Já para chegar ao vocábulo *cybernetics*, após a Segunda Guerra Mundial, um grupo de 21 cientistas reuniu-se em Nova Iorque para discutir o que seria *feedback* e os sistemas que tinham intenção, entre eles, Norbert Wiener, o qual percebeu a existência de um campo científico perquirido nas relações da informação, ao comandar as máquinas com a conexão do sistema nervoso do homem e o envio de mensagens por meio dos aparelhos. Assim, segundo Norbert Wiener[8], o vocábulo *cybernetics* é materializado pelo conjunto da Teoria do Controle e da Teoria da Comunicação em uma máquina ou animal, elevando o grau de importância da informação e tornando possível a criação de um ambiente em que os computadores, sistemas de comunicação e transmissões eletrônicas pudessem ser desenvolvidos.

Assim, embrionariamente, a guerra cibernética é uma violência contra o opositor utilizando o ambiente dos computadores, sistemas de comunicação e transmissões eletrônicas.

Hoje, a ciberguerra é o mais novo domínio da guerra e é travado no campo de batalha virtual, que é denominado espaço cibernético.

Entendendo a guerra cibernética, enceta-se, primeiramente, o conceito asseverado pelo Departamento de Defesa dos Estados Unidos da América (DoD) que é uma teoria emergente da guerra na era da informação, em que há a identificação de novas fontes de poder e sua relação entre si e com os resultados e objetivos políticos.[9]

David Stephen, em uma publicação do programa de pesquisa cooperativa do Departamento de Defesa dos Estados Unidos da América, esclarece que a *Network-centric*

---

[8] WIENER, Norbert. *Cybernetics or the control and communication in the animal and the machine*, 1948.
[9] Estados Unidos da América. Departamento de Defesa. *Office of Force Transformation*. Washington:2005.

warfare como é o comportamento humano e organizacional, baseado em um novo jeito de pensar aplicado às operações militares, não se confundindo e afastando do conceito de guerra cibernética.[10]

Já o Dr. Martin R. Stytz (2006, p. 95-96) nos ensina:

> *Cyberwarfare is the broadly defined term used to describe any type of hostile activity taken against computer systems, computer networks, and computerised databases with the objective of degrading or disabling the targeted system(s). Cyberwarfare attacks make these systems unusable, degrade performance, may lead commanders to make poor decisions due to faulty data, may yield valuable secrets, and may leave behind code that could provide continuing back-door access to a system or be activated on a predetermined event to take obstructive action*.[11]

O Glossário das Forças Armadas Brasileiras define guerra cibernética como conjunto de ações para uso de informações e seus sistemas para perturbar o adversário, com fulcro em informações, sistemas de informação e redes de computadores a fim de obter vantagens em qualquer campo.[12]

Em que pesem as definições acima, percebe-se que não existe consenso sobre a definição em lide, mas uma aproximação nas posições de autores estadunidenses. Ademais, o próprio Departamento de Defesa dos Estados Unidos da América não tem uma definição precisa sobre ciberguerra.

Nesse capítulo insta direcionar o que é a guerra cibernética, contudo, primeiramente, é de bom alvitre discorrer seus princípios em termos gerais, o ambiente em que opera e seus conflitos.

---

[10]ALBERTS, David S. *Network centric warfare: developing and leveraging information superiority. CCRP publication series*. 1999.

[11] Guerra Cibernética é o termo amplamente definido usado para descrever qualquer tipo de atividade hostil tomada contra sistemas de computador, redes de computadores e bancos de dados computadorizados com o objetivo de degradar ou desativar o (s) sistema (s) alvo. Os ataques de guerra cibernética tornam esses sistemas inutilizáveis, degradam o desempenho, podem levar os comandantes a tomar más decisões devido a dados defeituosos, podem gerar segredos valiosos e podem deixar código que poderia fornecer acesso contínuo à porta traseira para um sistema ou ser ativado em um evento predeterminado para tomar medidas obstrutivas. (tradução nossa)

[12] BRASIL. Ministério da Defesa. MD35-G-01: glossário das Forças Armadas. 2007.

2.1 PRINCÍPIOS DA GUERRA CIBERNÉTICA

Quando se fala em princípios da guerra, primeiramente, remete-se aos grandes pensadores da guerra como Clausewitz e Sun Tzu. Este considerava cinco fatores fundamentais: influência moral, clima, terreno, comando e doutrina. Já Clausewitz propôs nove: objetivo, ofensiva, massa, economia de forças, manobra, unidade de comando, segurança, surpresa e simplicidade.

Trazendo para o escopo deste estudo, Parks e Duggan (2011) consideram oito princípios sobre a ciberguerra, quais sejam:

a) Princípio da falta de limitação física visto que a distância física não é um obstáculo nem um facilitador para conduzir ataques, que podem ser conduzidos em qualquer lugar do planeta, bastando ter tecnologia;

b) Princípio do efeito cinético que deve ter efeitos cinético-mundiais. Isto é, tem que afetar objetos no mundo físico;

c) Princípio da discrição que se assemelha à camuflagem no mundo real. Os atores da guerra cibernética buscam ocultar evidências nos fluxos de dados existentes;

d) Princípio da mutabilidade e inconsistência que coloca a inexistência de leis imutáveis no mundo cibernético, com exceção daquelas que exigem uma ação no mundo físico. O ciberespaço é inconsistente e não confiável;

e) Princípio da identidade e privilégios que assegura a uma entidade a autoridade de executar qualquer ação que um atacante deseja executar. O objetivo do atacante é assumir a identidade dessa entidade, de alguma forma. Todas as partes do ciberespaço são controladas, seja por uma pessoa ou entidade;

f) Princípio da dualidade que fala sobre as ferramentas de Ciberguerra que são sempre de dupla utilização, ou seja, os atacantes usam scanners de vulnerabilidade para

procurar oportunidades de exploração como parte de um ataque, ao mesmo tempo, os defensores usam os mesmos scanners de vulnerabilidade para detectar pontos fracos em seus próprios sistemas;

g) Princípio da infraestrutura de controle que trata do ciberespaço onde tanto defensores quanto os atacantes controlam um parte. Quem controla um parte do ciberespaço que o oponente usa pode controlar o adversário; e

h) Princípio da informação como ambiente operacional em que cada parte do ambiente operacional da guerra é informação. Cada dado captado é transformado em informação.

Isto posto, pode-se inferir que a guerra cibernética, travada no ciberespaço, tem algumas características como o anonimato, ocultação, surpresa, inexistência de limites físicos separando os atores e com fulcro em operações assimétricas.

Por fim, a ciberguerra pode ter vários fatos geradores e se materializar por diversos tipos de ações, sejam ofensivas, defensivas e exploratórias, no intuito de apoiar as ações realizadas no mundo exterior, sendo para tal necessário entender onde ela ocorre.

2.2 O ESPAÇO CIBERNÉTICO

Richard Clarke (2015) assegura que o espaço cibernético faz-se presente em todas as redes de computadores e a tudo conectado a ela. Ademais, ainda nos ensina a diferença entre a internet e o ciberespaço. A internet, segundo Sidney Guerra (2006), caracteriza-se por conjunto de tecnologias para acesso, distribuição e disseminação de informação ou dados em uma rede de computadores em escala global. Havendo internet, qualquer dispositivo pode se comunicar com outro conectado a umas das redes da internet. Já o ciberespaço inclui a internet e outras redes de computadores não acessíveis a mesma, ou

seja, segregadas. Não há que se olvidar ainda das redes transnacionais que fazem o fluxo de dados e as de sistema de controle, muito usual nas indústrias.

Investigando a conceituação, verifica-se que a Organização das Nações Unidas (ONU)[13] define o espaço cibernético[14] como sendo uma rede globalmente interconectada de informação digital e infraestrutura de comunicações, incluindo a internet, redes de telecomunicações e sistemas informáticos. O Ministério da Defesa do Brasil[15] define-o como espaço virtual, interconectado ou não, onde trafegam e são processadas as informações digitais.

Do conceito supra, depreende-se que as informações trafegam por uma infinidade de conexões conectadas por fibras óticas ou via satélite, formando-se assim uma extensa e complexa malha de comunicação mundial. Logo, o espaço abarca desde o operador do sistema, passando pelo equipamento e os dados que fluem por ele, até o sistema de informação.

Devido ao alto fluxo de informações, a preocupação com a circulação de informações foi denominada de “fluxo de dados transfronteiras” e foi alvo de preocupação do Conselho da Europa na década de 80, que editou uma convenção para proteger as informações pessoais.

Com tantas particularidades, o espaço cibernético configura-se como um espaço altamente atrativo para atividades ilícitas, sendo fonte potencial de conflitos nesse novo domínio, como será visto a seguir.

---

[13] MELZER, Nils. *United Nations. UNIDIR resources. Cyberwarfare and international Law.* Disponível em: <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.> Acesso em: 18 de março de 2017.

[14] Para outras definições veja: NATO *Cooperative Cyber Defense, Centre of excellence* Tallinn, Estonia. Disponível em: < https://ccdcoe.org/cyber-definitions.html> Acesso em: 12 de março de 2017.

[15] BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. Minuta de Nota de Coordenação Doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa. Brasília, 2010, p.9.

2.3 OS CONFLITOS NO ESPAÇO CIBERNÉTICO

Nesse tópico será investigada a relevância dos ataques que podem originar os conflitos no ciberespaço, que se configuram como ameaças.

No espaço cibernético não há uma clara definição das ações, lideradas por atores estatais ou não, que podem estar atreladas a espionagem, crimes, terrorismo cibernético e até ser o estopim de uma guerra. Para todos os casos há uma semelhança, que é a utilização de armas ou ferramentas cibernéticas para realizar ataques que podem desestabilizar setores relevantes da sociedade ou até mesmo de um Estado, comprometendo a segurança. A alta relevância do assunto é demonstrada por diversos relatórios e pesquisas realizados por empresas do ramo, com finalidades, critérios e abrangências variáveis.

O relatório *Cyber-security: The vexed question for global rules*, elaborado pela *Security and Defence Agenda*, a pedido da *McAfee*[16], atentou para entrevistas com oitenta especialistas em segurança digital e pesquisas com outros 250 de 35 países. Dessa pesquisa ressalta-se que 60% revelaram a percepção de que, hoje, existe uma corrida armamentista cibernética em curso.

Em outra pesquisa realizada pelo *Center For Strategic and International Studies*[17], foram ouvidos 600 executivos da área de segurança de empresas de infraestruturas críticas de 14 países, onde se constatou que mais de 50% das empresas já sofreram ataques de grande escala ou invasões de governos, grupos criminosos ou terroristas.

No campo estatal internacional, destaca-se a criação, em 2009, do *United States Cyber Command* (USCYBERCOM). Ressalta-se a importância dada ao assunto pelos Estados Unidos da América, visto que o USCYBERCOM está diretamente subordinado ao

---

[16] Relatório disponível em: <http://www.securitydefenceagenda.org/Portals/14/Documents/ Publications/SDA_ Cyber_report_FINAL.pdf>. Acesso em 24 fev. 2017.

[17] Relatório disponível em: <http://img.en25.com/Web/McAfee/CIP_report_final_pt-br_fnl_lores.pdf>.Acesso em 24 fev. 2017.

United States Strategic Command (USSTRATCOM) junto com outros cinco comandos estratégicos (*Joint Warfare Analysis Center, Joint Functional Component Command for Global Strike, Joint Functional Component Command for Space, Joint Functional Component Command for Integrated Missile Defense e Joint Functional Component Command for Intelligence, Surveillance and Reconnaissance*); e, em 2011, foi anunciada a Estratégia Internacional para o Espaço Cibernético, na qual é proposta a criação de normas internacionais de segurança que considere um ataque cibernético com danos e transtornos de grandes proporções, oriundo de outro país, como ato de guerra, logo podendo motivar resposta com força militar convencional.[18]

A OTAN considera que, na próxima década, os conflitos cibernéticos estão entre as mais prováveis ameaças não convencionais e divulgou o entendimento de que um ataque contra uma infraestrutura crítica de um país membro pode gerar uma resposta militar.[19]

Ressalta-se que o ataque é caracterizado por uma tentativa de acesso ou uso não autorizado que resulte no acesso, manipulação ou destruição de informações em um computador.

Consolidado o conceito de ataque e situado acerca da importância da matéria frente à comunidade internacional, esses ataques configuram-se como o fato gerador de conflitos, que são denominados como ameaças e são divididas em três grandes blocos conforme Paulo Zuccaro (2011, p.61) atesta:

> Guerra Cibernética – é focada em conflito interestatal. Independente de métodos e executantes, o que estará por trás das ações, de forma velada, ou não, será a agressão de um Estado a outro na busca da redução de poder nacional, que pode estar associada a outros métodos de ataque, inclusive físicos. Bom exemplo pode ser a ação desencadeada a partir do território russo contra a Geórgia, embora nunca tenha havido uma efetiva admissão por parte do governo russo da autoria dos ataques.
> Terrorismo cibernético – neste caso, os interesses a serem alcançados têm motivação política, como, naturalmente, também é o caso da guerra cibernética. A diferença fica por conta do fato de que seus autores, normalmente, serão grupos não estatais.

[18] Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em: 25 mar. 2017.
[19] Disponível em: <http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/PT/index.htm> e em: <http://www.nato.int/cps/en/natolive /index.htm>. Acesso em 26 mar. 2017.

> As agressões, em geral, serão dirigidas aos Estados cuja ação ou postura política seja contrária aos interesses ou à visão de mundo daqueles grupos. Também podem ser atacadas instituições ou empresas que possuam ponderável carga simbólica em relação ao Estado ou grupo de Estados a ser agredido, como, por exemplo, uma grande multinacional de uma potência econômica ocidental.
> Crime cibernético – quanto a este último bloco, geralmente as motivações serão de indivíduos ou de pequenos grupos, com fins privados e egoísticos. Na maioria dos casos, são ilícitos com objetivo de ganhos econômicos, como, por exemplo, o roubo de senhas bancárias, fraudes com cartões de créditos e outros afins.

O mesmo autor ainda cita uma quarta ameaça que é o ativismo cibernético, mas como de menor potencial.

As ferramentas dos ataques cibernéticos são bastante diversificadas, podendo utilizar desde técnicas mais rudimentares e de domínio público amplamente divulgadas na própria internet, técnicas inovadoras e complexas até métodos de espionagem ou de inteligência cibernética. Dessas ferramentas e técnicas de ataque, algumas sobressaem em razão da gravidade da sua repercussão, podendo configurar uma ameaça à segurança nacional, que podem envolver redes estatais, das infraestruturas críticas até as privadas.

É mister salientar que não é o escopo desse trabalho aprofundar tecnicamente a descrição e as técnicas de ataque cibernético, valendo registrar que, diariamente, novas técnicas são desenvolvidas.

Regressando aos conflitos, alguns se diferenciam dos corriqueiros ataques por envolverem atores estatais de diferentes países como possíveis protagonistas ou apenas como alvos de ataques, contudo as empresas privadas não escapam desse campo de batalha. Não obstante a presença estatal, nenhum país admitiu oficialmente qualquer tipo de ataque cibernético, assim como não há provas que permitam inferir sua autoria a qualquer Estado.

Pode-se citar, a termo exemplificativo, o vírus *stuxnet*[20] que foi infiltrado nos sistemas do reator nuclear de Bushehr (Irã) com o fito de inutilizar centrífugas. O episódio retardou o projeto nuclear iraniano e por isso é amplamente noticiado como espécie de ataque

[20] Disponível em: <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?page wanted=all>. Acesso em: 12 mar. 2017.

de guerra cibernética. A empresa de segurança da computação *Kaspersky Labs* afirmou que o s*tuxnet* pode ter sido o primeiro de um conjunto de armas cibernéticas.[21]

Apesar do exemplo supra, não há que se petrificar que os alvos são só os sistemas governamentais, visto que as redes controladoras de serviços considerados essenciais também estão passíveis de ataque e sua indisponibilidade pode causar algum tipo de colapso tais como hidrelétricas, usinas nucleares, redes hospitalares, instituições financeiras entre outros, como o ciberataque de escala mundial[22] – 74 países atingidos – efetivado, em 12 de maio de 2017, por um *malware*[23] chamado w*annacry*, que indisponibiliza os arquivos ao criptografá-los, pedindo pecúnia como condição para a devolução, atacando uma vulnerabilidade do sistema operacional *Windows* da Microsoft. O *malware* foi roubado da *National Security Agency* (NSA) do governo norte-americano, aproveitando uma vulnerabilidade.[24]

Com efeito, apesar das três ameaças citadas anteriormente, há que se focar na guerra cibernética, que está relacionada aos conflitos que envolvem diferentes Estados, situação distinta das outras duas ameaças que em *lato sensu* são praticados por indivíduos ou organizações que atuam por diversos motivos contra Estados ou redes, sistemas, estruturas, instalações tanto privadas como estatais.

Nesse âmago da guerra cibernética, percebe-se que os países estão se mobilizando para desenvolver novas estratégias de segurança em função dos diversos ataques noticiados e o potencial das ameaças para colocar a segurança dos países em risco. Uma

---

[21] Disponível em: <http://blogs.estadao.com.br/link/tag/stuxnet/> Acesso em: 12 mar. 2017.
[22]Disponível em: <http:// http://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml>. Acesso em: 12 mai. 2017.
[23] O termo *malware* é uma contração de *malicious software*, ou seja, é qualquer parte de software que tenha sido escrita para causar danos. Disponível em:< http://www.avg.com/pt/signal/what-is-malware>. Acesso em: 12 mai. 2017.
[24] Disponível em: <http://www.npr.org/sections/thetwo-way/2017/05/15/528439968/wannacry-ransomware-microsoft-calls-out-nsa-for-stockpiling-vulnerabilities> e <https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#50eca66de599>. Acesso em: 29 mai. 2017.

dessas mobilizações encontra-se no campo intelectual, visto que vários Estados e Organizações Internacionais, destacando a própria ONU e a OTAN, já se dedicam a estudar a guerra cibernética, entretanto ainda não existem definições ou doutrina consolidadas, muito menos normas jurídicas.

Assim sendo, é meritório registrar que há estudos sobre o assunto, sendo um dos mais conhecidos o Manual de Tallinn que será estudado posteriormente, e que existe a necessidade da comunidade internacional definir regras a respeito da guerra cibernética ou tomar essas iniciativas retrocitadas sobre o tema em lide para uniformizar condutas ou até mesmo expandir a interpretação das normas para abarcar esse novo domínio da guerra.

Logo, faz-se necessário que se perscrute a regulamentação da ciberguerra no Direito Internacional Público, o que será feito a seguir.

3 A REGULAMENTAÇÃO DA GUERRA CIBERNÉTICA NO DIREITO INTERNACIONAL PÚBLICO

Desde os primórdios da humanidade, o homem já apresentava características fundamentais e qualidades comuns para a evolução dos agrupamentos humanos que evoluíram até a formação da sociedade, com todas as implicações que esta lhe impõe. Uma destas é a criação de determinadas normas de conduta a fim de reger a vida em grupo.

A sociedade evoluiu, por conseguinte, o Direito também evoluiu e passou a não mais estar restrito às fronteiras territoriais, ou seja, aos limites do Estado Soberano, que, à semelhança das comunidades de indivíduos, também apresentam diferentes características, e crescentes relações internacionais. Essa evolução acaba por transcender as fronteiras dos Estados rumo à instituição de um sistema de normas jurídicas internacionais no intuito de conciliar conjuntamente os diversos interesses Estatais. A esse complexo sistema de normas dá-se o nome de Direito Internacional Público

Já acolhido o que é a guerra cibernética como um novo domínio, conforme exposto no capítulo retro, faz-se necessário assinalar que regulamentar é agir conforme a regra, que nesse caso é atuar de acordo com o sistema de normas internacionais, o qual será visto a seguir.

3.1 PRINCÍPIOS, USOS E COSTUMES NO DIREITO INTERNACIONAL PÚBLICO

Primeiramente, a Convenção de Haia de 1907 foi a primeira norma internacional a fundar um rol de fontes formais do DIP. Posteriormente (1945), edita-se o

Estatuto da Corte Internacional de Justiça[25], contendo um rol, não taxativo, das fontes do DIP, quais sejam:

a) os princípios gerais de direito;

b) as convenções internacionais que estabeleçam regras formalmente reconhecidas pelos Estados que litigam;

c) o costume internacional como prática corriqueira geral aceita; e

d) as decisões judiciárias e doutrinas dos juristas de elevado saber jurídico das diferentes nações como meio subsidiário.

Desse modo, os princípios gerais de direito, tratados e costumes são as fontes primárias do Direito Internacional, que não guardam hierarquia entre si, ou seja, não existe uma prioridade de um sobre o outro. Por outro lado, as decisões judiciárias e doutrinas constituem-se como meios de auxílio a decretar o direito que pode ser aplicado.

Estudando os princípios gerais de direito, nota-se que são formas legítimas de manifestação do Direito Internacional Público no que tange ao reconhecimento destes princípios pelos Estados signatários, sendo os mesmo amplamente utilizados em situações em que uma regra do DIP não está expressa nos tratados e não é configurada como prática costumeira. Logo, os princípios gerais de direito são os aceitos por todos os ordenamentos jurídicos.

Valério Mazzuoli (2008) explicita que o costume internacional é a fonte mais antiga do DIP e tem tido um papel que merece consideração na formação e progresso do Direito Internacional, seja por criar um corpo de regras aplicáveis de forma universal e por

---

[25] Art. 38 – A Corte, cuja função é decidir de acordo com o direito internacional as controvérsias que lhe forem submetidas, aplicará: a. as convenções internacionais, quer gerais, quer especiais, que estabeleçam regras expressamente reconhecidas pelos Estados litigantes; b. o costume internacional, como prova de uma prática geral aceita como sendo o direito; c. os princípios gerais de direito, reconhecidos pelas nações civilizadas; d. sob ressalva da disposição do Artigo 59, as decisões judiciárias e a doutrina dos juristas mais qualificados das diferentes nações, como meio auxiliar para a determinação das regras de direito.
A presente disposição não prejudicará a faculdade da Corte de decidir uma questão *ex aequo et bono*, se as partes com isto concordarem.

admitir a criação de regras gerais que são o alicerce de firmamento da sociedade internacional. Assim, nota-se que é um elemento essencial de assentamento das regras do DIP, valendo lembrar que nenhum tratado multilateral alcançou a ratificação de todos os Estados na sociedade internacional e assim os costumes permanecem como fonte-base. Destarte, pode-se dizer que o costume internacional é consequência de uma prática geral e reiterada dos atores internacionais que admitem como válidas e exigíveis de uma situação determinada.

Agora, na atualidade, os tratados internacionais são a principal fonte do DIP em função da segurança que trazem às relações internacionais por retratarem a livre, espontânea e articulada vontade dos Estados, trazendo consigo a força normativa de regular diversas matérias, dando maior segurança aos signatários.

Ressalta-se que os tratados, depois de trazidos para o ordenamento interno de cada Estado signatário, revogam as leis internas anteriores que lhes sejam oponíveis e, ainda, devem ser estritamente observados pelas leis editadas posteriormente, corroborando com as regras ou princípios estabelecidos pelos mesmos.

Salienta-se ainda a importância dos tratados visto que estes podem assentar normas de Direito Internacional, além de fonte, o que pode ocorrer quando os acordos internacionais têm aceitação dilatada ou abertura à adesão.

No que tange as decisões judiciárias e doutrinas dos juristas, estas figuram como meios auxiliares na determinação das regras de direito.

As decisões judiciárias são as da própria Corte Internacional de Justiça e só serão obrigatórias para as partes litigantes e a respeito do caso em lide com fulcro no art. 59 do Estatuto da própria Corte, não cabendo olvidar que essas decisões são conhecidas por jurisprudência são percebidas como decisões reiteradas, sobre o mesmo caso ou semelhante,

chegando ao mesmo desfecho. Assim, percebe-se que a jurisprudência interpreta o direito, não criando normas.

Insta destacar a importância da jurisprudência em função do número expressivo de normas que estão em vigor a título costumeiro, logo com a necessidade de interpretação para evitar ambiguidade, valendo o mesmo para os princípios gerais de direito.

Valério Mazzuoli (2008, p.118-119) ainda complementa que:

> As "decisões judiciárias" referidas pelo Estatuto da Corte Internacional de Justiça não são, de forma alguma, as proferidas pelos tribunais internos de determinado Estado. Por "decisões judiciárias" deve ser entendido a jurisprudência internacional, que é o conjunto de decisões dos tribunais internacionais sobre determinado assunto e no mesmo sentido, incluindo-se aí as sentenças proferidas pelos tribunais internacionais permanentes (decisões judiciárias), bem como as provenientes das cortes arbitrais internacionais desde longa data (muito antes, aliás, de começarem a aparecer os primeiros tribunais internacionais de caráter permanente).
> As decisões da Corte Internacional de Justiça, como meio de auxílio na determinação das regras de direito, são as que estão investidas da mais alta autoridade no plano internacional. [...] Também não fica descartada do conceito de decisão judiciária os pareceres emitidos pela Corte Internacional de Justiça proferidos dentro do quadro de sua competência consultiva[...].

Já as doutrinas dos juristas mais qualificados de diferentes nações, conforme o art. 38, funciona, modernamente, como coleção de doutrina acadêmica produzida por associações científicas, outros institutos especializados e organizações internacionais em prol do avanço do Direito Internacional.

Contudo, apesar de não constar no rol do art. 38, urge citar outras fontes consideradas pela doutrina como a analogia e equidade, atos unilaterais dos Estados, decisões das Organizações Internacionais, normas de *jus cogens* e *Soft Law*, não cabendo seu aprofundamento neste trabalho a fim de evitar o desvio do seu propósito.

A regulação da guerra cibernética e seu domínio é um desafio que o DIP deve enfrentar, sem qualquer empecilho quanto ao uso dos princípios vigentes, porém sem olvidar que possa ser necessário repensar ou ajustar a aplicação dessas em prol de uma regulação do ciberespaço, que se torna complexa haja vista a falta de precedentes históricos.

Por fim, há que se registrar que os Estados demonstram preocupação no assunto, v.g., quando elaboram suas doutrinas militares de segurança cibernética ou por

ocasião da edição de Leis, como feito pelo Brasil que ficou conhecida como o Marco Civil da Internet Brasileira[26]. Assim, resta demonstrado que, no que tange o ciberespaço, as principais fontes são as práticas adotadas pelos Estados, as iniciativas regionais ou estudos de organizações internacionais. Logo, vistas as fontes passa-se ao ordenamento internacional para investigar qual o regramento existente e se atende ou não à demanda internacional.

3.2 ORDENAMENTO INTERNACIONAL

Os atores presentes no ciberespaço participam de múltiplas relações de proporções globais e com característica de espaço global, portanto são regulados pelo Direito Internacional, que busca vencer o desafio de regular esse espaço sem utilizar a censura e monitoramento e assim adaptar ou trazer a baila uma nova interpretação do DIP para o ciberespaço aspirando ao benefício comum da humanidade.

Isto posto, dois pressupostos fundamentais para a regulação do espaço cibernético são vislumbrados: proteção dos recursos físicos de difusão da informação e a identificação dos usuários.

Sobre os recursos de difusão, esses podem ser de propriedade privada ou estatal. Não há que se falar em ciberespaço sem a infraestrutura física, custeada e com localização física determinada e sob a jurisdição de algum Estado soberano, que deve zelar pelo direito de propriedade, a respectiva proteção legal e policial. Portanto, há uma estrutura e ela está situada em um território, assim sendo, o Estado exerce positivamente sua autoridade soberana sobre ela, abarcando consequentemente o princípio da extraterritorialidade em termos de matéria penal, além dos princípios de regras do Direito Internacional.

---

[26] Lei n ° 12.965 de 23 de fevereiro de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

No que tange a identificação dos usuários, é fato que a localização dos atores não é virtual e possui uma localização geográfica, seja ele pessoa física ou jurídica, ocasionando submissão à soberania do Estado e assim sujeito as consequências jurídicas. Porém não é tão simples quanto parece dadas as tecnologias existentes e a possibilidade de efetuar ataques utilizando estruturas de terceiros, além da dificuldade em provar o mesmo. Nesse ambiente transnacional, faz-se necessário uma cooperação internacional legal, onde o DIP entra em cena.

Aplicando o Direito Internacional, percebe-se o enfoque multilateral da questão em função da interconectividade da informação e comunicação, além da infraestrutura global, exigindo assim abordagem transnacional e o respeito às soberanias estatais com o fito de combater a guerra cibernética, que cada vez mais preocupa em termos de segurança nacional devido à presença cada vez maior das forças armadas. As avançadas tecnologias são notadas como fator de força e elemento essencial do sucesso militar.

A guerra cibernética tem se mostrado tão inquietante que desde 1998 os Estados têm registrado dúvidas acerca do assunto em Assembleia Geral da ONU. No mesmo ano, os membros foram incitados a combater o crime e terrorismo no ciberespaço, apresentar princípios internacionais sobre o tema, pontos de vista sobre a segurança da informação internacional; e a Comissão de Segurança editou a Resolução “Desenvolvimentos no campo da informação e das telecomunicações no contexto da segurança internacional”.

No espaço temporal do ano de 2005 a 2010, as resoluções da Assembleia Geral da ONU optaram por um trabalho de conscientização sobre a multilateralidade e internacionalidade referente à guerra cibernética. Ademais, o Instituto das Nações Unidas para pesquisas sobre desarmamento (UNIDIR) realizou pesquisas sobre a segurança das informações no ciberespaço entre 1999 e 2008, além da OTAN, União Européia (UE) e a Organização de Cooperação de Xangai (OCX), entre outras.

Examinado o papel das organizações supra, inicia-se pela OCX que tomou ações preliminares para cooperação na área, adotando um conceito amplo de ciberataques, incluindo o uso da tecnologia para atacar a estabilidade política. A organização adota postura tímida, mas a China mostra-se mais incisiva em suas manifestações sobre o conceito de soberania na internet, sendo a internet regulamentada pelos Estados Membros, preservando ao máximo a soberania dos Estados e estendendo a jurisdição nacional a esse domínio. Ademais, o país vem promovendo várias iniciativas de Lei a partir da ONU, destacando-se um novo código de conduta para a indústria atuante no ciberespaço, para emplacar sua solução que é um direito cibernético interestatal.

Prosseguindo com a UE, esta tem defendido o investimento em segurança cibernética como forma de proteção e evitar ataques indesejados, trabalhando em várias frentes para prover a segurança e assinando tratados de cooperação internacional. A Convenção de Budapeste sobre o Cibercrime de 2001 foi o primeiro tratado internacional a versar sobre o assunto com o objetivo de criar uma política criminal comum visando a proteção contra os cibercrimes por meio da cooperação internacional; e em 2004 criou um órgão para gerir a segurança das informações dos entes privados europeus – Agência Europeia para a Segurança das Redes e da Informação. Vale ressaltar que os Estados Unidos ratificaram o tratado. Em 2014, o Parlamento Europeu aprovou a diretiva de alto nível de segurança das informações de rede na EU, mas ainda a ser aprovada pelo Conselho Europeu.

Já a OTAN vem envidando esforços para se defender e regular suas ações nesse novo domínio da guerra, iniciando pela proteção das informações e posteriormente criando o Órgão de Administração de Defesa Cibernética e o Centro de Ciberdefesa Cooperativa de Excelência. Em 2013, esse centro em parceria com a Universidade de Cambridge, publicou o Manual de Tallinn que foi a primeira tentativa de se verificar se as

atuais Leis da guerra seriam aplicáveis ao novo domínio da guerra, o que será visto posteriormente.

Como última organização, a ONU tem fomentado a formação de uma mentalidade de segurança cibernética, disseminando a necessidade de políticas globais a fim de não colidir com a dinâmica de manutenção da paz e estabilidade internacionais. As discussões sobre o assunto são divididas em duas vertentes: político-militar e econômica. Ademais há uma ação conjunta de diversos órgãos (Primeiro Comitê de Assembleia Geral da ONU, União Internacional de Telecomunicações- UIT, UNIDIR e Força-Tarefa de implementação do combate ao terrorismo- CTITF) para a problemática, que gerou o "Relatório sobre os desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional", um grande marco para a manutenção da estabilidade no ciberespaço reconhecendo a aplicabilidade do DIP no ciberespaço e a obediência dos mesmos princípios do Direito e medidas de segurança fixadas para os outros domínios.

Em se falando de ONU, há que se analisar a Carta da Organização das Nações Unidas e perscrutar as definições tradicionais com o fito de posicioná-las perante à guerra cibernética como "Lei Maior", com base no exposto retro.

3.2.1 Carta da Organização das Nações Unidas

A Carta de São Francisco criou a ONU com o intuito de manter a paz e segurança internacionais, centralizando o monopólio do uso legítimo da força quando necessário. Em seu art. 2º estabeleceu que todos os Estados membros deverão evitar a ameaça ou o uso da força contra a integridade territorial ou qualquer outra ação incompatível com os propósitos das Nações Unidas, cabendo ao Conselho de Segurança (CS), conforme o art. 39, decidir quais medidas coercitivas ou preventivas devem ser adotadas caso haja ruptura da paz

ou ato de agressão, decidindo quais medidas devem ser adotadas para o retorno ao *status quo* anterior, que podem ser desde a interrupção completa ou parcial das relações econômicas até a campanha militar propriamente dita. Já o art. 51 assegura o direito de legítima defesa[27], individual ou coletiva, a qual pressupõe identificação segura da autoria da ameaça ou do ataque sofrido, na ocorrência ou na iminência de ataque armado contra qualquer Estado Membro até que o CS adote medidas, observados os princípios da necessidade e da proporcionalidade. Vale ressaltar que o *US Cyber Command* considera justificável o ataque somente quando o dano causado é compatível com um ataque cinético, hipótese que justifica a legítima defesa conforme o art. supra.

Considerando que a Carta da ONU foi editada antes do advento da internet e trazendo esses critérios para o novo domínio da guerra, constata-se a complexidade do assunto em virtude das tradicionais definições de força[28], armas e ataque serem insuficientes para esclarecer o que se considera uma arma cibernética, quais ataques são toleráveis e como o uso da força opera nesta modalidade, bem como a medida da necessidade e da proporcionalidade da resposta.

Os ataques cibernéticos podem definitivamente causar danos físicos ou morte de seres humanos, assim como as perturbações de ordem econômica que ameaçam a paz. Sem tardança, há que se revisitar o paradigma do *jus ad bellum* a fim de incrementar a proteção dos Estados e, intrinsecamente ao tópico, faz-se necessário reinterpretar o uso da força no espaço cibernético para que seja enquadrado no art. 2° da Carta a fim de possibilitar que se invoque o direito à legítima defesa.

---

[27] KESAN, Jay P.; HAYES, Carol M. *Mitigative counterstriking: self-defense and deterrence in cyberspace.* (April 7, 2011). Illinois Public Law Research Paper No. 10-35; Illinois Program in Law, Behavior and Social Science Paper No. LBSS11-18; Harvard Journal of Law and Technology, Forthcoming. Disponível em: <http://ssrn.com/abstract=1805163>. Acesso em: 25 fev. 2017.

[28] SCHMITT, Michael N. *Computer network attack and the use of force in international law: thoughts on a normative framework.* Columbia Journal of Transnational Law. v. 37. 1998-99. Disponível em: <http://ssrn.com/abstract=1603800>. Acesso em: 25 fev. 2017.

Mas qual seria essa nova interpretação? Uma interpretação mais expansiva incluiria todas as ações de guerra cibernética dentro da definição de uso da força, todavia os atos de coerção seriam arrastados a contrabordo. Por outro lado, mostra-se imperioso definir quais tipos de ataques cibernéticos não causam danos físicos dentro do conceito de uso da força, e, principalmente, quanto aos ataques às infraestruturas críticas da economia, que foram excluídos da definição do uso da força na Carta em vigor, mas que podem ter efeitos devastadores.

Outro questionamento pertinente seria quem atacar, considerando que no espaço cibernético a identificação da origem de um ataque é difícil e a hostilidade do mesmo, levando em conta os ataques remotos e a diuturna invenção de técnicas inovadoras e a possibilidade de utilizar estruturas e atores inocentes. A legítima defesa requer que o autor seja identificado, por conseguinte não autoriza atos de defesa ativa além das fronteiras se não for atribuída a outro país.

Por fim, as características e princípios da guerra cibernética dificultam o processo de evolução normativa/interpretativa da Carta, particularmente quanto aos conceitos de uso da força, legítima defesa, necessidade e proporcionalidade, identificação da autoria e hostilidade que precisam ser harmonizados com a Carta em vigor.

3.3 MANUAL DE TALLINN

Aos moldes do que foi feito no processo de elaboração do Manual de San Remo e outros, em 2009, o Centro de Excelência em Defesa Cibernética Cooperativa da OTAN, com sede em Tallinn – Estônia, iniciou o processo de produção de uma manual sobre o Direito aplicável à Ciberguerra.

Desde 2007, foi percebida a presença dos Estados, por meio de suas forças armadas, em operações cibernéticas, a começar pelo ataque contra a Estônia, no mesmo ano, e, no ano seguinte, contra a Geórgia. Dois anos após, ocorreu o ataque ao projeto nuclear iraniano com utilização de código malicioso. Essa presença não se deu só com ataques, mas sim com maior atenção, estudos e a conscientização do novo teatro de operações e do novo domínio da guerra.

O Manual buscou a conexão do DIP ao *jus ad bellum* (direito à guerra) e *jus in bello* (direito na guerra) com enfoque na guerra cibernética, ou seja, estritamente nas operações cibernéticas contra alvos cibernéticos tanto para conflitos internacionais e locais ou de âmbito regional.

A componente humana desse processo foi um grupo de pessoas de notável saber no assunto, tais como operadores do Direito, técnicos no assunto e acadêmicos, que, por unanimidade, afirmaram a aplicabilidade das operações cibernéticas ao *jus ad bellum* e *jus in bello* e a aplicabilidade das leis vigentes.

O Manual contém noventa e cinco artigos, sendo dividido em duas partes que tratam:

a) Parte I – Lei internacional de segurança cibernética; e

b) Parte II – Lei do conflito armado cibernético.

A parte I divide-se em dois capítulos que tratam dos Estados e o ciberespaço e o uso da força. No primeiro capítulo é abordado a soberania, a jurisdição e o controle e, no segundo, a responsabilidade do Estado.

Já a parte II divide-se em cinco capítulos que tratam sobre o Lei dos conflitos armados; a condução das hostilidades; pessoas, objetos e atividades; e ocupação e neutralidade, respectivamente.

A fim de não desviar do escopo do presente estudo, a análise do Manual se aterá a primeira parte, especificamente ao primeiro capítulo.

Primeiramente, faz-se mister ressaltar o conceito de soberania que se constitui na independência na relação entre Estados, que seria a autonomia sobre determinada porção do globo, com exclusão de qualquer outro Estado, as funções do Estado[29]; assim como o de infraestrutura cibernética que é abrangida pelas comunicações, armazenamento e recursos computacionais sobre os quais os sistemas de informação operam; e operações cibernéticas que é o emprego da capacidades cibernéticas com os objetivos primários de atingir o opositor ou objetivo no ciberespaço ou por meio dele.

Percebidas as definições, segue-se para o primeiro capítulo que inicia em asseverar que, sob a égide do regramento internacional, os Estados podem ser responsabilizados pelas operações cibernéticas conduzidas por seus órgãos, podendo até ser imputados aos Estados às operações realizadas por outros atores não estatais. Ademais, as regras valem para tempo de paz e de guerra, ressaltando que durante o período de conflito, a lei de neutralidade abarca os direitos e obrigações no que tange a infraestrutura ciber e as operações cibernéticas.

Em seu art. 1°, o manual expõe que nenhum Estado pode reivindicar a soberania no ciberespaço, mas sim sobre a infraestrutura cibernética e atividades correlatas, localizadas no seu território, ou seja, porções de território onde o Estado tenha soberania plena (mar territorial, águas interiores, arquipélagos, território terrestre e espaço aéreo sobrejacente). Sobre essa infraestrutura, a soberania impõe o poder de império do Estado, logo está sujeita as suas Leis e regulações, todavia o Estado também tem o dever de protegê-las, independendo de qual finalidade e quem seja o detentor da propriedade.

---

[29] Conceito derivado de precedente firmado pela Corte Permanente de Justiça Internacional no laudo arbitral sobre a Ilha de Palmas de 1928.

Desse modo, uma operação cibernética conduzida por um Estado contra uma infraestrutura de outro Estado pode violar a soberania do atacado. Por exemplo, se essas operações configurarem uma coerção a determinado governo, recaem sobre a figura da intervenção proibida, prevista no art. 2° da Carta das Nações Unidas ou uso proibido da força, podendo ensejar o acionamento do Conselho de Segurança, represálias e até legítima defesa no caso dessas operações se qualificarem como ataques armados. (LUIZ VERGUEIRO, 2015)

Nesse contexto cibernético, o princípio da soberania dá poderes ao Estado para restringir ou proteger o acesso à Internet, sem prejuízo das normas do DIP, normas de Direitos Humanos ou de Telecomunicações internacionais, assim como o mesmo não é pleno nos casos previstos na Convenção das Nações Unidas sobre o Direito do Mar (CNUDM III) que tratam da passagem inocente, passagem em rotas marítimas arquipelágicas e passagem em trânsito. Porém, não há que se olvidar que, relativo a colocação de cabos submarinos, o Estado exerce controle total em seu mar territorial, mas não na plataforma continental visto que todos os Estados têm o direito de colocar cabos e dutos submarinos na plataforma continental em conformidade com as disposições do art. 79 da Convenção e o Estado Costeiro não pode impedir a colocação ou manutenção dos referidos cabos ou dutos, cabendo ao mesmo somente consentir quanto ao traçado da linha para a colocação.[30]

Luiz Vergueiro (2015, p. 634) nos brinda:

> Enfrentando a tensão aparente entre o conceito tradicional de soberania – adotado pelo Manual - e os novos paradigmas postos pelo ciberespaço, a célebre cientista política Saskia Sassen ensina que, embora a ideia da Internet como rede de redes descentralizada tenha contribuído para a noção de sua autonomia intrínseca com relação ao poder estatal, o núcleo da Internet está conformado por uma série de elementos de infraestrutura: os pontos de intermodo que seu grau de abertura e sua tecnologia contêm em si elementos com potencial controle indireto.

Tradicionalmente, a definição de violação de soberania está restrita aos Estados, entretanto existe uma corrente minoritária que já fala nessa violação por parte de atores não Estatais. E apesar dos Estados não exercerem a soberania no ciberespaço, os

[30] CNUDM III, arts. 17-19, 37-8, 52, 53 e 79(2).

mesmos podem exercer sua jurisdição sobre os cibercrimes e operações cibernéticas nos termos das normas internacionais, o que será explanado a seguir.

A palavra jurisdição é derivada do latim *jurisdictio* (administrar a justiça), sendo decorrente da soberania, visto que o Estado moderno, para atingir o bem comum, dividiu seu poder soberano em três, quais sejam: Poder Legislativo, Poder Executivo e Poder Judiciário, que tem por função, *lato sensu*, a resolução de litígios nos casos concretos. O Manual define jurisdição como a autoridade do Estado para editar normas, fazer serem cumpridas e julgar os casos concretos de violação, tendo com base para esse exercício a presença física de uma pessoa ou coisa em seu território. Ademais, pode-se alcançar até mesmo as entidades privadas que estão estabelecidas dentro do território, porém operam em um Estado alienígena. Ou seja, por estarem formalmente registradas em um Estado, estão aptas a sofrer a regulação deste.

Nessa linha, a jurisdição se baseia na territorialidade, apesar da dificuldade de determinação da jurisdição do ciberespaço em função da interconectividade do sistema e de operarem em nuvens e redes baseados fora das fronteiras, a pessoa e a infraestrutura estão fisicamente em algum lugar e assim sujeitas à jurisdição do Estado. Com a natureza territorial, a jurisdição deriva em dois outros tipos, que são: subjetiva e objetiva.

A natureza subjetiva abarca a aplicação da Lei do Estado exercendo jurisdição sobre atos praticados a partir de seu território e finalizado em qualquer outro local fora do Estado de origem. Já a natureza objetiva concede jurisdição sobre indivíduos onde os atos cibernéticos terão efeitos, mesmo que a ação tenha se iniciado fora de seu território.

É iminente destacar que o Manual de Tallinn também prevê hipóteses de extraterritorialidade da jurisdição do Estado em função das operações de guerra cibernética, em geral, produzir efeitos em um Estado-Alvo, a quem cabe e interessa a responsabilização dos autores da ação. As hipóteses supra são: nacionalidade do autor; nacionalidade da vítima;

questões de ameaça à segurança nacional; e violação de normas de Direito Internacional. Daí extrai-se que pode haver jurisdição concorrente por dois ou mais Estados, mas sem olvidar que esta não é plena, como nada do Direito, visto que há circunstâncias que a afastam, v.g. a imunidade diplomática.

Ponto que desperta interesse é sobre a situação dos navios e aeronaves. Contudo, antes, faz-se mister esclarecer alguns pontos.

Trazendo a jurisdição para âmbito marítimo, verifica-se que em alto-mar não há soberania nos termos do art. 89 da CNUDM III, ao passo que em águas interiores e mar territorial é consagrada a jurisdição plena do Estado costeiro, salvo as circunstâncias de extraterritorialidade, princípio da jurisdição do Estado de bandeira e passagem inocente. (MARCELO BARBOSA, 2015)

Ademais, o Manual define alto-mar como todas as áreas marítimas além do limite externo do mar territorial do Estado Costeiro e demarca o conceito de espaço aéreo internacional como sendo o espaço aéreo compreendido acima do alto-mar.

Nessas plataformas (navios, plataformas, aeronaves, satélites, entre outras), a infraestrutura cibernética estará a bordo dos mesmos e em muitos casos, esta infraestrutura comandará importantes sistemas a bordo, local onde a jurisdição aplicada é a do Estado de Bandeira, no caso dos navios, plataformas e embarcações de um modo geral e do Estado de Registro no caso das aeronaves e satélites. Nota-se que nesse caso também há a concorrência na jurisdição dos Estados. Ainda tratando dessas plataformas, há que se registrar e não confundir as plataformas que são providas de imunidade como as de Estado, independente do local onde estejam, e extensiva as pessoas, objetos e infraestrutura cibernética do meio, de acordo com as normas internacionais em vigor, com uma única ressalva referente a parte cibernética que deve atender aos propósitos governamentais para fazer jus a tal imunidade e qualquer violação a mesma é violação de normas internacionais.

Ainda sobre a infraestrutura cibernética, previsto no art. 5°, o Estado não pode permitir, conscientemente, que ela seja usada para ataques cibernéticos em outros Estados, seja essa localizada em seu território ou sobre o controle estatal com o intuito de prevenir de que a mesma seja empregada para infligir danos a pessoas ou à qualquer patrimônio situado fora de seu território. Para tal, o Grupo de Especialistas pautou-se em dois precedentes da Corte Internacional de Justiça.[31]

Nesse mesmo viés, o Manual ainda prevê que o Estado que permitir que sua infraestrutura cibernética, em seu território, seja utilizada por grupo terrorista para materializar ataque contra outro Estado; e esse mesmo que for notificado por outro Estado de que está sendo conduzida atividade cibernética e falhar na interrupção, infringe o art. retrocitado. Ademais, esse art. abrange ainda os atos contra o DIP originados de infraestrutura ciber sob o controle estatal que estão situadas fora do território do Estado controlador.

Se um Estado falha em assumir as ações para impedir que seu território seja usado para causar danos a um Estado alienígena, este tem o direito de resposta por violação de normas do Direito do Internacional, inclusive com fulcro no art. 51 da Carta das Nações Unidas.[32] Assim, um ilícito internacional pode gerar uma crise internacional com consequências graves, desde sanções até o uso da força[33] em legítima defesa[34].

---

[31] *Case concerning the military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America).* Disponível em: <http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5>. Acesso em: 08 abr. 2017.
Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania). Disponível em: <http://www.icj-cij.org/docket/index.php?p1=3&p2=3&case=1&p3=0>. Acesso em: 08 abr. 2017.

[32] Carta da Nações Unidas. Artigo 51. 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 e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais.

[33] Manual de Tallinn. Art. 11 – Uma operação cibernética constitui o uso da força quando sua escala e efeitos são comparáveis ao de uma operação não cibernética aumentando ao nível do uso da força.

[34] Manual de Tallinn. Art. 13 – O Estado que é alvo de uma operação cibernética equiparada à um ataque armado pode exercer seu direito a legítima defesa. Se uma operação cibernética é considerada um ataque armado depende de sua escala e efeitos.

No campo da guerra cibernética, foi visto que esse novo domínio adentra o complexo sistema de regramento internacional, sujeitando-se, por conseguinte as normas de Direito Internacional, como a Carta da ONU e, mais especificamente, as normas do Direito Internacional dos Conflitos Armados (DICA) que constituem elementos reguladores das condutas dos Estados, seja antes ou durante o conflito. (LUIZ VERGUEIRO, 2015)

Por fim, faz-se mister ressaltar que no próprio manual resta registrado que ele não é um documento oficial, mas sim o resultado de uma produção intelectual, não representando a posição da OTAN, Estados patrocinadores da Organização ou do Centro de Excelência em Defesa Cibernética Cooperativa, e nem a própria doutrina da OTAN. Além disso, nota-se uma concordância dos especialistas quanto ao regramento existente, sem a necessidade da criação de outro, somente fazendo-se necessária uma interpretação adaptada a esta nova realidade mundial, a guerra cibernética.

3.4 DESAFIOS E TENDÊNCIAS FACE AO DIREITO INTERNACIONAL PÚBLICO

O sistema social global move-se constantemente transformando-se em um tipo de aldeia global, seguindo a globalização que impõe novos paradigmas intensificando as relações sociais mundiais, conectando locais a quilômetros de distância de modo que alguns acontecimentos locais podem modelar eventos do outro lado do mundo e vice-versa, ou seja, estabelece-se uma globalidade de padrões, valores e ideias tendo como meio as redes de comunicação e a internet. (SIDNEY GUERRA, 2006)

A natureza transnacional da guerra cibernética, sem dúvida, necessita de uma resposta coordenada a nível internacional que exige um trabalho sobre as relações

---

Manual de Tallinn. Art. 14 – O uso da força envolvendo operações cibernéticas realizado por um Estado no seu direito de exercício da legítima defesa tem que obedecer aos critérios de necessidade e proporcionalidade.

internacionais que necessitam serem regulamentadas e controladas por normas jurídicas lineares e universais que enfrenta a diversidade presente no âmbito nacional dos Estados. Assim, a ciberguerra apresenta ao Direito Internacional desafios que envolvem a necessidade de se adaptar a esse novo domínio.

Essa adaptação começa pelas diferentes visões a respeito das políticas de segurança cibernéticas que são derivadas das distintas formas de tratar o fluxo de informações, a internet e das respostas estatais referente aos crimes cibernéticos, ressaltando que, analogamente às iniciativas das organizações mundiais no que tange a sua regulamentação, há , atualmente, quatro grandes modelos de pensamento sobre a segurança no espaço cibernético[35], que são: o americano que considera o ciberespaço sem fronteiras, defendendo que os ataques cibernéticos podem ser respondidos por força militar convencional; o europeu defende o livre fluxo da informação no espaço cibernético, com foco na proteção das infraestruturas críticas, cooperação internacional e combate aos crimes cibernéticos; o russo considera o ciberespaço sem fronteiras, mas com o fluxo de informações regulado; e o modelo chinês com o espaço cibernético com fronteiras e a circulação de informações com regulação.

Ainda nessa adaptação, Renata de Barros (2015, p. 118-121) assevera:

> A guerra travada no ciberespaço não pode ser analisada, de forma dissociada, da guerra convencional, pois é utilizada como uma nova capacidade de exploração da força, com novas dimensões e, portanto, modifica a forma como a guerra é realizada. [...] Apesar dessa forma positiva de se pensar na sociedade internacional complexa, as demandas, que surgem, não são solucionadas com a guerra cibernética somente pela instituição de tratados que possam regular essas relações, pois no ciberespaço, os Estados não são os únicos atores que podem ameaçar a segurança e praticar a guerra e nem sempre pode-se contar com a boa-fé dos Estados na obediência dos tratados. Os atores não regulados pelo Direito Internacional não podem ser ignorados, pois se apresentam como possíveis partícipes de uma guerra cibernética. A possível solução para a regulação e punição de ataques cibernéticos, realizados por entes privados, não caracterizados como sujeitos de Direito Internacional, como indivíduos e empresas, deveria contar com as jurisdições estatais ou internacionais, dotadas de competência para punir as violações praticadas. [...] A primeira premissa para se estudar um Direito Internacional regulatório do estado de guerra cibernética, que toda sociedade internacional hoje vive, é entender que embora ataques de rede de computador suscitem questões desafiadoras para as atuais leis de conflito armado,

[35] Palestra proferida por Raphael Mandarino no II Seminário de Defesa Cibernética, novembro de 2011.

> na maior parte, as leis existentes são capazes de se adpatarem à nova tecnologia.[...] Não há campo de batalha exclusivamente virtual, completamente dissociado da realidade do mundo real, no qual a guerra cibernética ocorra e que justifique a necessidade de uma legislação completamente nova para sua regulação. A guerra ainda é vivida nos espaços físicos, mas também utiliza-se das redes vituais para se propagar e provocar prejuízos de ruptura em massa.

Importante destacar que a percepção da egrégia autora supra fortifica a percepção do estudo e reforça o fato de que a legislação atual atinge o ciberespaço, que apesar de ser virtual, logo seu espaço não possui limitação física, porém sua infraestrutura cibernética e seus atores são "reais" e tem localização física passível de localização, apesar de ser difícil.

Para materializar a prova e assim ensejar uma responsabilização adequada pelos entes estatais, há que se localizar os atacantes e conectá-los as vítimas para se estabelecer uma conexão e a partir daí determinar o *link* que se mostra vital. Como muitos ataques ocorrem em locais distantes fisicamente da origem, faz-se mister a interação entre os atores soberanos de forma a combater os crimes virtuais, e até mesmo no caso de guerra cibernética com o cooperação internacional, não olvidando a dificuldade em se determinar o fato gerador, principalmente quando o mesmo é estatal. Assim, uma tendência que se apresenta é a cooperação, em função da visão do ciberespaço ser regional com ponto de vista regional, com a tendência até da criação de uma assistência legal internacional. (RENATA DE BARROS, 2015)

Consolidando essa tendência, traz-se à baila as iniciativas dos Estados Unidos da América e a Rússia (2011) sobre a terminologia para a segurança cibernética, denominado *Russia – U.S. Bilateral on Cybersecurity Critical Terminology Foundations*[36] com definições técnicas para o ciberespaço, circunstâncias agravantes e definições de ataque e contra-ataque, capacidade ofensiva e defensiva, exploração e intimidação, contramedidas e estado de guerra.

---

[36] Acordo firmado entre o *EastWest Institute* dos Estados Unidos e o *Information Security Institute of Moscou State University* da Rússia. Disponível em: <http://www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20(2).pdf>. Acesso em 20 mar. 2017.

Outra iniciativa foi o Manual de Tallinn[37], já exposto supra, elaborado pelo Centro de Excelência e Cooperação em Defesa Cibernética da OTAN, baseado em Tallin, na Estônia, coordenado pelo Professor Michael N. Schmitt. Ademais, destaca-se a proposta *Ten Rules of Behavior for Cyber Security* elaborada por autores de diferentes países e universidades e até membros do Centro de Excelência e de Cooperação em Defesa Cibernética da OTAN com dez princípios, destacando-se: cooperação, territorialidade, responsabilidade e criminalização. Ainda, há que se citar outra iniciativa de um professor de Direito Internacional ucraniano, Doutor Alexander Merezhko, que produziu uma proposta de Convenção Internacional para a Proibição da Guerra Cibernética, propondo que a internet seja usada exclusivamente para fins pacíficos, em prol da segurança e da liberdade. Ademais, estabelece que os Estados não devem recorrer/apoiar a guerra cibernética, comprometendo-se a tipificar essas condutas ilícitas e envidar esforços para o desenvolvimento de um sistema global de segurança. (SALDAN, 2012)

Isto posto, põe-se o desafio de que as normas do DIP possam alcançar respostas adequadas para os atos tipificados no ciberespaço e a guerra cibernética de forma a combatê-los e regulá-los, fortalecendo o exercício da soberania em detrimento da característica transnacional da ciberguerra, logo a aplicação das leis nacionais, mas, principalmente, do próprio Direito Internacional, que busca a solução pacífica dos conflitos sem o uso da força de forma a prevenir uma guerra, além da adequação da ONU, especialmente do CS, e do Tribunal Penal Internacional para conduzir investigações e julgar crimes decorrentes da guerra cibernética .

Por fim, investigadas o ordenamento internacional sobre o assunto em lide, sua relação e comportamento em relação do DIP e os desafios e tendências insta verificar a relação entre os Estados no campo da guerra cibernética para fins de soberania.

---

[37] MILCW – *Manual on Internacional Law Applicable to Cyber Warfare*. Disponível em: <http://www.ccdcoe.org/249.html>. Acesso em: 20 mar. 2017.

4 A RELAÇÃO ENTRE ESTADOS E GUERRA CIBERNÉTICA

Uma nova realidade se apresenta com a utilização do ciberespaço e como consequência direta o cometimento de ilícitos e a guerra cibernética, que traz a presença dos Estados para este campo figurando como atores no campo virtual e buscando preparar-se para o enfretamento às ameaças nesse novo domínio que desafia o poder soberano entes estatais.

4.1 SOBERANIA ABSOLUTA OU RELATIVA?

Inicialmente, insta consolidar que os ataques militares, com exceção da legítima defesa ou com autorização do Conselho de Segurança da ONU, são ilegais e figuram com atores estatais e soberanos. Com isso, essa análise de soberania passa pelas ações de guerra cibernética violando o ciberespaço que não tem limitações físicas, conforme já visto retro em suas características.

O conceito de soberania absoluta é um conceito ultrapassado no Direito Internacional e existem vários fatores que contribuem para o seu desgaste, em alguns aspectos. Com a globalização, há uma propensão a interdependência e cooperação entre os sujeitos de Direito Internacional. (QUINTÃO SOARES, 2008)

Modernamente, existem quatro conceitos de soberania em uso no DIP. Inicia-se pelo tradicional conceito de Westfália, que fulcrou o conceito de soberania com base na territorialidade, exclusão de fatores externos e o estabelecimento da autoridade soberana do Estado nessa porção de terra de forma a organizar a vida política. Segue-se com a concepção de soberania interna que é a capacidade de controle das relações no campo interno e a organização da autoridade política dentro do Estado. Ademais, tem-se, ainda, a soberania

jurídica internacional que tem como propósito estabelecer e manter o Estado como uma entidade política independente no sistema internacional. E, por último, a noção de soberania de interdependência que se refere com a aptidão do Estado para controlar e decidir nos movimentos de integração. (RENATA DE BARROS, 2015)

Insta registrar que Miguel-Angel Davara Rodríguez coloca em dúvida a questão da soberania dos Estados em função do desenvolvimento tecnológico, partindo da premissa do desvio de finalidade das normas e tendo como possível solução um regresso à ética clássica e aos princípios gerais do Direito para a concepção de um senso comum.

Vistos os conceitos supra, é notório que nenhum deles atende as demandas cibernéticas exigidas, visto que o ciberespaço tem a sua identidade e sua comunicação particular e interativa, levando a uma crença de que no ciberespaço não há limites, interferência ou regulação, logo imune à soberania dos Estados.

Entretanto, como já exposto supra, os atores – pessoas físicas – e as infraestruturas cibernética estão sujeitas à jurisdição e soberania do Estado pelo fato de estarem fisicamente sob o guarda-chuva estatal. Assim sendo, a soberania no ciberespaço faz-se presente em função do Estado necessitar tipificar e combater os cibercrimes que necessitam das infraestruturas com base territorial em algum Estado. Ademais, é mister regular as relações virtuais, até mesmo para assegurar o direito dos seus cidadãos e empresas de forma a dar segurança jurídica às relações entre as pessoas em sentido *lato*, de forma a assegurar, principalmente, o conteúdo das informações. (KRASNER, 1999)

Ante ao exposto, é notório que o princípio da soberania aplica-se ao ciberespaço, e, consequentemente, à guerra cibernética e não há que se falar em relativização, visto que o componente territorial é um princípio eficaz que deve ser aplicado ao ciberespaço, necessitando somente de uma nova interpretação do ordenamento internacional em vigor.

Para ilustrar o estudo, passa-se a um caso de guerra cibernética ocorrido no Irã, conhecido como s*tuxnet.*

4.2 CASO S*TUXNET*

Em 2009, ataques cibernéticos foram conduzidos com o *worm*[38] chamado s*tuxnet*[39]sobre os sistemas de computadores das instalações de enriquecimento nuclear da República Islâmica do Irã – Natanz – deflagrando uma Operação denominada *Olympic Games*, com o intuito de retardar o progresso no desenvolvimento da capacidade de construção de artefatos nucleares do país, com a estimativa de retardo de 18 a 24 meses. Posteriormente, como resultado dos ataques, foram colocadas fora de operação entre 1.000 e 5.000 centrífugas.[40] Por ocasião do ataque, a República Islâmica do Irã negou-o, contudo logo em seguida, afirmou que tinha contido o mesmo, ressaltando que o governo norte-americano nunca admitiu a autoria dos ataques, oficialmente. Inicialmente, depreende-se a dificuldade na identificação dos autores e a extraterritorialidade do ataque conforme os princípios da GC expostos no capítulo dois, além de ferir a soberania do Estado ao considerarmos a componente territorial conforme descrito acima, que mostra importante no EC.

Nessa operação, foi a primeira vez que os "Estados Unidos da América" utilizaram uma arma cibernética (*software*) a fim de paralisar uma infraestrutura física de um outro país. Ademais, há sinais de que houve colaboração das Forças Armadas de Israel, que

---

[38] É um programa auto-replicante semelhante aos vírus. Ele cria cópias funcionais de si mesmo e infecta outros computadores.

[39] Descoberto em 2010 pela empresa bielorussa *VirusBlokAda*, que verificou a infecção de sistemas de controle industriais fabricados pela empresa alemã Siemens. Segundo a empresa em lide, o *worm* foi introduzido nos sistemas com o intuito de controlar as plantas industriais não conectadas à Internet e que possuem portas USB. Assim, somente por meio de um *pen drive* infectado haveria a possibilidade de controlar e explorar suas vulnerabilidades.

[40] Disponível em: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-i-ran.html?_r=0>. Acesso em: 12 abr.2017. Disponível em: < https://www.foreignaffairs.com/articles/iran/2015-04-05/deal-it>. Acesso em: 12 abr. 2017.

detinha conhecimentos técnicos que rivalizavam com a *National Security Agency* (NSA) (SANGER, 2012). Assim, é perceptível o prejuízo causado à República Islâmica do Irã em uma infraestrutura física, ou seja, efeitos no mundo real.

O s*tuxnet*, com elevado nível de sofisticação, demonstrou possuir um vetor de ataque específico limitado a certos computadores que operam de forma bastante singular. De acordo com a empresa Symantec, havia cerca das 100.000 máquinas infectadas no mundo, sendo aproximadamente 60.000 localizadas no Irã, ou seja, ele possuía um alvo geográfico específico.[41]

Ainda de acordo com a Symantec, o *Stuxnet* foi programado para contaminar os *Programmable Logic Controller* (PLC)[42] abarcando quatro ataques *zero-day*[43] tendo como alvo as unidades conversoras de frequência, que controlam a velocidade de um motor.[44]

Essas unidades foram projetadas para receber comandos do *software* da Siemens que foram alterados pelo *worm*, fazendo com que os motores elétricos oscilassem em velocidades supersônicas, danificando quase 1.000 centrífugas que estavam interligadas.

O *worm* ficou inativo na planta por semanas, mas quando realizou o ataque, enviou sinais de aparente normalidade para sala de controle, configurando-se essa como sua característica mais sofisticada (LANGNER, 2013).

Logo, percebe-se que o *stuxnet* causou dano material ao Estado Iraniano, integrante da infraestrutura nuclear e estratégica do país, além de retardar o seu programa nuclear, ou seja, gera efeitos cinéticos no mundo real, um dos princípios da GC vistos supra. Além disso, outro fato notório nesse caso é que o sistema de controle não estava conectado à

---

[41] SYMANTEC, 2011, p. 5.
[42] *Programmable Logic Controller* (PLC) é um sistema de controle de computador industrial que monitora continuamente o estado de dispositivos de entrada e toma decisões 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 mar. 2017.
[43] *Zero-day* é um ciberataque que acontece no dia em que um ponto fraco for descoberto no software. Disponível em: < http://www.kaspersky.com/pt/in-ternet-security-center/definitions/zero-day-exploit>. Acesso em: 30 mar. 2017.
[44] SYMANTEC, *op. cit.*, p. 3.

rede mundial de computadores conforme exposto supra, logo algum agente foi responsável pela introdução do *worm*, sem usar o EC.

Outro fato digno de menção é o fato de ter sido realizada a engenharia reversa do s*tuxnet* e ficou constatado seu elevado nível de sofisticação, logo aventando uma possível participação estatal no ataque. (BROAD; MARKOF; SANGER, 2011)

Finalmente, no exemplo supra, percebe-se a dificuldade em materializar a identificação dos autores do ataque, que pode determinar dois caminhos, quais sejam: uma GC ou um crime cibernético. Dependendo do autor, o Estado pode adotar condutas diferentes de forma a responsabilizar o mesmo ou até exercer a legítima defesa, conforme já exposto no capítulo três desse estudo. Ademais, é mister não olvidar a extraterritorialidade do ataque visto que foi fora do território do atacante, e a República Islâmica do Irã poderá invocar o princípio penal da extraterritorialidade para tentar punir, após identificação, os responsáveis, a semelhança do ocorrido em Barcelona em abril de 2017[45], quando um cidadão russo foi preso por ser alvo de um pedido internacional de extradição dos Estados Unidos da América, com fulcro em uma **suposta participação** na ação de hackers na campanha eleitoral dos Estados Unidos, que teria favorecido a candidatura de Trump. (grifo nosso)

4.3 CASO *WANNACRY*

No dia 12 de maio de 2017 houve um ataque cibernético global, no qual 150 países foram afetados pelo código malicioso *wannacry*, atingindo inclusive órgãos do governamentais, como o Serviço Nacional de Saúde do Reino Unido e o Ministério Público

[45] Disponível em: <http://www.dw.com/pt-br/espanha-prende-suposto-hacker-russo-buscado-pelos-eua/a-38372403>. Acesso em 11 jul. 2017.

de São Paulo, sendo registrados, pelo menos, 200.000 mil ataques[46]. Registra-se a extraterritorialidade do ataque contra instituições de alguns Estados, assim como empresas privadas, entre outros, além do uso do EC como meio para os ataques.

Entendendo o w*annacry*, basicamente, este sequestra arquivos de dados, por meio de criptografia, em troca de resgates em *bitcoins*[47], aproveitando uma vulnerabilidade do sistema operacional, obrigando as vítimas a efetuarem o "resgate" em um determinado prazo sob ameaça de perdimento dos dados.[48]

Cabe salientar que isto foi revelado ao público como parte de um vazamento de documentos relacionados com NSA, que supostamente criou o w*annacry,* que tratam sobre ferramentas de hacking para infectar computadores e criptografar seus conteúdos.[49]

Como um dos princípios da GC é o anonimato, fato contínuo ao ataque global, foi a busca mundial para tentar identificar a origem do mesmo, tendo como uma das linha de investigação o idioma utilizado na tela de resgate. Algumas análises anteriores do *software* sugeriram que criminosos na Coréia do Norte, talvez, estivessem por trás disso, mas pesquisadores da empresa *Flashpoint*[50] identificaram que, na tela de resgate, a língua coreana tinha uma tradução pobre do texto em inglês. Contudo, constataram que o uso de gramática e pontuação, apenas na versão chinesa, indicou que quem digitou era "nativo ou pelo menos fluente" em chinês, sendo as demais traduções (28 idiomas) mais automatizadas, ou seja, ferramentas do tipo *Google Translator*. O professor Alan Woodward, especialista em segurança cibernética, da Universidade de Surrey, assevera que "foram apenas as versões chinesa e inglesa que pareciam ser escritas por alguém que entendeu o idioma", e os atacantes

---

[46] Disponível em: < http://www.bbc.com/news/technology-39896393>. Acesso em: 13 jun. 2017.
[47] O Bitcoin é uma nova moeda que foi criada em 2009 conhecida como dinheiro digital, *cryptocurrency*, a internet de dinheiro.
[48] Disponível em: <https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20>. Acesso em: 13 jun. 2017.
[49] Disponível em: < http://www.bbc.com/news/technology-39905509>. Acesso em: 13 jun. 2017.
[50] Empresa privada especializada em tecnologia. Disponível em: < https://www.flashpoint-intel.com>. Acesso em: 13 jun. 2017.

não tentaram resgatar o dinheiro pago pelas vítimas, a fim de não serem facilmente identificados.[51]

Já segundo a empresa de segurança russa Kaspersky, segue outra linha de investigação pelas semelhanças com um ataque realizado em Bangladesh, realizado pelo grupo Lazarus[52], acreditando que o grupo trabalhou fora da China, mas em nome dos norte-coreanos em função de semelhanças encontradas entre o código encontrado dentro do *wannacry* e outras ferramentas que o Lazarus criou no passado.

Independente da linha de investigação adotada, percebe-se que não há certeza sobre a autoria, entretanto, até agora pouco foi falado sobre a presença estatal no ataque, mas sim sobre grupos de *hackers*, fato este comum no EC. Assim, a tendência é rumo a um crime cibernético visto que não há indícios de presença estatal.

A única característica comum é a extraterritorialidade e consequente ofensa à soberania, visto que foi desferido indiscriminadamente contra vários países, o que enseja preocupação, especialmente no que tange aos órgãos governamentais, em função de poder ser um possível fato gerador de uma guerra cibernética por ensejar o direito de legítima defesa contra uma infraestrutura crítica de um país que esteja acobertando ou não tenha tomado providência acerca de um crime cibernético praticado do seu território, conforme já exposto no capítulo três.

---

[51] Disponível em: < http://www.bbc.com/news/technology-39926855>. Acesso em: 13 jun. 2017.
[52]Grupo de hackers altamente sofisticado responsável pelos ataques na Sony Pictures em 2014, e outro em um banco de Bangladesh em 2016.

5 CONCLUSÃO

A ciberguerra ou guerra Cibernéttica é o mais novo domínio da guerra, sendo travado no campo de batalha virtual, que é denominado espaço cibernético. É necessário entender seu conceito em termos gerais em função de que cada sujeito de Direito Internacional possuir um diferente. Isto posto, registre-se o conceito do Departamento de Defesa do Estados Unidos da América que é uma teoria emergente da guerra na era da informação, em que há a identificação de novas fontes de poder e sua relação entre si e com os resultados e objetivos políticos; e o brasileiro como sendo o conjunto de ações para uso de informações e seus sistemas para perturbar o adversário, com fulcro em informações, sistemas de informação e redes de computadores a fim de obter vantagens em qualquer campo.

Para entender a ciberguerra investigou-se o que é a guerra cibernética, seus princípios, o ambiente em que opera (ciberespaço) e seus conflitos; destacando-se o ciberespaço que se configura como um espaço altamente atrativo para atividades ilícitas sendo fonte potencial de conflitos nesse novo domínio por seu caráter transnacional e facilidade de ocultação, assim como os respectivos ataques que se configuram como o fato gerador de conflitos e são divididas em três grandes blocos: guerra cibernética, entre atores estatais; terrorismo cibernético e crime cibernético.

Nesse bojo da guerra cibernética, é fato que os países estão se mobilizando para desenvolver novas estratégias de segurança, sendo uma dessas mobilizações no campo intelectual, visto que vários Estados e Organizações Internacionais, destacando a própria ONU e a OTAN, já se dedicam a estudar a guerra cibernética, tendo como produto dessa atividade o Manual de Tallinn da OTAN.

Com essas iniciativas, estudou-se a regulamentação da guerra cibernética pelo DIP, passando por suas fontes, chegando ao ordenamento vigente, que busca vencer o desafio

de regular esse espaço sem utilizar a censura e monitoramento e assim adaptar ou trazer a baila uma nova interpretação do DIP para o ciberespaço aspirando ao benefício comum da humanidade, com a preservação de dois pressupostos fundamentais para a regulação do espaço cibernético: proteção dos recursos físicos de difusão da informação e a identificação dos usuários.

Nesses pressupostos, o Estado exerce sua autoridade soberana em função de sua localização ser real e não virtual e assim sujeito as consequências jurídicas, porém não é tão simples quanto parece dadas as tecnologias existentes e a possibilidade de efetuar ataques utilizando estruturas de terceiros, além da dificuldade em provar o mesmo. Nesse ambiente transnacional, faz-se necessário uma cooperação internacional legal, devido ao enfoque multilateral da questão e com a presença cada vez maior das forças armadas.

Além dessa multilateralidade, verificou-se que há legislação em vigor e que a mesma já atende, sendo exemplo a Carta da ONU, porém é necessário a mudança metodológica de interpretação jurídica para uniformizar condutas ou até mesmo expandir a interpretação das normas para abarcar esse novo domínio da guerra que requer novas definições de força, armas e ataque para esclarecer o que se considera uma arma cibernética, quais ataques são toleráveis e como o uso da força opera nesta modalidade, bem como a medida da necessidade e da proporcionalidade da resposta, visto que esses ataques podem causar danos físicos ou morte de seres humanos, assim como as perturbações de ordem econômica que ameaçam a paz. Assim, as características e princípios da guerra cibernética dificultam o processo de evolução normativa/interpretativa da Carta, particularmente quanto aos conceitos de uso da força, legítima defesa, necessidade e proporcionalidade, identificação da autoria e hostilidade que precisam ser harmonizados com a Carta em vigor.

Já o Manual de Tallinn configurou-se como um processo de produção de uma manual sobre o Direito aplicável à Ciberguerra, buscando uma conexão do DIP ao *jus ad bellum* e *jus*

in bello com enfoque na guerra cibernética, ou seja, estritamente nas operações cibernéticas contra alvos cibernéticos tanto para conflitos internacionais e locais ou de âmbito regional, iniciando com o conceito de soberania e asseverando que os Estados podem ser responsabilizados pelas operações cibernéticas conduzidas por seus órgãos, podendo até ser imputados aos Estados às operações realizadas por outros atores não estatais em tempo de paz e de guerra. Ademais, foi frisado que nenhum Estado pode reivindicar a soberania no ciberespaço, mas sim sobre a infraestrutura cibernética e atividades correlatas, localizadas no seu território, ou seja, porções de território onde o Estado tenha soberania plena e assim exercer sua jurisdição que pode ser objetiva ou subjetiva.

Verificou-se também que o Manual prevê hipóteses de extraterritorialidade da jurisdição do Estado em função do efeito das operações de guerra cibernética ser materializado em um Estado-Alvo, a quem cabe e interessa a responsabilização dos autores da ação; e a situação particular dos navios e aeronaves como plataformas móveis e que circulam diariamente pelo globo.

Finalizando ao que tange ao Manual, ficou registrado que ele não é um documento oficial, mas sim o resultado de uma produção intelectual, não representando a posição da OTAN e nem a própria doutrina da OTAN, mas uma concordância dos especialistas quanto ao regramento existente, sem a necessidade da criação de outro, somente fazendo-se necessária uma interpretação adaptada a esta nova realidade mundial, a guerra cibernética.

Com o avançar do estudo, ficou evidenciado que o DIP tem desafios pela frente e necessita de uma resposta coordenada a nível internacional para se adaptar a esse novo domínio de forma a alcançar respostas para os atos tipificados no ciberespaço e a guerra cibernética de forma a combatê-los e regulá-los, fortalecendo a soberania em detrimento da característica transnacional da ciberguerra e consequentemente do DIP, lembrando que a virtualidade não existe sem o componente físico.

Assim, apresenta-se uma tendência que é a cooperação, em função da visão do ciberespaço ser regional com ponto de vista regional, com até a criação de uma assistência legal internacional.

Isto posto, passou ao estudo da relação entre os Estados no campo da guerra cibernética para fins de soberania a qual ficou revelado que não há que se falar em relativização da mesma, apesar dos conceitos de soberania não se encaixarem nesse novo domínio da guerra. A soberania mostrou-se absoluta e interativa de forma a combater os cibercrimes e evitar uma guerra cibernética.

Concluindo, entende-se que a guerra cibernética têm suas peculiaridades, destacando-se a transnacionalidade e ocultação, e não olvidando as iniciativas da comunidade internacional sobre a questão da extraterritorialidade e possíveis consequências, verificando que não há relativização da soberania dos Estados frente ao caráter transnacional da guerra cibernética, que está abarcada pelos princípios basilares do Direito Internacional de preservação da paz e segurança, poder soberano dos Estados e não utilização da força. Todavia, nessa nova “ciber-realidade”, os Estados devem se adequar e romper os paradigmas de forma a não utilizar o ciberespaço como ferramenta de domínio e violação do DIP e buscar uma nova metodologia de interpretação jurídica para uniformizar o entendimento do ordenamento em vigor que se mostrou adequado.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTS, David S. ***Network centric warfare: developing and leveraging information superiority***. 2. ed. rev. *Cooperative Research Program Series: Library of Congress*, 2000.

ALEXANDER, Keith B. ***Warfighting in cyberspace***. *National Defense University Washington DC Institute for National Strategic Studies*, 2007. Disponível em: < http://www.dtic.mil/get-tr-doc/pdf?AD=ADA518148>. Acesso em: 10 mar. 2017.

AMORIM, Celso. **Segurança Internacional: Novos desafios para o Brasil.** Revista Contexto Internacional. Vol. 35, n° 1, jan./jun. 2013, p.287-311. Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro, 2013. Disponível em: < http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292013000100010&lng=pt&tlng=pt>. Acesso em: 10 mar. 2017.

BARROS, Renata Furtado de. Guerra Cibernética: **Os novos desafios do Direito Internacional.** Belo Horizonte: Editora D'Plácido, 2015.

BONANATE, Luigi. **A guerra.** São Paulo: Estação Liberdade, 2001.

BRASIL. Ministério da Defesa. **MD35-G-01: glossário das Forças Armadas**. 4.ed. Brasília: Ministério da Defesa, 2007.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde: segurança cibernética no Brasil.** Org. Claudia Canongia e Raphael Mandarino Junior. Brasília: 2010. 63 p.

BRASIL. Presidência da República. Secretaria de Assuntos Estratégicos da Presidência da República. **Desafios estratégicos para segurança e defesa cibernética.** Org. Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes e Whitney Lacerda de Freitas. Brasília: 2011. 216 p.

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: 30 mar. 2017.

CAPEZ, Fernando. **Curso de Direito Penal, volume 1: parte geral.** 10 ed. rev. atual. São Paulo: Saraiva, 2006.

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 V. **Da guerra.** 2. ed. São Paulo: Editora Martins, 1996.

DIPERT, Randall R. ***Other-than-internet (OTI) cyberwarfare: challenges for ethics, law and policy.*** *Journal of Military Ethics*, NY, v. 12, n. 1, p. 34-53, 2013. Disponível em: <http://dx.doi.org/10.1080/15027570.2013.785126>. Acesso em: 10 mai. 2017.

GUERRA, Sidney. **A internet e os desafios para o direito internacional**. Revista eletrônica da Faculdade de Direito de Campos, Campos dos Goytacazes, RJ, v. 1, n. 1, nov. 2006. Disponível em: <http://bdjur.stj.jus.br//dspace/handle/2011/18803>. Acesso em: 10 mar. 2017.

KRASNER, Stephen D. ***Sovereignty: organized hypocrisy.*** Princeton: Princeton University Press, 1999, 264 p.

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: 30 mar. 2017.

LIBICKI, Martin C. ***The Mesh and the Net. Speculations on armed conflict in a time of free silicon.***Washington DC: *National Defense University*, 1996.

MANDARINO JÚNIOR, Raphael. **Segurança e defesa do espaço cibernético brasileiro.** Recife: Cubzac, 2010.

MARQUES, Fernando César de Siqueira. **A Guerra Cibernética e o Direito Internacional dos Conflitos Armados**. Rio de Janeiro: Escola de Comando e Estado-Maior do Exército, 2012. CD-ROM.

MARQUES, José Augusto Sacadura Garcia. **Telecomunicações e proteção de dados. As telecomunicações e o direito na sociedade da informação.** Coimbra: Instituto Jurídico da Comunicação, 1999.

MAZZUOLI, Valério de Oliveira. **Curso de direito internacional público**. 3. ed. rev., atual e ampl. São Paulo: Editora Revista dos Tribunais, 2008.

MOURÃO, Anderson Marques. **Guerra Cibernética e o DICA: a tecnologia desafia a Lei da Guerra**. Dissertação (Mestrado). Rio de Janeiro: Escola de Guerra Naval, 2014. CD-ROM.

NUNES, Luiz Artur Rodrigues. **Guerra Cibernética. Está a MB preparada para enfrentá-la?** Dissertação (Mestrado). Rio de Janeiro: Escola de Guerra Naval, 2010. CD-ROM.

_____. **Guerra Cibernética e o Direito Internacional : Aplicabilidade do *Jus ad Bellum* e do *Jus in Bello***. Rio de Janeiro : Escola Superior de Guerra, 2015. 60f. CD-ROM.

OLIVEIRA, Luis Henrique Almeida de. **Cyberwar: novas fronteiras da guerra.** 2011. 69 f. Monografia (Especialização em Relações Internacionais) — Universidade de Brasília, Brasília, 2011. Disponível em: < http://bdm.unb.br/bitstream/10483/1991/1/2011_LuisHenriqueAlmeidadeOliveira.pdf>. Acesso em: 10 mar. 2017.

PAESANI, Liliana Minardi, coord. **O Direito na sociedade da informação**. São Paulo: Atlas, 2007.

_____. Direito de informática: comercialização e desenvolvimento internacional do *software*. 6. ed. São Paulo: Atlas, 2007.

PAPANASTASIOU, Afroditi. ***Application of international law in cyber warfare operations*** (September 8, 2010). Disponível em: <http://ssrn.com/abstract=1673785>. Acesso em: 25 mar. 2017.

PARKS, Raymond C., DUGGAN, David P. ***Principles of Cyberwarfare***, *IEEE Security & Privacy*, vol. 9, no. 5, pp. 30-35, September/October 2011. Disponível em: < https://pdfs.semanticscholar.org/ea86/ceef326d328fbf3ced92f9a27d85cd727d7c.pdf>. Acesso em: 15 abr. 2017.

PEREIRA, Leonardo Pires Black. **A Guerra Cibernética e o Direito Interrnacional: a aplicação do DICA no ciberataque realizado nas facilidades de enriquecimento de urânio do Irã em Natanz com a utilização da arma cibernética *Stuxnet*.** Dissertação (Mestrado). Rio de Janeiro: Escola de Guerra Naval, 2015. CD-ROM.

PONCE, Guerric. ***La nouvelle cyberguerre mondiale***. Le point, n. 2316, p. 50-62, 2017.

QUINTÃO SOARES, Mário Lúcio. **Teoria do Estado: novos paradigmas em face da globalização.** São Paulo: Atlas, 2008.

REPETTO, Guillermo. ***La ciberguerra***. *Revista de la Escuela de Guerra Naval*. Año XXXIII, p. 160-183, 2001.

REZEK, Francisco. **Direito internacional público: curso elementar**. São Paulo: Saraiva, 2000.

RODRIGUÉZ, Miguel-Angel Davara. ***La liberalización del mercado de las telecomunicaciones: uma perspectiva desde la ética.* As telecomunicações e o direito na sociedade da informação**. Coimbra: Instituto Jurídico da Comunicação, 1999.

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 mai. 2017.

SALDAN, Eliane. **Os desafios jurídicos da guerra no espaço cibernético**. Brasília, 2012. 118 f. - Dissertação (Mestrado). Instituto Brasiliense de Direito Público.. Disponível em: < http://dspace.idp.edu.br:8080/xmlui/handle/123456789/1223 >. Acesso em: 10 mar. 2017.

SCHMITT, Michael N. ***The Law of cyber targeting.*** *Naval War College Review*, v. 68, n. 2, p. 11-30, 2015. Disponível em: < https://www.usnwc.edu/getattachment/05986280-7072-4038-a253-560105093fbe/The-Law-of-Cyber-Targeting.aspx>. Acesso em: 10 mar. 2017.

_____. ***Internacional Law in cyberspace: The Koh speech and Tallinn Manual juxtaposed.*** *Harvard Internacional Law Journal*.v. 54, p. 13-37, 2012. Disponível em: < http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/>. Acesso em: 10 mar. 2017.

_____. ***Tallinn Manual on the Internacional Law Applicable to Cber Warfare.*** *Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defensa Centre of Excellence.* Cambrigde: Cambridge University Press, 2013.

SILVA, Júlio Cezar Barreto Leite da. **Guerra cibernética: a guerra no quinto domínio, conceituação e princípios**. Revista da Escola de Guerra Naval. v. 20, n. 1, 2014. Rio de Janeiro: Revista da Escola de Guerra Naval.

STYTZ, Martin R. ***Cyberwafare distributed training.*** Military Technology, v. XXX, 11 ed., p. 95-99, 2006.

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: 30 mar. 2017.

TORRES, Lucia Regina de Castro. **Defesa Cibernética na MB: Desafios e perspectivas para a próxima década**. Rio de Janeiro: Escola de Guerra Naval, 2012. CD-ROM.

TZU, Sun. **A arte da guerra**. 17. ed. Rio de Janeiro: Editora Record, 1996. 111 p. Tradução de José Sanz.

UN. ***United Nations*.** http://www.un.org. Acesso em: 20 mar. 2017.

UNIDIR. ***United Nations Institute for Disarmament Research***. http://www.unidir.org. Acesso em: 20 mar. 2017.

VERGUEIRO, Luiz Fabricio Thaumaturgo. **Marco civil da internet e guerra cibernética: Análise Comparativa à luz do Manual de Talin sobre os princípios do Direito Internacional aplicáveis à guerra cibernética.** Direito & *Internet III*, Marco Civil da Internet, Lei n° 12.965/2014. Tomo II, 1. ed., p. 619-640. São Paulo: Quartier Latin, 2015. 686 p.

WARFARE, Network-Centric. ***The Implementation of Network-Centric Warfare***. Department of Defense. *Office of Force Transformation* Washington DC, 2005.

WEINER, Norbert. ***Cybernetics or control and communication in the animal and the machine.*** 2. ed. Nova Iorque: John Wiley & Sons Inc., 1965. 232p.

_____. **Cibernética e a sociedade: o uso dos seres humanos.** Tradução José Paulo Paes. São Paulo: Cultrix, 1954.

YANNAKOGEORGOS, Panayotis A. ***Internet Governance and National Security***. *Air University Maxwell AFB AL Air Force Research Institute*, 2012. Disponível em: < http://www.dtic.mil/get-tr-doc/pdf?AD=ADA619096>. Acesso em: 10 abr. 2017.

ZUCCARO, Paulo Martino. **Tendência global em segurança e defesa cibernética – reflexões sobre a proteção dos interesses brasileiros no ciberespaço.** *In*: **Desafios** estratégicos para segurança e defesa cibernética. Org. Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes e Whitney Lacerda de Freitas. Brasília: 2011. 216 p.