A GUERRA CIBERNÉTICA NO AMBIENTE MARÍTIMO*

MARCELO DE SOUZA BARBOSA**
Capitão de Corveta

SUMÁRIO

CONSIDERAÇÕES PREAMBULARES

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

É inquestionável que o mundo, com modernas tecnologias computacionais e de comunicações, vem sofrendo transformações signi¿cativas que estão in uenciando

* Adaptação da dissertação "A extraterritorialidade no ambiente da guerra cibernética à luz do Direito Internacional Público" apresentada, em 2017, à Escola de Guerra Naval – Curso de Estado-Maior para O¿ciais Superiores (Cemos).

** Mestre em Ciências Navais pela Escola de Guerra Naval. Bacharel em Direito pela Universidade Federal do Rio de Janeiro. Pós-graduado em Direito Marítimo pela Maritime Law Academy. Mestre em Direito Econômico e Desenvolvimento pela Universidade Cândido Mendes. Legal Advisor da Força-Tarefa Marítima da United Nations Interim Force in Lebanon (Uni¿l).

a vida da sociedade, tendo a internet[1] um papel fundamental. Com seu surgimento, a sociedade ¿rmou um sistema global, tendo aquela como ambiente de interação, permitindo o acesso e a 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, um indivíduo ou o 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 tem levado a mudanças não somente nos domínios, mas no modo de condução da atividade cibernética, nos seus limites e nos conflitos oriundos dele, os quais estão crescendo nos últimos anos em um ritmo acelerado.

Este assunto tornou-se tão relevante que os Estados e as 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 ¿rmar 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.

Não há que se olvidar a regulamentação da guerra cibernética no DIP, tendo por conteúdo a Carta da Organização das Nações Unidas, que foi escrita antes do fenômeno da internet. Assim, a ciberguerra torna-se um desa¿o, especialmente no que tange ao uso da força com suas de¿nições clássicas e o teatro de operações, que foge do campo físico e evolui para o virtual.

A ciberguerra torna-se um desa¿o, especialmente no que tange ao uso da força com suas de¿nições clássicas e o teatro de operações, que foge do campo físico e evolui para o virtual

Nesse mundo virtual interligado, estão inseridos os conceitos de espaço cibernético (ECiber) ou ciberespaço, ataques cibernéticos (AC) e guerra cibernética (GC) ou ciberguerra. Ainda nesse 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 elas. Assim sendo, favorece-se a prática de atos ilícitos, como invasões à rede ou roubo de informações, denominados ataques cibernéticos, que podem evoluir para um estado de guerra[3], constituindo-se uma guerra cibernética.

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 Abrange a internet, além de várias outras redes, incluindo as transnacionais e as bancárias. (KNAKE, 2015, p. 60-61)

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 identi¿cados como sujeitos do Direito Internacional.” (RENATA DE BARROS, 2015, p. 92)

Tratando-se da ciberguerra, investiga-se como se comporta a soberania dos Estados nesse novo domínio, se de maneira absoluta ou relativa, de forma que o Estado possa combater essa atividade; e particularmente a situação dos navios e plataformas que trafegam pelo globo e são responsáveis pela espinha dorsal da economia global, visto que transportam mais de 80%[4] do comércio mundial e possuem uma característica ímpar, a extraterritorialidade.

José Augusto Sacadura Garcia Marques[5] 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.

Miguel-Angel Davara Rodríguez[6] coloca em dúvida a questão da soberania dos Estados em função do desenvolvimento tecnológico, partindo da premissa do desvio de ¿nalidade 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.

À consideração do supra exposto, o propósito deste artigo consiste na análise da guerra cibernética, veri¿cando como se comporta a soberania estatal, principalmente no que tange aos navios.

GUERRA CIBERNÉTICA

Mas o que é a guerra cibernética? A guerra cibernética é uma violência contra o opositor utilizando o ambiente dos computadores, sistemas de comunicação e transmissões eletrônicas, sendo considerado o mais novo domínio da guerra, sendo travado no campo de batalha virtual, que é denominado espaço cibernético.

O Glossário das Forças Armadas (Brasil) de¿ne 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 ¿m de obter vantagens em qualquer campo.[7]

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

> Guerra Cibernética é o termo amplamente de¿nido 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 ou 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)

Neste 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 con[illegible]os.

Princípios da guerra cibernética

Parks e Duggan (2011, p. 32-34) consideram oito princípios sobre a ciberguerra,

4 Disponível em: http://www.imo.org/en/about/pages/default.aspx. Acesso em: 29 out. 2017.
5 Telecomunicações e proteção de dados. As telecomunicações e o direito na sociedade da informação, p. 85.
6 La liberalización del mercado de las telecomunicaciones: una perspectiva desde la ética.
7 BRASIL. Ministério da Defesa. MD35-G-01: Glossário das Forças Armadas. 2007.

quais sejam: a) Princípio da falta de limitação física; b) Princípio do efeito cinético; c) Princípio da discrição; d) Princípio da mutabilidade e inconsistência; e) Princípio da identidade e privilégios; f) Princípio da dualidade; g) Princípio da infraestrutura de controle; e h) Princípio da informação.

Assim, 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 fulcro em operações assimétricas.

Por ¿m, 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.

O espaço cibernético

Richard Clarke (2015) assegura que o espaço cibernético faz-se presente em todas as redes de computadores e em tudo conectado a elas. Ademais, 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 ela, ou seja, segregadas. Não há que se olvidar, ainda, as redes transnacionais que fazem o £uxo de dados e as de sistema de controle, muito usuais nas indústrias.

Investigando a conceituação, veri¿ca-se que a Organização das Nações Unidas (ONU)[8] de¿ne o espaço cibernético[9] 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[10] define-o como espaço virtual, interconectado ou não, onde trafegam e são processadas as informações digitais. Logo, nota-se que não há um conceito dominante e aceito universalmente.

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

Os conÀitos no espaço cibernético

Neste tópico será investigada a relevância dos ataques que podem originar os con£itos no ciberespaço, que se con¿guram como ameaças.

No espaço cibernético não há uma clara de¿nição 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

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

9 Para outras de¿nições veja: NATO Cooperative Cyber Defense, Centre of excellence. Tallinn, Estonia. Disponível em: < https://ccdcoe.org/cyber-de¿nitions.html> Acesso em: 12 de março de 2017.

10 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.

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 ¿nalidades, critérios e abrangências variáveis.

Em pesquisa realizada pelo Center for Strategic and International Studies[11], foram ouvidos 600 executivos da área de segurança de empresas de infraestruturas críticas de 14 países, constatando-se que mais de 50% das empresas já sofreram ataques de grande escala ou invasões de governos, grupos criminosos ou terroristas.

No campo internacional, 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.[12]

No campo internacional, a Otan considera que os conÀitos cibernéticos estão entre as mais prováveis ameaças não convencionais e divulgou que um ataque contra uma infraestrutura crítica de um país membro pode gerar uma resposta militar

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

Consolidado o conceito de ataque e situado acerca da importância da matéria diante da comunidade internacional, esses ataques con¿guram-se como o fato gerador de conflitos, que são denominados como ameaças e divididos 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 ¿ca por conta do fato de que seus autores, normalmente, serão grupos não estatais. 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

11 Relatório disponível em: <http://img.en25.com/Web/McAfee/CIP_report_¿nal_pt-br_fnl_lores.pdf>. Acesso em 24 fev. 2017.

12 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.

exemplo, uma grande multinacional de uma potência econômica ocidental.

Crime cibernético ou cibercrime – quanto a este último bloco, geralmente as motivações serão de indivíduos ou de pequenos grupos, com ¿ns 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 a¿ns.

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

Regressando aos con  os, 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 o¿cialmente qualquer tipo de ataque cibernético, assim como não há provas que permitam inferir sua autoria a qualquer Estado.

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 do potencial das ameaças para colocar a segurança dos países em risco. Uma 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 de¿nições 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 de a comunidade internacional de¿nir regras e conceitos 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 e, assim, evitar con  os.

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

A REGULAMENTAÇÃO DA GUERRA CIBERNÉTICA

Ordenamento Internacional

Os atores presentes no ciberespaço participam de múltiplas relações de proporções globais e com características de espaço global, portanto são regulados pelo Direito Internacional, que busca vencer o desa¿o de regular esse espaço sem utilizar censura e monitoramento e, assim, adaptar ou trazer à 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 identi¿cação dos usuários.

Sobre os recursos de difusão, estes 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 e 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, abar-

cando, consequentemente, o princípio da extraterritorialidade em termos de matéria penal, além dos princípios de regras do Direito Internacional.

No que tange à identi¿cação dos usuários, é fato que a localização dos atores não é virtual, mas sim, possui uma localização geográ¿ca, seja o ator pessoa física ou jurídica, ocasionando sua submissão à soberania do Estado e ¿cando, assim, sujeito às 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 di¿culdade em comprovar o ataque e o local. Nesse ambiente transnacional, faz-se necessária uma cooperação legal internacional, em que o DIP entra em cena.

Aplicando-se 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 ¿to 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 na Assembleia Geral da Organização das Nações Unidas. 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 a internacionalidade referentes 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, da União Europeia (UE) e da Organização de Cooperação de Xangai (OCX), entre outras.

Entre as organizações, cabe ressaltar a Otan, que 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, este centro, em parceria com a Universidade de Cambridge, publicou o Manual de Tallinn, que foi a primeira tentativa de se veri¿car se as atuais leis da guerra seriam aplicáveis ao novo domínio da guerra, o que será visto posteriormente.

A guerra cibernética tem se mostrado tão inquietante que desde 1998 os Estados têm registrado dúvidas acerca do assunto na Assembleia Geral da Organização das Nações Unidas

A ONU também tem fomentado a formação de uma mentalidade de segurança cibernética, disseminando a necessidade de políticas globais a ¿m de não colidir com a dinâmica de manutenção da paz e da estabilidade internacionais. Assim, há que se analisar a Carta da Organização das Nações Unidas e perscrutar as de¿nições tradicionais com o ¿to de posicioná-las perante a guerra cibernética como “Lei Maior”, com base no exposto.

Carta da Organização das Nações Unidas

A Carta de São Francisco criou a ONU com o intuito de manter a paz e a 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 e também quais medidas devem ser tomadas 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[13], individual ou coletiva, o qual pressupõe identi¿cação 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 justi¿cável o ataque somente quando o dano causado é compatível com um ataque cinético, hipótese que justi¿ca a legítima defesa, conforme o artigo 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 de¿nições de força[14], armas e ataque serem insu¿cientes para esclarecer o que se considera uma arma cibernética, quais ataques são toleráveis e como o uso da força opera nessa modalidade, bem como a medida da necessidade e da proporcionalidade da resposta.

> Os ataques cibernéticos podem de¿nitivamente causar danos físicos ou morte de seres humanos, assim como perturbações de ordem econômica que ameaçam a paz

Os ataques cibernéticos podem de¿nitivamente causar danos físicos ou morte de seres humanos, assim como perturbações de ordem econômica que ameaçam a paz. Sem tardança, há que se revisitar o paradigma do jus ad bellum a ¿m 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. 2º da Carta, a ¿m de possibilitar que se invoque o direito à legítima defesa.

Mas qual seria essa nova interpretação? Uma interpretação mais expansiva incluiria todas as ações de guerra cibernética dentro da de¿nição de uso da

13 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.

14 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.

força, todavia os atos de coerção seriam arrastados a contrabordo. Por outro lado, mostra-se imperioso de¿nir 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 de¿nição 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, o rastreamento 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 identi¿cado, por conseguinte não autoriza atos de defesa ativa além das fronteiras se não for atribuída a outro país.

Por ¿m, as características e os princípios da guerra cibernética di¿cultam o processo de evolução normativa/interpretativa da Carta, particularmente quanto aos conceitos de uso da força, legítima defesa, necessidade e proporcionalidade, identi¿cação da autoria e hostilidade que precisam ser harmonizados com a Carta em vigor.

Manual de Tallinn

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

O manual buscou a conexão do DIP ao jus ad bellum (direito à guerra) e ao jus in bello (direito na guerra) com enfoque na guerra cibernética, ou seja, estritamente nas operações cibernéticas contra alvos cibernéticos tanto para con[illegible]os 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, a¿rmaram a aplicabilidade das operações cibernéticas ao jus ad bellum e ao jus in bello e a aplicabilidade das leis vigentes.

O manual contém 95 artigos, sendo dividido em duas partes: Parte I – Lei Internacional de Segurança Cibernética; e Parte II – Lei do Con[illegible]o Armado Cibernético.

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

O primeiro capítulo inicia asseverando 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 as operações realizadas por outros atores não estatais. Ademais, as regras valem para tempo de paz e de guerra, ressaltando que, durante o período de con[illegible]o, a lei de neutralidade abarca os direitos e as obrigações no que tange à infraestrutura ciber e às operações cibernéticas.

Em seu art. 1º, 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, nas 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 ¿nalidade e de quem seja o detentor da propriedade.

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 con¿gurarem uma coerção a determinado governo, recaem sobre a ¿gura da intervenção proibida, prevista no art. 2º da Carta das Nações Unidas, ou no uso proibido da força, podendo ensejar o acionamento do Conselho de Segurança, represálias e até legítima defesa no caso dessas operações se quali¿carem como ataques armados (LUIZ VERGUEIRO, 2015).

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 de¿nição 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 de os Estados não exercerem a soberania no ciberespaço, os mesmos podem exercer sua jurisdição sobre os cibercrimes e operações cibernéticas nos termos das normas internacionais, o que será explanado a seguir.

O manual de¿ne, ainda, como a autoridade do Estado tem jurisdição para editar normas, fazer com que estas sejam cumpridas e julgar os casos concretos de violação, tendo como base para este exercício a presença física de uma pessoa ou coisa em seu território. Ademais, podem-se alcançar até mesmo as entidades privadas que estão estabelecidas dentro do território, mas que 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 di¿culdade de determinação da jurisdição do ciberespaço, em função da interconectividade do sistema e de operarem em nuvens e redes baseadas fora das fronteiras, a pessoa e a infraestrutura estão ¿sicamente em algum lugar e, assim, sujeitas à jurisdição do Estado. Com a natureza territorial, a jurisdição deriva em dois outros tipos: subjetiva e objetiva.

A natureza subjetiva abarca a aplicação da lei do Estado exercendo jurisdição sobre atos praticados a partir de seu território e ¿nalizados em qualquer outro local fora do Estado de origem. Já a natureza objetiva concede jurisdição sobre indivíduos no local 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 de as operações de guerra cibernética, em geral, produzirem efeitos em um Estado-alvo, a quem cabe e interessa a responsabilização dos autores da ação. As hipóteses 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, visto que há circunstâncias que a afastam, como, por exemplo, a imunidade diplomática.

Ponto que desperta interesse é a situação dos navios, que será abarcada no próximo capítulo.

Ainda sobre a infraestrutura cibernética, como previsto no art. 5º, o Estado não pode permitir, conscientemente, que ela seja usada para ataques cibernéticos em outros Estados, seja esta localizada em seu território ou sob o controle estatal, com o intuito de prevenir de que a mesma seja empregada para infligir danos a pessoas ou a qualquer patrimônio situado fora de seu território. Para tal, o grupo de especialistas pautou-se em dois precedentes da Corte Internacional de Justiça.[15]

No próprio Manual de Tallinn, resta registrado que ele não é um documento oficial, mas sim o resultado de uma produção intelectual

Nesse mesmo viés, o manual prevê, ainda, que o Estado que permitir que sua infraestrutura cibernética, em seu território, seja utilizada por grupo terrorista para materializar ataque contra outro Estado e, mesmo notificado, falhar na interrupção, infringe o artigo retrocitado. Ademais, esse artigo 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 falhar 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 Internacional, inclusive com fulcro no artigo 51 da Carta das Nações Unidas. Assim, um ilícito internacional pode gerar uma crise internacional com consequências graves, desde sanções até o uso da força em legítima defesa.

No campo da guerra cibernética, foi visto que esse novo domínio adentra o complexo sistema de regramento internacional, sujeitando-se, por conseguinte, às normas do 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, de 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.

15 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.

ESTADOS VERSUS GUERRA CIBERNÉTICA

Uma nova realidade se apresenta com a utilização do ciberespaço e, como consequências diretas, o cometimento de ilícitos e a guerra cibernética, que traz a presença dos Estados para este campo, ¿gurando estes como atores no campo virtual e buscando preparar-se para o enfrentamento às ameaças nesse novo domínio que desa¿a o poder soberano dos entes estatais.

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 ¿guram com atores estatais e soberanos. Com isso, esta análise de soberania passa pelas ações de guerra cibernética violando o ciberespaço, que não tem limitações físicas, conforme já visto anteriormente, em suas características.

> 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 está imune à soberania dos Estados

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 à interdependência e à cooperação entre os sujeitos de Direito Internacional (QUINTÃO SOARES, 2008).

Modernamente, existem quatro conceitos de soberania em uso no DIP. Iniciemos 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 a soberania jurídica internacional, que tem como propósito estabelecer e manter o Estado como uma entidade política independente no sistema internacional. E, por último, há a noção de soberania de interdependência, que se refere à 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 ¿nalidade 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 às 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 está imune à soberania dos Estados.

Entretanto, como já exposto supra, os atores – pessoas físicas – e as infraestruturas cibernéticas estão sujeitas à

jurisdição e à soberania do Estado pelo fato de estarem ¿ sicamente sob o guarda-chuva estatal. Assim sendo, a soberania no ciberespaço faz-se presente em função de o Estado necessitar tipi¿ car 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 de seus cidadãos e suas empresas, de forma a dar segurança jurídica às relações entre as pessoas em sentido lato, a ¿ m de assegurar, principalmente, o conteúdo das informações (KRASNER, 1999).

Diante do 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 e¿ caz que deve ser aplicado ao ciberespaço, necessitando somente de uma nova interpretação do ordenamento internacional em vigor.

O princípio da soberania aplica-se ao ciberespaço, e, consequentemente, à guerra cibernética. O componente territorial é um princípio e¿ caz que deve ser aplicado ao ciberespaço

A ciberguerra no mar

Ciberguerra no mar? Parece distante, mas não há que se pensar desta forma, porque os navios possuem sistemas complexos a bordo, que podem ser infectados por dispositivos móveis.[16 e 17]

Inicialmente, faz-se mister registrar que a Lei do Mar esclarece que o alto-mar abrange todas as partes do mar não incluídas na zona econômica exclusiva, no mar territorial ou nas águas interiores de um Estado, nem nas águas arquipélagicas de um Estado-arquipélago. Logo, já se percebe uma pequena oposição conceitual sobre o alto-mar em relação ao Manual de Tallinn, que de¿ ne 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.

Trazendo a jurisdição para âmbito marítimo, veri¿ ca-se que em alto-mar não há soberania nos termos do art. 89 da CNUDM III, ao passo que em águas interiores e no 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). Acrescenta-se, ainda, a liberdade de navegação[18], a sua utilização para ¿ ns pací¿ cos[19], logo já há um "repúdio" a qualquer tipo de ato hostil nessa área.

Destaca-se o artigo 94 da CNUDM III, que assevera os deveres do Estado, entre eles o de exercer de modo efetivo a sua jurisdição e seu controle em questões administrativas, técnicas e sociais sobre navios que arvorem a sua bandeira, e es-

16 Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/wikileaks-cia-tem-software-para-extrair-dados-de-pcs-desconectados.html. Acesso em: 01 dez. 2017.

17 Disponível em: https://www.humansatsea.com/2017/06/29/prevent-spread-petya-virus-vizag-port-handle-maersk-line-vessels-manually/. Acesso em: 01 dez. 2017.

18 CNUDM, arts. 87 e 90.

19 CNUDM III, art. 88.

pecialmente sua jurisdição conforme o seu direito interno sobre todo navio que árvore a sua bandeira. Ainda neste artigo, nota-se o dever de ordenar a abertura de um inquérito em relação a qualquer acidente marítimo ou incidente de navegação no alto-mar que envolva um navio arvorando a sua bandeira e no qual tenham perdido a vida ou sofrido ferimentos graves nacionais de outro Estado ou se tenham provocado danos graves a navios ou a instalações de outro Estado. Assim, percebe-se que o artigo abarca as situações da ciberguerra.

Há que se registrar, pela CNUDM, a imunidade completa dos navios de guerra relativamente a qualquer outro Estado e dos seus navios ou por ele operados e utilizados unicamente em serviço o¿cial não comercial[20]. Já o manual (art. 4º) destaca que, independentemente do local, os navios de Estado gozam de imunidade, porém, especi¿camente sobre a infraestrutura cibernética, esta somente gozará dessa imunidade se servir exclusivamente aos propósitos estatais, ressaltando que essa imunidade engloba a inviolabilidade e qualquer interferência e ¿nalizando que qualquer transgressão é violação de normas internacionais.

Nesses navios ou plataformas, a infraestrutura cibernética estará a bordo dos mesmos e, em muitos casos, esta infraestrutura comandará importantes sistemas a bordo, como o controle da propulsão, navegação e posicionamento e outros. No caso das plataformas, o Estado de Registro também concorre na jurisdição. De qualquer forma, temos um Estado que possui jurisdição sobre a infraestrutura cibernética.

Apesar das divergências ou concordâncias entre a CNUDM III e o manual, é vital não esquecer que o manual é só um estudo e não tem valor normativo, totalmente diferente da Lei do Mar.

Por ¿m, o tema reveste-se de tamanha relevância que especialistas já consideram que os países retrocedam na história e desenvolvam sistemas de backup com raízes na tecnologia de rádio da Segunda Guerra Mundial.[21]

CONSIDERAÇÕES FINAIS

A ciberguerra, ou guerra cibernética, é o mais novo domínio da guerra, sendo necessário entender seu conceito em termos gerais. Para entender a ciberguerra, investigou-se seus princípios, o ambiente em que opera e seus con□itos, destacando-se o ciberespaço, que se con¿gura como um espaço altamente atrativo para atividades ilícitas, sendo fonte potencial de con□itos nesse novo domínio, por seu caráter transnacional e facilidade de ocultação, assim como os respectivos ataques que se con¿guram como o fator gerador de con□itos e são divididos 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, chegando ao ordenamento vigente, que busca vencer o desa¿o de regular esse

20 CNUDM III, arts. 95 e 95.

21 Disponível em: http://defesaeseguranca.com.br/ameacas-ciberneticas-incentivam-volta-de-tecnologia-de-radio-da-segunda-guerra/. Acesso em: 01 dez. 2017.

espaço sem utilizar censura e monitoramento e, assim, adaptar ou trazer à 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 identi¿cação 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 di¿culdade na obtenção de provas.

Além dessa multilateralidade, veri¿cou-se que há legislação em vigor e que a mesma já atende, sendo exemplo a Carta da ONU, porém é necessária 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 de¿nições 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 os princípios da guerra cibernética di¿cultam o processo de evolução normativa/interpretativa da Carta, particularmente quanto aos conceitos de uso da força, legítima defesa, necessidade e proporcionalidade, identi¿cação da autoria e hostilidade, que precisam ser harmonizados com a Carta em vigor.

Já o Manual de Tallinn con¿gurou-se como um processo de produção de um manual sobre o direito aplicável à ciberguerra, buscando uma conexão do DIP ao jus ad bellum e ao jus in bello com enfoque na guerra cibernética, ou seja, estritamente nas operações cibernéticas contra alvos cibernéticos para con¿itos internacionais, 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 imputadas aos Estados as 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, exerça sua jurisdição, que pode ser objetiva ou subjetiva.

Veri¿cou-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 como plataformas móveis e sua relação interconectada com o Direito do Mar, revelando que a CNUDM III está conectada com o ambiente virtual.

Isto posto, passou ao estudo da relação entre os Estados no campo da guerra cibernética para ¿ns de soberania, ¿cando revelado que não há que se falar em relativização da mesma, mostrando-se absoluta e interativa de forma a combater os cibercrimes e evitar uma guerra cibernética.

Trazendo a ciberguerra para o ambiente marítimo, a particularidade extraterritorial dos navios, foram veri¿cados pontos em

comum entre a CNUDM III e o Manual de Tallinn, assim como os divergentes, mas ressaltando a soberania do país de bandeira e sua responsabilidade e seu dever com a utilização da infraestrutura cibernética a bordo, inclusive para fazer jus à imunidade, e principalmente no alto-mar que deve ser utilizado para ¿ns pací¿cos e sem soberania de nenhum Estado.

Concluindo, entende-se que a guerra cibernética tem suas peculiaridades, destacando-se a transnacionalidade e a ocultação, e não olvidando as iniciativas da comunidade internacional sobre a questão da extraterritorialidade, principalmente no que tange aos navios, e possíveis consequências, veri¿cando que não há relativização da soberania dos Estados diante do 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. Ademais, há que se construir um conceito com aceitação global para a GC e ECiber, de forma a facilitar a interpretação jurídica das normas e evitar que o mar vire um fator gerador de con□itos, em função da importância para a economia global que □ui pelos sete mares.

1 CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:
<GUERRAS>; Guerra cibernética; Direito Internacional; Direito do Mar; Soberania; Poder Nacional;

REFERÊNCIAS BIBLIOGRÁFICAS

ALEXANDER, Keith B. War¿ghting 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.

BARROS, Renata Furtado de. Guerra Cibernética: os novos desa¿os do Direito Internacional. Belo Horizonte: Editora D'Plácido, 2015.

BRASIL. Ministério da Defesa. MD35-G-01: glossário das Forças Armadas. 4ª 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. Desa¿os estratégicos para segurança e defesa cibernética. Org. Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes e Whitney Lacerda de Freitas. Brasília: 2011. 216 p.

CAPEZ, Fernando. Curso de Direito Penal, volume 1: parte geral. 10ª 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.

DIPERT, Randall R. "Other-than-internet (OTI) cyberwarfare: challenges for ethics, law and policy". Journal of Military Ethics, NY, v. 12, nº 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 desa¿os 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.

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

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. 3ª ed. rev., atual e ampl. São Paulo: Editora Revista dos Tribunais, 2008.

OLIVEIRA, Luis Henrique Almeida de. Cyberwar: novas fronteiras da guerra. 2011. 69 f. Monogra¿a (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.

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.

PONCE, Guerric. "La nouvelle cyberguerre mondiale". Le Point, nº 2.316, 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.

SALDAN, Eliane. Os desa¿os 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, nº 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, nº 1, 2014. Rio de Janeiro.

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

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 nº 12.965/2014. Tomo II, 1ª ed., p. 619-640. São Paulo: Quartier Latin, 2015. 686 p.

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

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: Desa¿os estratégicos para segurança e defesa cibernética. Org. Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes e Whitney Lacerda de Freitas. Brasília: 2011. 216 p.