UNIVERSIDADE FEDERAL DA BAHIA

FACULDADE DE DIREITO

CURSO DE GRADUAÇÃO EM DIREITO

FILIPE GOMES DIAS COSTA

OS DESAFIOS DO DIREITO INTERNACIONAL NO CIBERESPAÇO:

A INEFICÁCIA DO SISTEMA DE RESPONSABILIZAÇÃO INTERNACIONAL DOS ESTADOS E DOS NÍVEIS PROBATÓRIOS DAS CORTES INTERNACIONAIS

Salvador

2017

FILIPE GOMES DIAS COSTA

OS DESAFIOS DO DIREITO INTERNACIONAL NO CIBERESPAÇO:

A INEFICÁCIA DO SISTEMA DE RESPONSABILIZAÇÃO INTERNACIONAL DOS ESTADOS E DOS NÍVEIS PROBATÓRIOS DAS CORTES INTERNACIONAIS

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito, Faculdade de Direito da Universidade Federal da Bahia.

Orientação: Prof. Ms. André Luiz Batista Neves

Salvador

2017

FILIPE GOMES DIAS COSTA

OS DESAFIOS DO DIREITO INTERNACIONAL NO CIBERESPAÇO:

A INEFICÁCIA DO SISTEMA DE RESPONSABILIZAÇÃO INTERNACIONAL DOS ESTADOS E DOS NÍVEIS PROBATÓRIOS DAS CORTES INTERNACIONAIS

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito, Faculdade de Direito da Universidade Federal da Bahia.

Orientação: Prof. Ms. André Luiz Batista Neves

Aprovada em _____ de _____ de 2017.

BANCA EXAMINADORA:

André Luiz Batista Neves – Orientador _____

Mestre em Direito Público pela Universidade Federal da Bahia (UFBA).
Universidade Federal da Bahia

João Glicério de Oliveira Filho – Examinador _____

Doutor em Direito Público pela Universidade Federal da Bahia (UFBA).
Universidade Federal da Bahia

Paulo Augusto de Oliveira – Examinador _____

Mestre em Direito Público pela Universidade de Coimbra.
Faculdade Baiana de Direito e Gestão

AGRADECIMENTOS

Agradeço aos meus pais, Ebenezer e Marisilvia, por todo o apoio e amor ao longo destes 22 anos de jornada. Sou eternamente grato por todo o esforço, carinho e ensinamentos que me foram dados. Esses são os principais pilares que me sustentam enquanto pessoa e que um dia passarei para os meus filhos.

Agradeço ao meu orientador, Professor Mestre André Luiz Batista Neves, por ter aceitado o desafio de me orientar, e pela diligência, atenção e precisão de suas observações. Foi um privilégio ser orientado por um dos professores que mais admiro e que marcou minha vida acadêmica com seu comprometimento e lendário conhecimento.

Ao Professor Doutor João Glicério de Oliveira Filho, por todos os desafios e aventuras partilhadas nesses anos de faculdade. Sou imensamente grato pelas experiências que me foram proporcionadas e que moldaram o meu caráter. Obrigado por compreender todas as nuances do que verdadeiramente significa ser um professor e, também, um concretizador de sonhos.

Ao Professor Mestre Paulo Augusto de Oliveira, por todas as oportunidades e parcerias. Agradeço pelo acompanhamento e pelo estímulo na pesquisa e estudo do direito internacional, o que mudou para sempre a minha vida. Obrigado por todo o reconhecimento ao longo dos anos e por proporcionar o meu desenvolvimento enquanto pessoa e estudioso do direito internacional.

Agradeço também aos meus amigos do AVL – Aquele Velho Lápis que amplificaram e perenizaram a minha paixão por computadores e pelo espaço cibernético através de uma amizade sem precedentes.

Por fim, obrigado a todos os meus amigos da Faculdade de Direito da UFBA e do NCI – Núcleo de Competições Internacionais que me proporcionaram os melhores anos da minha vida. Em especial, agradeço a Thais Adileu, minha amada namorada e companheira de todos os momentos, Verônica Hassler Benn, minha eterna parceira e amiga-irmã, Bruno Guimarães, meu amigo inseparável, e Thaís Penalber, minha querida mentora.

“I am not an advocate for frequent changes in laws and Constitutions. But laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths discovered and manners and opinions change, with the change of circumstances, institutions must advance also to keep pace with the times.”

Thomas Jefferson

“The only thing that makes something non-hackable is one’s lack of interest to hack it.”

Ditado anônimo da comunidade hacker

COSTA, Filipe Gomes Dias. **Os desafios do direito internacional no ciberespaço: a ineficácia do sistema de responsabilização internacional dos Estados e dos níveis probatórios das cortes internacionais.** 79 fls. Monografia (Graduação) – Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2017.

RESUMO

Esta monografia procura discutir os diferentes aspectos normativos, desafios e dificuldades que as teorias tradicionais do direito internacional enfrentam quando lidam com a atribuição de responsabilidade no mundo cibernético. Em primeiro lugar, será explicado como o espaço cibernético é visto do ponto de vista do direito internacional, dando-se enfoque principal no *Tallinn Manual* e os incidentes e discussões que o antecederam. Em seguida será feita uma análise crítica visando demonstrar a ineficácia do sistema de responsabilização internacionais dos Estados por meio do estudo dos elementos constitutivos do ato internacionalmente ilícito, depurando os testes de controle e as principais hipóteses de descumprimento de obrigações internacionais no ciberespaço. Após, estudar-se-á a aplicação do direito processual pelas cortes internacionais, concedendo tratamento especial à valoração da prova realizada por esses tribunais e os diversos níveis probatórios exigidos pelas cortes para fins de atribuição de atos internacionalmente ilícitos e sua incompatibilidade com as peculiaridades do espaço cibernético. Finalmente, serão analisados possíveis mecanismos capazes de solucionar a atual situação de impunidade oriunda da inadequação das normas tradicionais de responsabilização para atos cometidos no espaço cibernético. Para tanto, serão foco principal do estudo a ampliação do escopo do principio do dever de devido cuidado e a mitigação do nível de prova tradicionalmente exigido pelas cortes internacionais, tudo com o objetivo de adaptar o direito internacional à dinâmica do espaço cibernético.

Palavras-Chave: Ciberespaço*;* Responsabilidade Internacional dos Estados; Devido Cuidado; Valoração Probatória.

COSTA, Filipe Gomes Dias. **The challenges of international law in the cyberspace: the ineffectiveness of the state responsibility system and the standard of proof of international courts.** 79 pg. Monograph (Bachelor) – Law Faculty, Universidade Federal da Bahia, Salvador, 2017.

ABSTRACT

This monograph proposes a discussion about the different normative aspects, challenges and hardships that the traditional theories face when addressing the matters regarding state responsibility in the cyberspace. Firstly, it will be explained in which manner the cyberspace is viewed from the international law perspective, focusing on the Tallinn Manual and the incidents and discussions that took part prior to its conception. Following this, it will be analyzed whether the system of state responsibility is ineffective regarding the cyberspace through the study of its constitutive elements, in which the control tests and the main violations of international law in the cyberspace will be highlighted. Then, the application of procedural norms in the international courts will be evaluated, endowing special treatment to the standard of proof usually required for the attribution of internationally wrongful acts and its incompatibility with the particularities of the cyberspace. Lastly, viable solutions to solve the present impunity originated from the defiency of the classical state responsibility norms in the cyberspace will be proposed. Therefore, in order to better adapt the international law to the new dynamics of the cyberspace, the main proposals will be the extension of the protective scope of the due diligence principle and the mitigation of the standard of proof usually required by international courts.

Keywords: Cyberspace, State Responsibility, Due Diligence, Standard of Proof

ROL DE ABREVIATURAS E SIGLAS

Art.	Artigo
CDI	Comissão de Direito Internacional
CVDT	Convenção de Viena sobre o Direito dos Tratados
CPJI	Corte Permanente de Justiça Internacional
DDoS	Ataque de Negação de Serviço
NATO CCD COE	Centro de Excelência da OTAN para Cooperação em Defesa Cibernética
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
Projeto de Artigos	Projeto de Artigos sobre Responsabilidade do Estado por Atos Internacionalmente Ilícitos
TPI	Tribunal Penal Internacional
TPIAI	Tribunal Penal Internacional para a Antiga Iugoslávia
Tor	*The Onion Router*

SUMÁRIO

1 INTRODUÇÃO

O advento do ciberespaço pode facilmente ser considerado uma das maiores conquistas tecnológicas do ser humano. Por meio dessa invenção existente apenas nas mentes mais férteis escritores de ficção científica, uma verdadeira revolução em todas as nuances da vida em sociedade foi promovida, seja pela instantaneidade da informação, pela consolidação da globalização ou pela verdadeira mudança na natureza das relações sociais. Em verdade, o que se observa é a verdadeira transformação de todas as relações humanas existentes e o surgimento de outras novas formas de interação social.

Inevitavelmente, o ciberespaço não gerou apenas avanços positivos. Como consequência do sentimento de anonimato e da dificuldade técnica de rastreamento, somado ainda às brechas existentes em um sistema de normas que ainda está se desenvolvendo, o ciberespaço oportunizou novas modalidades de condutas censuráveis em diversos graus das relações humanas.

Não obstante, o sentimento latente de impunidade que ainda permeia os atos cometidos através do espaço cibernético denota que as normas jurídicas não se encontram suficientemente adaptadas para lidar com essa nova invenção social. Nesse sentido, o Direito, enquanto ciência do espírito, não se encontra imune às drásticas mudanças ensejadas pelo ciberespaço, apesar de oferecer fortes resistências para se adequar a essa nova era da humanidade, honrando os dizeres de que a ciência jurídica é o último vagão do trem das mudanças sociais.

Inserido nesse contexto, uma das principais peculiaridades do ciberespaço que vem desafiando a mentalidade dos juristas contemporâneos é o desdenho que essas novas tecnologias tem por qualquer tipo de fronteira estatal ou limitações territoriais de ordenamentos jurídicos internos.

No mais das vezes, uma relação travada no ciberespaço se inicia em um computador pessoal localizado em determinado Estado, que se utilizará de cabos submarinos dispostos no mar territorial de um outro Estado, para acessar um servidor disposto em um terceiro Estado. Ainda nessa linha, pode-se facilmente pensar em um ataque cibernético ativado por um usuário em um determinado Estado, mas conduzido por inúmeros computadores-zumbis infectados com um vírus *botnet* localizados em vários Estados para atingir um servidor localizado em um terceiro Estado.

Esse cenário transfronteiriço resulta no incremento da importância do Direito Internacional como um dos poucos mecanismos que podem ser eficazes em regular as atividades dos Estados no ciberespaço.

Entretanto, o atual cenário normativo internacional denota uma situação de impunidade no que se refere aos atos ilícitos praticados pelo ciberespaço devido à atual configuração restritiva da aplicação de normas internacionais acerca da responsabilidade internacional dos Estados por atos internacionalmente ilícitos e à abordagem utilizada pelas cortes internacionais no que se refere ao direito probatório.

Inserido nesse contexto, o presente trabalho tem como objetivo demonstrar que a atual abordagem das normas internacionais é insuficiente para lidar com as peculiaridades inerentes do ciberespaço. Almejando contribuir para a remediação desse cenário, defende-se uma flexibilização do atual sistema de responsabilização internacional dos Estados através da ampliação do escopo da obrigação de devido cuidado no que se refere ao uso da ciberestrutura estatal e da mitigação do nível probatório exigido pelas cortes internacionais para a responsabilização de um Estado por um ato internacionalmente ilícito. Para isso, a pesquisa foi dividida em capítulos que abordam diferentes elementos acerca do assunto.

No Capítulo 2 desta monografia, é feita uma breve exposição sobre o desenvolvimento do ciberespaço dentro do Direito Internacional através da leitura de três emblemáticos incidentes e, em especial, sobre os debates acerca de sua possível concepção como domínio público internacional e dos avanços doutrinários do *Tallinn Manual*.

Em seguida, o Capítulo 3 busca demonstrar de que forma o sistema de responsabilidade internacional dos Estados seria aplicado a atos cometidos através do ciberespaço. Para tanto, será realizada uma análise dos elementos constitutivos do ato internacionalmente ilícito, na qual tanto a atribuição do ato ilícito a um Estado quanto os testes de controle serão objeto de depuração no que se refere às hipóteses de não cumprimento de uma obrigação internacional no contexto cibernético.

O Capítulo 4, por sua vez, trata do direito probatório utilizado pelas cortes internacionais como forma de identificar de que forma os elementos de prova colhidos no ciberespaço serão valorados em um processo judicial de responsabilização internacional de um possível Estado transgressor.

Por fim, o Capítulo 5 apresenta as diferentes formas capazes de evitar o cenário de impunidade existente por meio de uma adequação dos elementos do sistema de responsabilização internacional ora analisados por meio da ampliação do escopo do dever de devido cuidado e da mitigação do nível probatório tradicionalmente exigido pelas cortes internacionais.

2 O DIREITO INTERNACIONAL E O ESPAÇO CIBERNÉTICO

2.1 CONTEXTO ATUAL

Contemporaneamente, o mundo cibernético tem sido visto pela comunidade internacional como uma grande área cinzenta em que o direito como se conhece não seria plenamente aplicável. Nesse sentido, os principais Estados do mundo têm começado a dedicar recursos e atenção ao espaço cibernético, sobretudo no que diz respeito à defesa e ataques cibernéticos.[1] Similarmente, a discussão sobre o espaço cibernético tem chamado a atenção dos principais doutrinadores do direito internacional e também das organizações internacionais, criando-se nesta década, por exemplo, o *Tallinn Manual* e a NATO CCD COE ou Centro de Excelência da OTAN para Cooperação em Defesa Cibernética.

Esse movimento de aumento de importância das discussões sobre o espaço cibernético é mais bem compreendido mediante a análise de três impactantes casos de ataques cibernéticos que aconteceram nos últimos anos em diferentes países. Conjuntamente, esses incidentes foram os principais responsáveis por inflamar o debate sobre a importância de se rever as normas de direito internacional aplicáveis a esse contexto.

i) Estônia, 2007. Por volta de 27 de Abril de 2007, uma série de sites de organizações estonianas, como o parlamento, bancos, ministérios e grupos de mídia, foram atacados e derrubados por ataques cibernéticos, resultando em uma situação denominada de *blackout* virtual.[2] Acredita-se que esse ataque se utilizou da técnica de DDoS[3], em conjunto com uma rede *botnet*[4], para sobrecarregar os servidores em que esses sites estavam hospedados, forçando-os a se auto desligarem. Esse incidente foi conduzido durante um impasse diplomático entre a Estônia e a Rússia sobre a retirada de um memorial de soldados da antiga URSS,

---

[1] Por exemplo, em 2005 os Estados Unidos alterou a missão da sua força área para "*The mission of the United States Air Force is to fly, fight and win in air, space and cyberspace."*

[2] TRAYNOR, Ian. Russia accused of unleashing cyberwar to disable Estonia. **The Guardian**, [S.l.], 17 mai. 2007. Disponível em: <https://www.theguardian.com/world/2007/may/17/topstories3.russia>. Acesso em: 03 ago. 2017.

[3] Ataque cibernético que visa sobrecarregar determinado servidor através do estabelecimento simultâneo de diversas interações com esse servidor, forçando-o a se desligar devido à exaustão de sua memoria RAM ou processador.

[4] Sistema de computadores interligados, muitas vezes sem o conhecimento do usuário, capazes de serem controlados remotamente por um computador principal, com o fim de executar, conjuntamente, determinado comando.

localizado no centro da cidade de Tallinn, na Estônia, que era visto pelo povo estoniano como uma lembrança de um passado que se buscava, agora, ser esquecido. Essa inciativa, em conjunto com a sua entrada na OTAN, marcou um dos principais movimentos estonianos de rebelião contra a CEI, a Comunidade de Estados Independentes, pseudo bloco regional defendido e comandado pela Rússia como forma de perenizar sua influência sobre as ex-repúblicas soviéticas. Indubitavelmente, a Estônia logo acusou a Rússia de comandar os ataques cibernéticos, que, por sua vez, negou, *a priori,* qualquer envolvimento.

No entanto, em março de 2009, para a surpresa da comunidade internacional, em um painel russo-americano sobre o ciberespaço, o deputado Sergei Markov, pró-Kremlin e atual membro do Conselho Nacional de Estratégia da Rússia sob o comando de Vladimir Putin, ao atender uma pergunta sobre os incidentes na Estônia respondeu inesperadamente dizendo:

> About the cyberattack on Estonia... don't worry, that attack was carried out by my assistant. I won't tell you his name, because then he might not be able to get visas.[5]

Aproveitando o atordoamento dos presentes, Markov emendou ressaltando que esse seu "assistente" decidiu autonomamente que "algo deveria ser feito contra esses fascistas estonianos",[6] atitude que classificou como uma reação normal e esperada da sociedade civil diante dos atos do governo da Estônia.[7]

Apesar dessa manifestação do deputado Markov, especialistas de tecnologia asseveraram, à época, que o ataque em questão dificilmente poderia ser conduzido por um lobo solitário, visto que as operações afetaram servidores e sistemas críticos que, normalmente, não estão expostas para a rede mundial de computadores, exigindo um acesso especial ou, então, a ajuda técnica de um Estado para afetá-

[5] "Sobre o ataque cibernético na Estônia... não se preocupe, aquele ataque foi conduzido por meu assistente. Não lhe direi o nome, entretanto, pois ele poderá não conseguir mais vistos." (Tradução livre).
[6] COALSON, Robert. Behind the Estonia Cyberattacks. **Radio Free Europe/Radio Liberty**, [S.l.], 06 mar. 2009.Disponível em: <https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html>. Acesso em: 03 ago. 2017.
[7] ASADOVA, Nargiz. Нам, русским за границей, иностранцы ни к чему. **Echo of Moscow**, [S.l.], 05 mar. 2009. Disponível em: <http://echo.msk.ru/blog/n_asadova/576689-echo/>. Acesso em: 03 ago. 2017.

las.[8] Corroborando esse entendimento, o *hacker* russo Sp0Raw anotou que o ataque contra a Estônia dificilmente poderia ter ocorrido sem "recomendações" russas, ao mesmo tempo em que descaracterizou a tentativa da Estônia de atribuir os atos diretamente à Rússia por falta de provas concretas.[9]

Esse ataque cibernético mudou para sempre cidade de Tallinn, vez que nela foi estabelecido o Centro de Excelência da OTAN para Cooperação em Defesa Cibernética, responsável pela criação do *Tallinn Manual,* marco zero da codificação internacionalista sobre o espaço cibernético, consolidando sua transformação na capital mundial para assuntos relacionados ao ciberespaço.

ii) Geórgia, 2008. Em meio à escalada da guerra da Ossétia do Sul,[10] houve a deflagração de uma série de ataques cibernéticos ao território georgiano, que afetaram desde sites governamentais[11] até o Oleoduto Baku-Tbilisi-Ceyphan,[12] além de um completo *blackout* virtual em agosto por meio de DDoS, aos moldes do ataque ocorrido na Estônia.[13]

O governo russo negou quaisquer acusações ligando-o ao ataque cibernético,[14] indicando como verdadeiro responsável uma gangue de criminosos cibernéticos denominados RBN – *Russian Business Network*,[15] considerada como

---

[8] NEWLY Nasty. **The Economist**, [S.l.], 24 mai. 2007. Disponível em: <https://www.economist.com/node/9228757>. Acesso em: 03 ago. 2017.

[9] VERHULST, Stefaan. Estonian plan for 'data embassies' overseas to back up government databases. **New York University GovLab**, New York, 02 jun. 2012. Disponível em: <http://thegovlab.org/estonian-plan-for-data-embassies-overseas-to-back-up-government-databases>. Acesso em: 03 ago. 2017.

[10] Conflito armado em que a Rússia e a Geórgia se enfrentaram militarmente em resposta a um movimento separatista da região da Ossétia do Sul, território da Geórgia, que possuía apoio russo,

[11] DANCHEV, Dancho. Georgia President's web site under DDoS attack from Russian hackers. **Zero Day**, [S.l.], 22 jul. 2008. Disponível em: <http://www.zdnet.com/article/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers>. Acesso em: 03 ago. 2017; ROHAN, Brian; PEARCE, Tim. Georgia says Russian hackers block govt websites. **Reuters**, [S.l.], 11 ago. 2011. Disponível em: <http://uk.reuters.com/article/us-georgia-ossetia-hackers-idUKLB2050320080811>. Acesso em: 03 ago. 2017.

[12] ROBERTSON, Jordan; RILEY, Michael. Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar. **Bloomberg**, [S.l.], 10 dez. 2014. Disponível em: <https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>. Acesso em: 03 ago. 2017.

[13] KEIZER, Gregg. Cyberattacks knock out Georgia's Internet presence. **Computer World**, [S.l.], 11 ago. 2008. Disponível em: <http://www.computerworld.com/article/2532289/cybercrime-hacking/cyberattacks-knock-out-georgia-s-internet-presence.html>. Acesso em: 03 ago. 2017.

[14] ROHAN, Brian; PEARCE, Tim. Georgia says Russian hackers block govt websites. **Reuters**, [S.l.], 11 ago. 2011. Disponível em: <http://uk.reuters.com/article/us-georgia-ossetia-hackers-idUKLB2050320080811>. Acesso em: 03 ago. 2017.

[15] RBN – Georgia CyberWarfare – 2 – Sat 16 00 East Coast, 20 00 GMT. **RBNExploit**, [S.l.], ago. 2008. Disponível em: <http://rbnexploit.blogspot.com.br/2008/08/rbn-georgia-cyberwarfare-2-sat-16-00.html>. Acesso em: 03 ago. 2017.

um dos principais grupos mundiais ligados à disseminação de *malwares,* pornografia infantil, roubo de dados e outros crimes cibernéticos.[16]

Entretanto, ainda em 2008, um grupo composto por mais de 100 especialistas de informática oriundos de empresas como a Microsoft e a Oracle, além de ex-integrantes de agências de inteligência se formou com o intuito de analisar os elementos técnicos do ataque com vistas a identificar se haveriam provas do envolvimento da Rússia nesse ataque.[17] A essa iniciativa deu-se o codinome *Project Grey Goose*.

O *Project Grey Goose* consiste no primeiro trabalho independente com um viés técnico acerca da possibilidade de atribuir determinado ataque cibernético a um Estado,[18] possuindo, assim, grande relevância para a discussão da comunidade internacional sobre o tema. Sua atividade principal foi a de analisar os dados colhidos de dois fóruns de *hacker*s russos, o www.xakep.ru e o www.stopgeorgia.ru além das informações de registro (*log files)* dos sites georgianos alvos dos ataques.[19]

Em que pese o relatório do *Project Grey Goose* não tenha apontado nenhuma prova clara e convincente do envolvimento russo nos ataques, houve uma extensa demonstração de provas circunstanciais que, em conjunto, indicariam a coordenação russa como um dos fatores primordiais para a condução e sucesso dos ataques, que, aparentemente, se originaram de grupos civis.[20] Nesse sentido, similarmente aos incidentes na Estônia, haveria aqui a participação do Estado russo no sentido de incitar equipar e direcionar as ações de indivíduos[21] contra outro

---

[16] ESPINER, Tom. Georgia accuses Russia of coordinated cyberattack. **CNET**, [S.l.], 11 ago. 2008. Disponível em: <https://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/>. Acesso em: 03 ago. 2017.

[17] KREBS, Brian. Report: Russian Hacker Forums Fueled Georgia Cyber Attacks. **The Washington Post**, [S.l.], 16 out. 2008. Disponível em: <http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html>. Acesso em: 03 ago. 2017.

[18] CZOSSECK, Christian. State Actors and their Proxies in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013, p. 21. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017.

[19] PROJECT GREY GOOSE. **Project Grey Goose: Phase I Report**, [S.l.] 17 out 2008, Disponível em: <https://pt.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>. Acesso em: 04 ago. 2017.

[20] CZOSSECK, Christian. State Actors and their Proxies in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013, p. 21. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017.

[21] Particularmente interessante, o site StopGeorgia fornecia um software pré-montado e direcionado para servidores da Geórgia para qualquer um que quisesse colaborar nos ataques cibernéticos.

Estado, criando um distanciamento confortável para burlar qualquer tentativa de responsabilização.

iii) Irã, 2010. Em meio à tensão internacional acerca do projeto nuclear iraniano, misteriosamente, a principal usina nuclear do país asiático é altamente danificada devido ao comportamento inesperado de suas centrífugas, que, segundo boatos, soltou-se do seu eixo devido a um aumento brusco na sua velocidade e retalhou grande parte dos sistemas e maquinários da usina de Natanz.[22] Meses após esse incidente, a empresa de tecnologia e defesa cibernética Symantec identifica na rede mundial de computadores um *malware* denominado *Rootkit.TmpHider* ou *W32.Stuxnet*, um vírus altamente sofisticado que possuía em seu código-fonte o comando de ativação apenas quando infectar sistemas de controle industriais específicos desenvolvidos pela empresa *Siemens*, denominados SCADA, e utilizados pelo programa nuclear iraniano.[23] Com base na arquitetura do *Stuxnet,* descobriu-se que seu comando de ação era o de emendar o código dos dispositivos controladores dos sistemas SCADA para manipular a velocidade dos motores ligados ao painel de controle ora infectado.[24] Ademais, devido à complexidade e direcionamento do *Stuxnet*, acredita-se que os Estados Unidos e Israel tenham, conjuntamente, se envolvido na criação do *malware,*[25] apesar de não haverem, de fato, qualquer prova dessas alegações. Nesse supedâneo, Marco Roscini assevera que durante as discussões do *Tallinn Manual,* conclui-se que o S*tuxnet* se classificaria como uso da força, mormente devido à existência de danos cinéticos.[26]

Os efeitos desses três principais incidentes foram sentidos por toda a comunidade internacional, amadurecendo as discussões acerca da necessidade de regulamentar o espaço cibernético sob um viés internacionalista. Todavia, diversos

---

[22] THE Meaning of Stuxnet. **The Economist,** [S.l.], 30 set. 2010. Disponível em: <http://www.economist.com/node/17147862>. Acesso em: 04 ago. 2017.

[23] FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric. W32.Stuxnet Dossier Version 1.4, **Symantec Security Response**. [S.l.] fev 2011, Disponível em: <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>. Acesso em: 04 ago. 2017.

[24] ZIOLKOWSKI, Katharina. **Stuxnet – Legal Considerations**, NATO CCD COE Publications, Tallinn, 2012, p. 3 . Disponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf>. Acesso em: 07 ago. 2017.

[25] US and Israel were behind Stuxnet claims researcher. **BBC**, [S.l.], 04 mar. 2011. Disponível em: <http://www.bbc.com/news/technology-12633240>. Acesso em: 04 ago. 2017.

[26] ROSCINI, Marco. **Cyber Operations and the Use of Force in International Law**, 1 ed. Oxford: Oxford University Press, 2014, pp. 29-33.

desafios se mostram presentes para essa tarefa de normatização que chegam a afetar as próprias bases do direito internacional, como o conceito de domínio público internacional e a abordagem internacionalista sobre o *non-liquet.*

2.2 POSSÍVEL DOMÍNIO PÚBLICO INTERNACIONAL E O *NON-LIQUET*

A doutrina nacional, notadamente pelo trabalho de Hildebrando Accioly, dispõe que a noção de domínio público internacional guarda relação direta com os diferentes tipos de território em que se pode observar o alcance da soberania de determinado Estado.[27]

Tradicionalmente, pode-se identificar como principais domínios passíveis de compor o território de um Estado o terrestre, o fluvial, o marítimo, o lacustre e o aéreo. Não obstante, com o desenvolvimento científico do ser humano, houve a expansão desse rol de domínios, adicionando-se o espaço sideral e as regiões polares, mais marcadamente a Antártida. A esses foi elaborado um conjunto normativo diferenciado, em que a cooperação internacional ditaria a administração cooperativa desses domínios visando o desenvolvimento científico da raça humana, consolidando-se assim, o princípio da herança comum da humanidade.[28]

No entanto, cabe ressaltar que os demais domínios públicos internacionais estão plenamente sujeitos ao fenômeno da territorialidade estatal como produto da soberania. Dessa forma, os domínios públicos tradicionais compõem, por excelência, a parcela do globo terrestre sobre o qual determinado Estado pode fazer valer seu conjunto normativo próprio.[29]

Apesar desse traço similar, os domínios internacionais clássicos possuem normas internacionais próprias, adaptadas às suas particularidades. Por exemplo, as normas costumeiras sobre o Direito do Mar e a Convenção de Montego Bay conceberam um apanhado de restrições à incidência do poder soberano do Estado por meio da criação das faixas do mar territorial, da zona contígua e da zona econômica exclusiva, atribuindo, ainda, ao mar aberto, ou seja, as águas internacionais que não estão se enquadram nas referidas faixas, uma liberalidade à

---

[27] ACCIOLY, Hildebrando; SILVA, G. E. do Nascimento e; CASELLA, Paulo Borba. **Manual de Direito Internacional Público**. 20. ed. São Paulo: Saraiva, 2012. p. 559.
[28] MAZZUOLI, Valério de Oliveira. **Curso de direito internacional público**. 9 ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2015, p. 847
[29] CRAWFORD, James. **Brownlie's Principles of Public International Law**. 8. ed. Oxford University Press, 2012, p. 264

incidência do poder estatal pautado meramente no território.[30] Ainda nessa linha, o domínio aéreo por meio da Convenção de Chicago determina exceções ao poder soberano de um Estado sob seu próprio território ao conceber o instituto da escala técnica e das Nove Liberdades do Ar.[31]

Percebe-se, então, que cada domínio público internacional possui seu próprio conjunto de normas reguladoras condizentes com as suas características, podendo, inclusive disporem de formas diferentes acerca de um mesmo instituto.[32] Nesse contexto, surge, então, a discussão sobre se o espaço cibernético não constituiria um novo domínio público internacional que requer normas próprias, ora incipientes.

Wolff von Heinegg propõe que o espaço cibernético, constituiria, em verdade, mais uma região de *res communis omnium,* tal qual o alto mar e o espaço sideral, ou seja, além do escopo do poder soberano de um Estado, ou grupo de Estados e suas regramentos internos.[33]

Destarte, baseando-se nesse entendimento, é possível encontrar renomados doutrinadores que defendem que o ciberespaço não é, em verdade, regulado por normas jurídicas, visto que inexistiriam normas costumeiras sobre questões cibernéticas e que as normas previstas em tratados sobre as referidas questões são deveras escassas.[34]

Dentro desse escopo, a consequência direta prevista pelo direito internacional clássico seria a constatação de um cenário de *non-liquet,* do qual se aplica a tese principiológica do caso da Corte Permanente de Justiça Internacional sobre o *S.S. Lotus*.

O caso do *S.S. Lotus,* julgado em 1927 pela CPJI, é considerado como um dos principais marcos para o desenvolvimento do direito internacional do século XX.

---

[30] "Artigo 86: Âmbito de aplicação da presente Parte. As disposições da presente Parte aplicam-se a todas as partes do mar não incluídas na zona econômica exclusiva, no mar territorial ou nas águas interiores de um Estado, nem nas águas arquipelágicas de um Estado arquipélago. O presente Artigo não implica limitação alguma das liberdades de que gozam todos os Estados na zona econômica exclusiva de conformidade com o Artigo 58." (Tradução livre).

[31] MAZZUOLI, Valério de Oliveira. **Curso de direito internacional público**. 9 ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2015, p. 843.

[32] Por exemplo, não se admite a aplicação da passagem inocente, noção clássica do direito marítimo, ao espaço aéreo.

[33] VON HEINEGG, Wolff, Heintschel. Legal Implications of Territorial Sovereignty in Cyberspace In: CZOSSECK, Christian; OTTIS, Rain; ZIOLKOWSKI, Katharina. (eds.). **2012 4th International Conference on Cyber Conflict**., NATO CCD COE Publications, Tallinn, 2012.

[34] ZIOLKOWSKI, Katharina. General Principles of International Law as Applicable in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. pp. 147-151 Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017.

Seu litígio, travado entre a França e a Turquia, ocorreu após a colisão de um navio a vapor francês com outro navio de origem turca no alto-mar e o subsequente indiciamento criminal do oficial francês, responsável pelo navio, pelas autoridades turcas, quando o navio francês ingressou no território turco. Nesse caso, a CPJI, ao analisar o ato em questão constatou que o que passa a bordo de um navio, em alto-mar, deve ser considerado como se tivesse ocorrido no território do Estado cuja bandeira o navio usa. Então, se um ato delituoso, cometido num navio, em alto-mar, produz seus efeitos sobre um navio que usa outra bandeira ou sobre um território estrangeiro, devem ser aplicados ao caso os mesmos princípios que se aplicariam se se tratasse de dois territórios de Estados diferentes. Portanto, conclui-se que nenhuma regra de Direito Internacional proíbe o Estado, cuja bandeira o navio arvora e onde os efeitos do delito se manifestaram, de considerar esse delito como se tivesse sido cometido em seu território e, assim, exercer a ação penal contra o delinquente.[35]

Percebe-se, então, a criação de uma abordagem específica do direito internacional sobre o *non-liquet,* determinando que, na hipótese de não haver uma proibição normativa, os Estados gozam de liberdade referente a seus atos.[36]

Essa noção pode ser vislumbrada sob duas diferentes óticas: inicialmente, como um axioma lógico, indispensável para a operacionalização do direito internacional a partir da relação bivalente de permissibilidade e proibição. Dessa forma, inexistindo uma proibição da prática de determinada conduta, conclui-se pela permissibilidade do referido ato. Além disso, pode-se conceber o referido princípio como uma norma material de direito internacional oriunda da soberania dos Estados, que, por sua vez, implica que os Estados estariam livres para agir de acordo com a liberalidade ao menos se houver uma norma internacional ditando expressamente a reprovação da conduta sob análise.[37]

Essa segunda visão é bastante relevante para a análise do atual cenário normativo do espaço cibernético, sobretudo quando confrontado com as teses de

---

[35] PERMANENT COURT OF INTERNATIONAL JUSTICE. **The Case of the S. S. Lotus**. In: Publications of the Permanent Court of International Justice Series A. No. 10, 1927, The Hague, Netherlands.

[36] DEEKS, Ashley. An International Legal Framework for Surveillance. **Virginia Journal of International Law**, Charlottesville, Vol. 55:2, 2015, p. 301.

[37] BODANSKY, Daniel. ***Non Liquet***. Max Planck Encyclopedia of Public International Law, Oxford, 2012.

que o ciberespaço constituiria um novo domínio público internacional incompatível com as regras básicas do direito internacional.

De início, indispensável reconhecer que o cenário do *non-liquet* é altamente indesejável para a comunidade internacional, gerando sérias consequências para as relações internacionais diante de um flagrante cenário de insegurança jurídica.

Visando depurar esse fenômeno no espaço cibernético, Katharina Ziolkowski demonstra que o Direito Internacional contemporâneo compreende a coexistência das liberdades conflitantes dos Estados condicionadas à orientação dos princípios gerais do direito internacional. Destarte, para a autora, a própria existência de princípios gerais do direito, afasta a declaração de um estado de *non-liquet* como subterfúgio estatal para de agir de forma livre e irrestrita.[38]

Tais princípios são fundamentais no contexto cibernético, já que eles formam a base para o progressivo desenvolvimento do direito internacional, habilitando o sistema de normas internacionais para prover as respostas adequadas diante das necessidades dinâmicas da comunidade internacional, especialmente no que se refere à escalada dos avanços tecnológicos e teriam força normativa mesmo se partindo da premissa de que o ciberespaço consistiria um domínio público independente, visto que até mesmo as áreas de *res communis omnium* estão sujeitas aos princípios gerais do direito[39].

Consoante, os princípios gerais do direito internacional compõem a fundação de onde as normas sobre o ciberespaço devem se desenvolver.

Dito isso, se a tese de domínio público independente, de fato prosperasse na doutrina internacionalista, a utilização cada vez mais crescente do ciberespaço como palco para a condução de relações interestatais estaria à mercê de uma instabilidade normativa capaz de comprometer o seu desenvolvimento.

Em verdade, a concepção do ciberespaço como um domínio isolado e independente se mostra contraditório ao se considerar os mecanismos e plataformas a partir dos quais o próprio ciberespaço se estrutura.[40] Conforme já apresentado, o

---

[38] ZIOLKOWSKI, Katharina. General Principles of International Law as Applicable in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. p. 138 Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017.

[39] *ibid*

[40] CZOSSECK, Christian. State Actors and their Proxies in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International**

ciberespaço nada mais é que a reunião de elementos físicos que coletivamente sustentam a nuvem abstrata que denominamos de ciberespaço. Servidores, *backbones* e redes de fibra ótica constituem os pilares que sustentam essa amálgama abstrata, e, indubitavelmente, estão sujeitos às regulação das normas jurídicas. Por se localizarem em um dos domínios públicos internacionais já estabelecidos, mais notadamente o terrestre e subsidiariamente o marítimo por meio dos cabos submarinos.

Dessa forma, não é razoável a compreensão de que o ciberespaço está alheio à incidência das normas do direito internacional, uma vez que mesmo não sendo possível extrair normas costumeiras da prática estatal, os princípios gerais do direito internacional são plenamente aplicáveis a esta área do direito internacional.

Consequentemente, apesar das normas sobre o ciberespaço não estarem ainda consolidadas, este espaço não deve ser tratado como uma espécie de terra sem lei no qual não há sequer a aplicação de normas basilares. Não obstante, este campo do direito internacional deve ser passar urgentemente a se um dos principais focos dos doutrinadores e dos Estados no que se refere ao desenvolvimento do direito internacional, visto que a mera aplicação de princípios básicos pode acarretar equívocos em lidar de forma satisfatória com uma situação mais específica.

2.3 O *TALLINN MANUAL*

Durante os anos de 2009 e 2012, um grupo composto de dezenove especialistas internacionais foi convocado pelo Centro de Excelência em Defesa Cibernética Cooperativa da OTAN com o intuito de confeccionar um anteprojeto de um manual que trataria, principalmente, do dilema acerca da interpretação e aplicação do direito internacional para os contextos das operações e guerras cibernéticas. Foi a partir dessa iniciativa que o *Tallinn Manual on the International Law Applicable to Cyber Warfare* foi criado.

O *Tallin Manual* consiste em um compilado de propostas de normas, confeccionadas a partir de um estudo eminentemente acadêmico acerca do cenário cibernético contemporâneo, não possuindo, dessa forma, caráter vinculante. Nesse sentido, apresenta-se como o primeiro esforço concreto para analisar a referida

---

Relations and Diplomacy, NATO CCD COE Publications, Tallinn, 2013, p. 24. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017.

matéria de forma compreensiva, lançando luz sobre as questões complexas de natureza legais que circunscrevem essa nova área do direito internacional.[41] Seus principais pontos de debate são as discussões acerca da soberania, da responsabilidade internacional dos Estados, do *jus in bellum,* do direito internacional humanitário e das normas de neutralidade, tudo dentro do escopo do ciberespaço.

O Manual, logo no início, em sua introdução, contempla e examina em que medida as normas legais existentes seriam aplicáveis ao atrito cibernético entre Estados. Nesse sentido, vale asseverar que, em verdade, considera-se que o foco principal do Manual é tratar sobre conflitos armados que podem incluir ou se limitem a operações cibernéticas. Não obstante, o termo guerra cibernética ou *cyber warfare*, é empregado e definido de forma puramente descritiva e sem maiores sentidos normativos. De forma quase paradoxal, o Manual termina por não lidar com questões de maior pertinência temática como, por exemplo, qual deveria ser o tratamento legal em casos de atividades criminais praticadas por hackers.[42]

Seguindo o princípio estabelecido no caso *Corfu Channel* da Corte Internacional de Justiça, o Manual em sua Regra 5 institui que um Estado não permitirá conscientemente que sua infraestrutura cibernética, localizada em seu território ou sob o seu exclusivo controle governamental, seja utilizada para atos que adversamente ou ilicitamente afetem outros Estados:

> Rule 5 – Control of cyber infrastructure
> A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.[43]

[41] SCHMITT, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warfare**, New York: Cambridge University Press, 2013.
[42] O'CONNELL, Mary Ellen. Cyber Security without Cyber War. **Georgetown Journal of International Affairs**, Washington D.C., Vol. 17, 2012, p. 194.
[43] "Regra 5 – Controle sobre ciberestruturas. Um Estado não deverá, conscientemente, permitir que sua ciberestrutura, localizada em seu território ou sob o seu exclusivo controle governamental seja utilizada para a consecução de atos que adversamente e ilegalmente afetem outros Estados." (Tradução livre).

Os especialistas encarregados da redação dessa regra tiveram, dessa forma, o intuito de englobar quaisquer atos ilícitos e que gerem efeitos prejudiciais em outro Estado.[44]

Todavia, não foi possível chegar a um consenso acerca de se essa Regra seria aplicável apenas a operações cibernéticas que estão sendo de fato conduzidas ou também incidiria sobre os atos que indiquem uma mera probabilidade de ocorrerem. Além disso, não houve entendimento uníssono a respeito da natureza do conhecimento do Estado acerca da operação ilícita. Neste ponto, a principal discussão se deu a respeito da possibilidade de a noção construtivista ser aplicável, ou seja, pelo dever do Estado de ter ciência daquela operação ilícita, de forma semelhante ao modelo da responsabilidade objetiva do Estado para fins civis. Finalmente, também foi objeto de debate se a regra em questão seria apenas aplicável para atividades cibernéticas conduzidas no território do Estado ou se também estaria aqui inseridas as operações cibernéticas meramente roteadas através de ciberestruturas presentes nos Estados.

Tratando de atribuição de atos ilícitos, vale observar a Regra 6 que reconhece uma espécie de regra geral que, determina que a conduta de atores não estatais pode ser atribuída ao Estado mediante as bases firmadas pela Comissão de Direito Internacional por meio do seu Projeto de Artigos sobre Atos Internacionalmente Ilícitos e sua aplicação casuística pelas cortes internacionais:

> Rule 6 – Legal responsibility of States
> A State bears international responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation.[45]

Como uma das principais inovações do *Tallinn Manual,* destacam-se as regras 7 e 8 que versam sobre a utilização de estruturas cibernéticas estatais e suas consequências:

---

[44] SCHMITT, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warfare**, New York: Cambridge University Press, 2013, p. 27.

[45] "Regra 6 – Responsabilidade legal dos Estados. Um Estado suportará responsabilização internacional por uma operação cibernética e ele atribuído e que constitui uma violação de uma obrigação internacional." (Tradução livre).

> Rule 7 – Cyber operations launched from governmental cyber infrastructure
>
> The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State, but is an indication that the State in question is associated with that operation.[46]

> Rule 8 – Cyber operations routed through a State
>
> The fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State.[47]

Essa questão será melhor depurada mais adiante neste trabalho, após a discussão sobre o sistema de atribuição de atos internacionalmente ilícitos.

Pode-se, ainda, encontrar disposições sobre as consequências do cometimento de atos internacionalmente ilícitos. Mais marcadamente, o Manual traz referência às contramedidas, instituto já consagrado no âmbito do Projeto de Artigos sobre atos internacionalmente ilícitos, mas, aqui, adaptado às dinâmicas do ciberespaço:

> Rule 9 – Countermeasures
>
> A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.[48]

---

[46] "Regra 7 – Operações cibernéticas conduzidas através de uma ciberestrutura governamental. O simples fato de que uma operação cibernética tenha sido conduzida ou, de outra forma, origine de uma ciberestrutura governamental não constitui prova suficiente para atribuir tal operação ao Estado, mas sim um início que o Estado em questão está associado com a referida operação." (Tradução livre).

[47] "Regra 8 – Operações cibernéticas roteadas através de um Estado. O fato de que uma operação cibernética tenha sido roteada através da ciberestrutura localizada em um Estado não é prova suficiente para atribuir a operação a esse Estado." (Tradução livre)

[48] "Regra 9 – Contramedidas. Um Estado afetado por um ato internacionalmente ilícito poderá recorrer a contramedidas proporcionais, incluindo contramedidas cibernéticas, contra o Estado responsável." (Tradução livre).

Nota-se que a disposição expressa dessa regra incluindo as contramedidas cibernéticas se encontra em linha com a abordagem da comunidade internacional sobre contramedidas. Entende-se que não há uma vinculação necessária do meio que uma contramedida será efetivada, contanto que a proporcionalidade e sua necessidade sejam respeitadas, além de que tais providências sejam adotadas por um Estado na situação de ser vítima de um ilícito causado por outro Estado, com o objetivo de retomar a situação entre os entes ao *status quo,* conforme reconhecido pela CIJ no caso *Gabčíkovo–Nagymaros Project*.

Nesse caso, a Corte reconheceu a legalidade das contramedidas quando tais medidas são proporcionais ao ato ilícito; passíveis de serem revertidos, pois uma vez cessado o ato, a relação entre os Estados deve voltar a ser a mesma, e sejam executadas mediante uma notificação prévia.[49]

Destarte, um Estado para efetuar contramedidas pode se fazer valer do meio cibernético, contanto que respeite os requisitos delineados pelas normas costumeiras e pelo entendimento da Corte.

Por fim, dentre as normas iniciais, de maior relevância para o estudo em tela, podemos destacar as regras do capítulo “Use of Force”, em que se pode encontrar uma tentava de alinhamento das regras do Manual com o que se encontra disposto no artigo 2(4) da Carta da ONU sobre o princípio da não intervenção e a proteção concedida à integridade territorial e a independência política dos Estados.[50]

Como será visto mais adiante, vale pontuar que a classificação de uma operação cibernética como violação do dever de se abster de recorrer à força da Carta da ONU não é pacífica, sobretudo devido à natureza dos ataques cibernéticos quando comparados com ataques armados de traços cinéticos.

Devido à boa recepção do Tallinn Manual pela comunidade internacional, em 2017 foi confeccionada a obra *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, uma obra conjunta dos dezenove experts convocados para o *Tallinn Manual* original, com o intuito de expandir o escopo original do projeto para abarcar, também, as operações cibernéticas mais corriqueiras enfrentadas pelos Estados que não possuem o condão de se enquadrarem como uso da força ou

---

[49] INTERNATIONAL COURT OF JUSTICE. **Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)**, Merits, Judgment. In: ICJ Reports 7, 1997, The Hague, Netherlands.
[50] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Carta da ONU**. São Francisco, 1945, art. 2(4). Disponível em: <http://unicrio.org.br/img/CartadaONU_VersoInternet.pdf>. Acesso em: 10 ago. 2017.

mesmo conflito armado.[51] Ademais, nota-se que houve uma expansão da proposta de comentários de cada regra do *Tallinn Manual*, havendo, agora, uma discrepância no que se refere ase determinada análise de uma das normas do *Tallinn Manual 2.0* foi adotada de forma unânime ou não. Nesse sentido, pode-se encontrar também, as posições vencidas, o que contribui, ainda mais, para a riqueza e para a maturidade desse trabalho.

Destarte, o *Tallinn Manual* se coloca como a principal referência para qualquer estudo acerca do espaço cibernético tendo como ponto de partida o direito internacional. Em verdade, os frutos desse trabalho de sete anos do grupo de experts são apenas o começo para o desenvolvimento dessa nova seara do direito internacional, tendo como papel fundamental o de desbravar essa área juridicamente ainda incipiente.

[51] SCHMITT, Michael N. **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, New York: Cambridge University Press, 2017.

3 O CIBERESPAÇO E O SISTEMA DE RESPONSALIZAÇÃO DOS ESTADOS POR ATOS INTERNACIONALMENTE ILÍCITOS

3.1 OS ELEMENTOS CONSTITUTIVOS DE UM ATO INTERNACIONALMENTE ILÍCITO

A responsabilidade dos Estados é uma instituição fundamental no Direito Internacional, sendo resultado direto da personalidade jurídica dos Estados e do fato de que esses entes são os principais portadores de obrigações internacionais.

Dessa forma, as normas de responsabilidade dos Estados têm o importante papel de impedir a impunidade dos Estados por atos que violem direitos de outros entes, como outros Estados, indivíduos e comunidades.

De acordo com o conceito mais aceito, o termo *responsabilidade internacional* abrange as relações jurídicas de Direito Internacional ocasionadas em razão de atos internacionalmente ilícitos[52], resultando, assim, da personalidade jurídica geral dos Estados, e desses serem os principais titulares das obrigações internacionais[53].

O que exatamente irá constituir uma violação do Direito Internacional, por parte de um Estado, depende das obrigações internacionais assumidas, que variam de um Estado para o outro, pois não existe no ordenamento internacional um documento que enumere as obrigações de todos os Estados, de forma que esses sujeitos terão compromissos e responsabilidades distintas[54].

Por outro lado, os conceitos subjacentes da responsabilidade dos Estados (imputação, violação e as consequências) são de caráter geral. Assim, qualquer violação às normas do Direito Internacional, seja no caso de descumprimento de uma obrigação de um tratado ou uma violação de um princípio, as regras de atribuição e reparação serão as mesmas.

As normas de responsabilidade dos Estados foram examinadas pela

---

[52] INTERNATIONAL LAW COMMISSION. **Draft Articles On The Responsibility Of International Organizations, With Commentaries**, Yearbook of the International Law Commission v. II, part 2, [S.l.], 2011, art. 1(1); ANZILOTTI, Dionisio. **Cours de Droit International**. Paris: Panthéon-Assas LGDJ, 1999, p. 467.

[53] Assim como o Direito dos Tratados, as regras que regem a responsabilidade internacional dos Estados fornecem o quadro de referência para considerar outras formas de responsabilidades internacionais, em particular a responsabilidade de organizações internacionais.

[54] Por exemplo, se um Estado violar um tratado do qual ele é signatário, poderá ser responsabilizado internacionalmente. O mesmo não acontece com um Estado que não está vinculado a um tratado, pois não terá obrigação de seguir suas regras, a menos que sejam consideradas costumeiras.

Comissão de Direito Internacional ao longo de mais de 40 anos, tendo sido codificadas e desenvolvidas no Projeto de Artigos sobre a Responsabilidade dos Estados por Atos Internacionalmente Ilícitos de 2001.

Esse Projeto de Artigos é, atualmente, o documento mais importante sobre a responsabilidade internacional dos Estados e representa tanto uma codificação das normas costumeiras existentes, quanto o desenvolvimento progressivo de questões ainda não definidas pelo costume.[55]

Deve-se ressaltar que ao longo da elaboração dos Artigos sobre Responsabilidade dos Estados, a CDI especificou que seu trabalho de codificação se aplicava, apenas, às regras "secundárias", com a exclusão das regras "primárias" do Direito Internacional. Ou seja, a CDI limitou o alcance do projeto às regras que regulam, especificamente, a responsabilidade internacional, seus aspectos processuais e suas consequências, com a supressão das normas violadas que deram origem à responsabilidade[56] [57].

Nesse sentido, o Capítulo I do Projeto de Artigos estabelece certos princípios gerais: ***(i)*** todo ato internacionalmente ilícito de um Estado implica sua responsabilidade internacional (Art. 1); ***(ii)*** um ato internacionalmente ilícito existe quando a conduta ou omissão é atribuível a um Estado e constitui violação de uma obrigação internacional devida por esse Estado (Art. 2); ***(iii)*** a caracterização de um ato internacionalmente ilícito é regida pelo Direito Internacional, não sendo, assim, afetada por uma possível permissibilidade no Direito Interno (Art. 3).

---

[55] Por ter natureza costumeira, essas normas, meramente materializadas no Projeto de Artigos, possuem força vinculante perante os Estados, visto que se enquadram como uma das fontes do direito internacional de acordo com o Estatuto da Corte Internacional de Justiça.

[56] INTERNATIONAL LAW COMMISSION. **Report of the Commission to the General Assembly on the work of its thirty-second session**, Yearbook of the International Law Commission v. II, part 2, [S.l] 1980, p. 27, § 23.

[57] Ainda sobre essa temática, pode-se trazer o caso arbitral Rainbow Warrior, entre a França e Nova Zelândia, em 1990. Essa arbitragem se originou devido a um incidente em 1985, em que os agentes franceses destruíram o navio *Rainbow Warrior* no porto na Nova Zelândia. O Secretário-Geral da ONU foi convidado para mediar o caso, e sua decisão previu que a França deveria pagar uma indenização à Nova Zelândia, e que dois agentes franceses deveriam ser transferidos à uma base francesa no Pacífico, onde eles deveriam ficar por três anos e não sair sem o consentimento mútuo de ambos os Estados. No entanto, ambos os agentes foram repatriados para a França antes da data limite dos três anos, sem o consentimento da Nova Zelândia. O Acordo de 1986 continha uma cláusula de arbitragem e essa foi invocada pela Nova Zelândia. O argumento apresentado pela Nova Zelândia centrava no incumprimento de uma obrigação de tratado pela França, enquanto a França argumentou que somente a lei da responsabilidade dos Estados era relevante e que os conceitos de força maior e perigo extremo a exoneravam de responsabilidade. O tribunal arbitral decidiu que a lei dos tratados era relevante para o caso, mas as consequências legais da quebra do tratado, incluindo a determinação das circunstâncias excludentes de ilicitude e os remédios, eram sujeitos às regras costumeiras de responsabilidade dos Estados.

Dessa forma, configuram-se elementos constitutivos da responsabilidade internacional: (i) atribuição ou imputabilidade ao Estado de certo ato; (ii) e violação de uma obrigação internacional, por meio daquele ato[58].

3.2 ATRIBUIÇÃO DE RESPONSABILIDADE AOS ESTADOS E OS TESTES DE CONTROLE

3.2.1 Aspectos gerais

Como regra geral, a violação de uma obrigação por parte dos Estados deve surgir em virtude da ação ou omissão[59] de um ou mais de seus órgãos ou agentes[60].

Nos termos do Artigo 4 do Projeto de Artigos, eventual desrespeito a uma norma internacional praticada por qualquer órgão do Estado será imputada ao ente soberano, independentemente do caráter daquele órgão ou da função que ele exerce. Incluem-se aqui tanto os atos do poder executivo, legislativo ou judiciário, visto que compõem perante a comunidade internacional o Estado enquanto sujeito de Direito Internacional. Nesse sentido, o mesmo princípio se aplica para as forças armadas e suas diversas divisões, como os grupos de defesa cibernética sob a responsabilidade do Estado.

No caso *Armed Activities On The Territory Of The Congo*, a CIJ analisou se Uganda era responsável pelos atos e omissões de suas forças armadas no território do Congo. A Corte considerou que a conduta das forças armadas era atribuída à Uganda, uma vez que o Estatuto militar desse país enquadrava o Exército como órgão do Estado, restando, assim, infundada a alegação da Uganda de que seus soldados agiram sem autoridade governamental.[61]

Pertinente também é a forma de atribuição da conduta das forças militares de um Estado, quando essas atuarem sob o comando e controle de uma entidade

---

[58] A definição da CDI não incluiu o elemento dano como uma das condições para a configuração de um ato internacionalmente ilícito.

[59] Por exemplo, no caso *Corfu Channel*, a Albânia foi responsabilizada pelas consequências de minas postas em suas águas territoriais, apesar delas provavelmente terem sido colocadas pela Iugoslávia. Nesse caso, a responsabilidade veio do fracasso das autoridades albanesas de alertar sobre a presença das minas.

[60] Por exemplo, o caso *Armed Activities* (Congo *versus* Uganda), em que a Corte considerou que a conduta das Forças Armadas de Uganda era atribuível ao Estado, pois era um Órgão do Estado.

[61] INTERNATIONAL COURT OF JUSTICE. **Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)**, Judgment. In: ICJ Reports 168, 2005, The Hague, Netherlands.

diferente. No caso *Behrami*, a Corte Europeia de Direitos Humanos decidiu não atribuir a responsabilidade aos Estados pela conduta das suas forças militares, que faziam parte da "Força Internacional de Segurança no Kosovo" (KFOR), em 1999, autorizada pela resolução 1244 do Conselho de Segurança. O referido tribunal considerou que o Conselho teria a autoridade final e controle dessas tropas, e a OTAN, por sua vez, teria o controle efetivo das questões operacionais relevantes[62]. No entanto, a Corte de Apelações de Haia refutou esse raciocínio, considerando que existe a possibilidade de mais de uma parte ter o "controle efetivo" das tropas, logo não se pode excluir a responsabilidade do Estado simplesmente porque outro sujeito possa também exercer o controle sobre suas forças armadas[63].

Outra relevante forma de se atribuir um ato a um Estado é através da aprovação ou adoção do ato internacionalmente ilícito pelo Estado. Nesse sentido, pode-se atribuir responsabilidade a um Estado caso ele aceite ou adote para si uma conduta ilícita praticada por um indivíduo ou por um ente privado que não tem conexão com este ente.

Esse preceito já foi aplicado pela CIJ no caso *Tehran Hostages*. Nesse caso, um grupo de estudantes, sem qualquer ligação inicial com o governo iraniano, invadiu a embaixada americana em Teerã, sequestrando mais de sessenta Diplomatas e cidadãos americanos, que foram mantidos em cativeiro por 444 dias. Apesar de não estar envolvido com o ataque, o Irã falhou em condenar os atos, chegando até mesmo a endossar a conduta do grupo. Por esse motivo, a Corte considerou que, apesar de o Irã não ter sido inicialmente responsável pelos atos dos estudantes, o seu endosso posterior e sua postura diante da situação geraram responsabilidade internacional pelos atos ilícitos.

Entretanto, o mais importante dilema da responsabilização internacional por atos internacionalmente ilícitos diz respeito a atos cometidos por indivíduos que possuem, de certa forma, um vínculo com o Estado, sobretudo se o indivíduo ou entidade atuou sob a instrução, direção ou controle do Estado[64].

---

[62] EUROPEAN COURT OF HUMAN RIGHTS. **Decision On Admissibility Behrami and Behrami v. France and Saramati v. France, Germany and Norway**. Strasbourg, 12 fev. 1975. Disponível em: <http://hudoc.echr.coe.int/eng-press?i=003-2012546-2140039>. Acesso em 14 ago. 2017, §140.

[63] HOLANDA. Supreme Court of Netherlands. **The State of the Netherlands v. Hasan Nuhanović Case no. 12/03324, Judgment**. 2013, The Hague, Netherlands. Disponível em: <http://www.asser.nl/upload/documents/20130909T125927-Supreme%20Court%20Nuhanovic%20ENG.pdf>. Acesso em: 14 ago. 2017, §§5.9, 5.18, 5.20.

[64] CRAWFORD, James. ***State Responsibility*** **The General Part**. Cambridge: Cambridge University Press, 2014, p.141.

A responsabilidade do Estado, em razão de pessoas que agem sob sua instrução, ocorre quando um órgão do Estado terceiriza alguma de suas funções, contratando, por exemplo, pessoas ou entes privados para que o "auxiliem" na realização de certa atividade.

Em 2007, no caso *Genocide*[65], a CIJ tentou esclarecer suas hipóteses de aplicação. Na oportunidade, considerou que um Estado só seria responsabilizado pelos atos de indivíduos sob suas instruções se as determinações tivessem relação direta com ato ilícito, não existindo responsabilidade nas ações de caráter geral das pessoas ou grupos que cometeram as violações.

Isso, no entanto, não consegue resolver totalmente o problema da aplicação dessa regra, uma vez que a Corte não estabeleceu como seria interpretada essa relação direta, ficando ambíguo se o Estado precisa direcionar a entidade para um ato específico, ou se uma instrução geral, que deixa o método para cumprir a ordem em aberto, poderia levar à responsabilização do Estado. A doutrina tem se inclinado mais para essa segunda hipótese[66].

Em conclusão, tem-se que, se um Estado autorizou um ato, e o ilícito decorreu diretamente da conduta autorizada, haverá responsabilidade do Estado por esse ato, a menos que ele esteja claramente fora do escopo da ordem[67].

O Projeto de Artigos, em seu Artigo 8, estabelece que um Estado pode ser responsabilizado por atos de entes privados, se esses estiverem sob sua direção e controle[68].

Nesse sentido, direção e controle constituem elementos imprescindíveis para aferir o vínculo do Estado com o ato ilícito visando a avaliar se a conduta pode ser atribuída ao ente estatal.

No entanto, nem o Artigo 8 e nem a prática dos Estados definem o nível de controle necessário para que se possa atribuir determinado ato ao Estado, o que levou à criação de dois testes, ou critérios, diferentes de atribuição: o **controle**

---

[65] INTERNATIONAL COURT OF JUSTICE. ***Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)***, Judgment. In: ICJ Reports 43, 2007, The Hague, Netherlands, p. 169, §400.

[66] CRAWFORD, James. **Brownlie's Principles of Public International Law**. 8 ed. Oxford: Oxford University Press, 2012.

[67] INTERNATIONAL LAW COMMISSION. **Draft Articles On The Responsibility Of International Organizations, With Commentaries**, Yearbook of the International Law Commission v. II, part 2, [S.l.], 2011, art. 8(8).

[68] Apesar de falar em direção e controle de forma separada, muitos tribunais têm interpretado que essas duas palavras impõem um padrão único de atribuição.

efetivo (*effective control*), elaborado pela CIJ no caso *Nicaragua*; e o **controle geral (*overall control*)** do Tribunal Penal Internacional para a antiga Iugoslávia formulado no caso *Tadić*.

3.2.2 Controle Efetivo

Os doutrinadores do Direito Internacional Público, via de regra, apresentam conceitos elusivos acerca da definição do teste de controle efetivo. Notadamente, isso se deve devido à alta controvérsia sob a ótica da impunidade que cerca o principal caso da CIJ que abordou a referida técnica atributiva: o Caso *Nicaragua*, cuja análise é indispensável para a compreensão real do referido instituto.

O caso *Nicaragua* (Nicarágua v. Estados Unidos) é um dos mais emblemáticos da história da CIJ, devido à diversidade de temas abordados, e do desenvolvimento da jurisprudência da Corte. Nesse sentido, um dos avanços mais relevantes do caso em questão foi justamente o detalhamento do chamado teste de controle efetivo.

No caso em tela, a CIJ foi convocada a decidir se as violações a direitos humanos cometidas pelos Contras, um grupo paramilitar que lutou contra o Estado da Nicarágua na guerra civil, poderiam ser atribuídas aos Estados Unidos, que tinha dado suporte ao grupo durante a guerra.

Destarte, a Corte identificou da análise dos elementos factuais, três formas de conduta "privada" específicas que poderiam gerar responsabilidade do Estado americano: (a) operações militares específicas; (b) a campanha paramilitar em geral; (c) e violações de direito humanitário cometidas pelos *Contras* no decorrer das operações.

Em relação às missões específicas dos *Contras*, a Corte considerou que a Nicarágua não foi capaz de estabelecer um vínculo real entre os americanos e as operações paramilitares específicas, comprovando, tão somente, o envolvimento geral dos Estados Unidos na guerra civil[69]. Assim, os atos paramilitares específicos não poderiam ser atribuídos ao Estado americano, uma vez que a Corte decidiu que, nesses casos, não existiram provas concretas do envolvimento dos Estados Unidos.

---

[69] INTERNATIONAL COURT OF JUSTICE. ***Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)***, Merits, Judgment. In: ICJ Reports 14, 1986, The Hague, Netherlands.

Em relação aos dois últimos pontos, campanha paramilitar em geral e violações ao direito humanitário, a Corte, com vista a adotar um padrão de atribuição de responsabilidade, elaborou o **teste de controle efetivo**.

No julgamento, a Corte decidiu que, apesar de os Estados Unidos serem responsáveis por financiar, dar suporte logístico e treinamento militar ao grupo[70], ele não poderia ser responsabilizado internacionalmente pelas ações gerais dos *Contras*. A CIJ fundamentou sua decisão no fato de que os Estados Unidos não exerciam controle suficiente sobre o grupo, visto que os *Contras* não eram completamente dependentes[71] do Estado americano, assim, a campanha paramilitar em geral não ensejaria qualquer responsabilização dos Estados Unidos da América[72].

No que se refere às violações de direito humanitário, a CIJ observou que, apesar da participação de os Estados Unidos ter sido decisiva e preponderante, ela ainda era insuficiente para atribuir responsabilidade ao ente americano por atos cometidos pelos *Contras*[73]. Assim, só existiria responsabilidade dos Estados Unidos se ficasse comprovado o seu controle efetivo sobre as operações paramilitares que ocasionaram as violações de direito humanitário. A Corte enalteceu o fato de que a participação dos Estados Unidos não tinha, *prima facie*, a capacidade de direcionar ou endossar a realização de atos contrários ao Direito Internacional, pois os atos foram cometidos pelos *Contras* sem o controle efetivo dos Estados Unidos.

Observa-se, então, que o conceito de controle efetivo está diretamente relacionado com a capacidade do Estado direcionar a conduta do agente privado em questão mediante instruções específicas para a consecução de dado objetivo, configurando-se, assim, a existência de uma relação de dependência materializada através de um controle concreto ou efetivo.

Nesse sentido, no caso do Genocídio de 2007, a CIJ traçou um paralelo dessa noção de dependência com o termo "órgão de facto" no contexto do artigo 4

---

[70] INTERNATIONAL COURT OF JUSTICE. ***Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),*** Merits, Judgment. In: ICJ Reports 14, 1986, The Hague, Netherlands, p. 54, §115.

[71] No caso Genocide a CIJ identificou melhor essa noção de dependência completa pelo termo *de facto organ*, no contexto do Projeto de Artigos, Art 4. Para a Corte, esses órgãos são completamente vinculados aos Estados, de forma que não possuem real autonomia.

[72] A Corte, no entanto, considerou que existiu uma violação da proibição do uso da força, com base no suporte direto dado ao grupo paramilitar.

[73] INTERNATIONAL COURT OF JUSTICE. ***Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),*** Merits, Judgment. In: ICJ Reports 14, 1986, The Hague, Netherlands, p. 54, §115.

dos Projeto de Artigos. Para a Corte, este tipo de órgão encontrado no texto do artigo 4, embora não seja considerado um órgão do Estado, está completamente ligado a ele, não tendo autonomia e sendo completamente dependente, tal qual o ente privado sob o controle efetivo do Estado.[74]

A utilização desta ferramenta jurídica pela Corte reabasteceu, com razão, as críticas dos céticos ao Direito Internacional, sobretudo diante do resultado material do caso *Nicaragua*: a ausência de responsabilização devida dos Estados Unidos e a consequente criação de um cenário de impunidade. Não obstante, a utilização do teste de controle efetivo tem sido considerada como uma ferramenta de proteção estatal pelos próprios Estados, que a defendem em consonância com o argumento da CIJ que o teste de controle efetivo seria a ferramenta atributiva verdadeiramente adequada às particularidades normativas do Direito Internacional.

Destarte, conforme demonstra a prática internacional, resta inegável a predominância absoluta da aplicação deste teste de controle para fins de atribuição de atos internacionalmente ilícitos aos Estados quando praticados por particulares.

3.2.3 Controle Geral

Em contraposição à doutrina do Controle Efetivo, o Tribunal Penal Internacional para a Antiga Iugoslávia (TPIAI), no caso *Tadić*, estabeleceu o teste do controle geral.

Duško Tadić era guarda em um acampamento bósnio ao redor de Prijedor, na Bósnia-Herzegovina, e foi um dos responsáveis do massacre de 14.000 pessoas durante a Guerra da Bósnia[75]. Após o fim do conflito, Tadić, com base no Estatuto do TPIAI, foi acusado de crimes de guerra e crimes contra a humanidade.

Por ser um tribunal com jurisdição limitada a indivíduos, o TPIAI ordinariamente não é considerado competente para tratar questões de responsabilidade dos Estados. No caso *Tadić*, no entanto, o Tribunal, atuando dentro de sua jurisdição, tratou a responsabilidade dos Estados como uma questão

---

[74] INTERNATIONAL COURT OF JUSTICE. ***Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)***, Judgment. In: ICJ Reports 43, 2007, The Hague, Netherlands.

[75] A Guerra da Bósnia foi um conflito armado que ocorreu entre abril de 1992 e dezembro de 1995 na região da Bósnia e Herzegovina. A guerra foi causada por uma combinação complexa de fatores políticos e religiosos: o fervor nacionalista, crises políticas, sociais e de segurança que se seguiram ao fim da Guerra Fria e da queda do comunismo na antiga Iugoslávia.

preliminar, de forma a poder determinar a distinção entre conflito armado internacional ou não internacional[76]. Essa distinção era importante ao caso, pois a Convenção de Genebra de 1949[77], principal base jurídica dos crimes humanitários, em quase a sua totalidade, limitava sua aplicação aos conflitos internacionais.

Para definir se a guerra na Bósnia-Herzegovina era ou não um conflito internacional, a primeira instância do TPIAI ponderou a relação entre os três grupos étnicos da região[78] e a influência externa dos Estados envolvidos. Caso esses Estados fossem considerados responsáveis pelas atividades dos entes privados atuando na Bósnia, o conflito seria considerado internacional. O Tribunal focou especialmente nos atos da República Srpska, uma das entidades autônomas da Bósnia e Herzegovina contrária à independência e cujas forças foram responsáveis pelo Massacre de Srebrenica, em que 8.373 bósnios muçulmanos foram assassinados.

A grande maioria dos juízes de primeira instância utilizou o entendimento do caso *Nicaragua* para poder determinar se a República da Iugoslávia poderia ser responsabilizada pelos atos da República Srpska[79]. Ao final, o Tribunal concluiu que a Republica Srpska, ainda que aliada da Iugoslávia e dependente de sua assistência, não poderia ser considerada sob seu controle.

A Câmara de Apelações do TPIAI revisou o caso em 1999 e reafirmou a decisão de utilizar as regras de responsabilidade dos Estados para determinar a dimensão internacional do conflito, mas criticou a utilização do teste de controle efetivo, do caso *Nicaragua*, como critério de atribuição. Para a Câmara de Apelações, a noção de controle efetivo era contrária à "lógica" da responsabilidade dos Estados[80], pois permitia que esses se utilizassem de entes privados para cometer atos que não poderiam ser realizados por seus próprios órgãos, burlando, assim, as normas de responsabilização internacional.

---

[76] INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA. **Prosecutor v. Duško Tadic**, ICTY Case No. IT-94-1- T, Trial Chamber, 1997, The Hague, Netherlands.

[77] A IV Convenção de Genebra outorga proteção aos civis, inclusive em território ocupado, e serve como base nos julgamentos do TPIAI.

[78] Sérvios cristãos ortodoxos, os croatas católicos romanos e os bósnios muçulmanos.

[79] INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA. **Prosecutor v. Duško Tadic**, ICTY Case No. IT-94-1- T, Trial Chamber, 1997, The Hague, Netherlands, §206.

[80] INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA. **Prosecutor v. Duško Tadic, Appeal against Conviction** , ICTY Case No. IT-94-1- A, Appeals Chamber, 1999, The Hague, Netherlands, §§98-121.

A Câmara de Apelações, de forma semelhante à CIJ, reconheceu a necessidade do elemento controle na relação dos Estados com os agentes, porém, entendeu que o nível de controle poderia variar de acordo com as circunstâncias fáticas de cada caso, em especial ao nível de organização ou estruturação do ente.

Nesse sentido, em relação aos grupos não organizados, ou atos de indivíduos, aplica-se o teste de controle efetivo, enquanto que em relação a grupos organizados somente o controle geral seria satisfatório para a imputação da responsabilidade.

Portanto, de acordo com o teste de controle geral criado pelo TPIAI, se o Estado organizar, coordenar, financiar ou planejar as ações de grupos estruturados, poderá ser responsabilizado internacionalmente[81].

Essa teoria é muito criticada no Direito Internacional, inclusive pela própria Corte Internacional de Justiça.

No caso *Genocídio*, inserido no mesmo contexto factual do caso *Tadić*, a Corte analisou se a Iugoslávia, e mais tarde a Sérvia, era responsável pelo genocídio cometido pelos grupos armados sérvios durante a Guerra da Bósnia.

Em sua decisão, a Corte criticou a postura do TPIAI, argumentando que, apesar de o Tribunal ser uma autoridade no Direito Penal internacional, ele não teria a competência de emitir opiniões fora de sua jurisdição, ou seja, sobre responsabilidade internacional dos Estados[82]. Nesse sentido, a Corte decidiu, independentemente da situação, ainda que em casos de graves violações ao Direito Internacional, não relativizar o teste de controle efetivo para atribuição de um ato ilícito a um Estado.

Dessa forma, a CIJ entendeu que o teste do controle geral era impróprio para ser aplicado na atribuição. Nas palavras da Corte:

> It must next be noted that the 'overall control' test has the major drawback of broadening the scope of State responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its

[81] O efeito desse teste de controle geral é praticamente inutilizar, no campo da atribuição, a distinção entre órgãos do Estado e órgãos não estatais.
[82] INTERNATIONAL COURT OF JUSTICE. ***Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)***, Judgment. In: ICJ Reports 43, 2007, The Hague, Netherlands, p. 170, §403.

> own conduct, that is to say the conduct of persons acting, on whatever basis, on its behalf [...] In this regard the 'overall control' test is unsuitable, for it stretches too far, almost to breaking point, the connection which must exist between the conduct of a State's organs and its international responsibility.[83]

Isto posto, considerando o viés prático da discussão, faz-se necessário utilizar esse posicionamento da CIJ como modulador das tentativas de criação ou adoção de outros testes de controle além do efetivo, visto que a CIJ sacramentou a sua preponderância e aplicabilidade mesmo em casos extremos como a discussão da violação da obrigação de um Estado de prevenir a ocorrência de genocídio.

3.2.4 Os testes de controle e o contexto cibernético

Como visto, o Direito Internacional é integrado por um sistema de normas que prescrevem técnicas específicas para a atribuição de atos internacionalmente ilícitos. Diante disso, cabe, então, tecer considerações acerca da aplicação dessas normas ao cenário cibernético.

De antemão, cabe ressaltar que as principais questões concernentes às violações cometidas no ciberespaço dizem respeito a atos comissivos que infringem o dever de devido cuidado.

Nesse sentido, percebe-se que, marcadamente, violações ao art. 2(4) da Carta da ONU adquirem uma maior importância, visto que estes atacam diretamente a soberania de outros Estados, seja na dimensão de sua independência política ou da integridade territorial. Dessa forma, é imprescindível a análise do papel desempenhado pelo Estado diante de tais atos.[84]

---

[83] "Deve ser observado que o teste do 'controle geral' tem a grande desvantagem de alargar o âmbito da responsabilidade do Estado além do princípio fundamental que rege a responsabilidade internacional: um Estado é responsável somente pela sua própria conduta, isto é, a conduta das pessoas que atuam, em qualquer base, em seu nome. [...] Nesse contexto, o teste de 'controle geral' é inadequado, pois estende muito longe, quase ao ponto de ruptura, a ligação que deve existir entre a conduta dos órgãos do Estado e sua responsabilidade internacional." (Tradução livre).

[84] PIRKER, Benedict. Territorial Sovereignty and Integrity and the Challenges of Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 14 ago 2017.

Como já visto, por força do direito costumeiro internacional, materializado no art. 8 do Projeto de Artigos, considera-se como ato estatal perante o direito internacional, “a conduta de um indivíduo ou grupo de indivíduos se estes estiverem agindo mediante instruções ou direção e controle do referido Estado.” Diante dessa norma costumeira, surgiram duas principais técnicas para delimitar o alcance do elemento “controle”, que engloba as noções de instruções, direção e controle em sentido estrito.

Foram criados, para tal fim, os denominados Testes de Controle já abordados acima, com diferentes escopos no que se refere ao tratamento de determinadas ações do Estado perante o individuo ou grupo de indivíduos cometedores do ilícito internacional.

De forma mais predominante, nota-se a prevalência do Teste de Controle Efetivo, abordagem mais restritiva elaborada pela CIJ, em que se exige o estrito cumprimento de instruções e comandos, sendo insuficientes para a satisfação do referido teste medidas de financiamento ou treinamento.

Aplicado ao cenário cibernético, percebe-se que tal Teste de Controle pode ser satisfeito em hipóteses, por exemplo, em que determinado Estado celebra um contrato com uma entidade privada para incumbências de segurança cibernética, situação em que a conduta da referida companhia pode ser atribuída ao Estado na medida em que tais condutas originem de instruções do Estado.

Michael Schmitt, o editor do *Tallinn Manual,* destaca, ainda, uma situação interessante oriunda de empresas de tecnologia estatais. O renomado autor destaca que qualquer atribuição nesse contesto deve se basear nas delimitações do teste de controle efetivo, visto que não haveria, aqui, uma atribuição *prima facie* devido à natureza jurídica da empresa, visto que, com base nas normas costumeiras, o mero fato de que determinada empresa é pública não constitui elemento suficiente para atribuir suas ações ao Estado.[85]

Ainda nessa linha, ações como as praticadas por *hacktivists* ou mesmo hackers patriotas,[86] que eventualmente conduzam ataques DDoS, a título figurativo, são extremamente difíceis de serem atribuíveis ao Estado diante da sistemática

[85] SCHMITT N., Michael. Cyber Activities and the Law of Countermeasure In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 14 ago 2017.

[86] A exemplo dos incidentes na Estônia e na Geórgia analisados no capítulo 2.

normativa dos Testes de Controle, somado ao entendimento da CIJ no caso *Tehran Hostages* sobre adoção pelo Estado de um ato ilícito cometido por terceiros, sendo necessário, em verdade, o reconhecimento e a aprovação expressa do Estado.[87]

Michael Schmitt assevera, ainda, que a questão geográfica se torna total irrelevante para fins de atribuição do ato internacionalmente ilícito. O principal exemplo materializa-se através da técnica do *botnet,* em que entes não estatais assimilam diversos computadores ao redor do globo para, conjuntamente comandados remotamente, conduzam atividades cibernéticas contra determinado alvo. Nessa situação, o que realmente se mostra relevante é o grau de controle apurado na ligação desse ente não estatal com determinado Estado, observando-se se houve, efetivamente, o cumprimento dos requisitos já estudados para a atribuição de atos internacionalmente ilícitos, independentemente da localização desse agente ou de seus instrumentos de ataque.[88]

O *Tallinn Manual* também se propõe em abordar o presente dilema, fazendo clara referência ao teste de controle efetivo e ao geral. Nesse supedâneo é necessário reconhecer que, ao se referir sobre o teste de controle geral, em nenhum momento o *Tallinn Manual* se alinha a tal técnica ou mesmo busca relativizar as noções traçadas no caso *Tadić,* que considera o comportamento de conceder auxílios gerais como suficiente para atribuir o ato ao Estado.[89] Em verdade, os redatores do Manual escolheram utilizar denominações textuais que denotam uma maior rigidez para a atribuição de atos ilícitos, através do qual o reconhecimento da responsabilidade estatal devesse requerer a participação oficial no planejamento e supervisão das operações cibernéticas. Sob essa ótica, o Estado não seria responsabilizado internacionalmente por um dano causado por um grupo particular por meio de atividades cibernéticas, ao menos que o Estado tenha realizado

---

[87] PIRKER, Benedict. Territorial Sovereignty and Integrity and the Challenges of Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 14 ago 2017.

[88] SCHMITT N., Michael. Cyber Activities and the Law of Countermeasure In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 14 ago 2017.

[89] SCHMITT, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warfare**, New York: Cambridge University Press, 2013.

condutas que fossem além do financiamento e equipagem do grupo.[90] Dessa forma, há uma clara aproximação normativa com o teste de controle efetivo aplicado pela Corte Internacional de Justiça, posição a qual este trabalho se alinha, devido à maior estabilidade jurídica concedida por tal técnica.

Não obstante a posição aqui defendida acerca da prevalência do Teste de Controle Efetivo, via de regra, a aplicação dessa teoria acaba por causar situações de impunidade devido ao tratamento probatório atual das cortes internacionais na qual, de forma mais cabal, obsta a viabilidade da responsabilização de atos internacionalmente ilícitos cometidos através do espaço cibernético.

3.3 NÃO CUMPRIMENTO DE UMA OBRIGAÇÃO INTERNACIONAL NO CONTEXTO CIBERNÉTICO

3.3.1 Ataques cibernéticos e a vedação ao uso da força

O início do século XX foi acompanhado, na seara internacional, pela revisão do comportamento estatal de uso indiscriminado da força perante outros Estados. Nesse sentido, já em idos do século XIX, com o progressivo desenvolvimento do chamado “Direito Internacional da Paz”, foi-se, cada vez mais, enfraquecendo a concepção que o recurso à guerra constituía um dos principais traços da manifestação da soberania dos Estados.[91]

A principal materialização dessa linha pensamento foi na Carta da Liga das Nações, na qual se verifica uma tentativa de incorporação de técnicas limitadoras ao uso da força no ambiente europeu, mais notadamente nos arts. 11 a 17, em que se observa a criação de um procedimento formal que os Estados signatários deveriam seguir para que pudessem promover uma guerra legítima. Nota-se, dessa forma, que, nesse momento, o uso da força e a promoção da guerra ainda não constituíam atos internacionalmente ilícitos em si mesmos.

Vale asseverar, ainda, que foi na Carta da Liga das Nações que primeiramente houve o advento de uma proteção especializada à integridade territorial e à independência política, elementos constitutivos do chamado princípio

[90] SCHMITT, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warfare**, New York: Cambridge University Press, 2013.

[91] A exemplo da anexação da Alsácia e Lorena pelo Império Alemão em meados do século XIX que foi alvo de uma política de não reconhecimento por parte da maioria dos Estados europeus, sobretudo da própria França.

da não intervenção, cujo escopo de proteção apenas abarcava os Estados membros.[92] Essa lógica de pensamento reforçou, ainda mais, as críticas da época ao regime da Liga das Nações que buscou, no mais das vezes, instituir o que se chama de “paz dos vencedores” após a Primeira Guerra Mundial, o que contribuiu de forma determinante para a deflagração da Segunda Grande Guerra.

Alternativamente, foi no período entre guerras que surgiu a principal inspiração para o atual regramento sobre o uso da força: o Pacto Briand-Kellogg ou Tratado Geral para Renúncia de Guerras. Através dele, foi criado um sistema normativo composto de quatro principais elementos, todos posteriormente incorporados, com as devidas adequações, ao regime da Carta da ONU: ***(i)*** a obrigação de não se utilizar da guerra para resolver disputas internacionais; ***(ii)*** a obrigação de resolver conflitos por meios pacíficos; ***(iii)*** a possibilidade de reservas pontuais às obrigações anteriores em casos de defesa própria ou coletiva; e ***(iv)*** ressalva às obrigações dispostas no Carta da Liga das Nações.

Após o fim da Segunda Guerra Mundial, em que se observou o desfacelamento das normas limitadoras do uso da força, uma das principais preocupações dos Estados ao momento de criação da ONU foi justamente conceber um novo sistema de normas que considerasse as lições aprendidas nos regimes da Liga das Nações e no Briand-Kellogg, buscando evitar suas principais falhas.

Destarte, com isso em mente, houve o advento do artigo 2º da Carta da ONU, que em seu parágrafo 4, em conjunto, de forma auxiliar, com o parágrafo 3 e 7, prescreve a denominada regra geral de vedação ao uso da força baseada no princípio da não intervenção:

> Artigo 2. A Organização e seus Membros, para a realização dos propósitos mencionados no Artigo 1, agirão de acordo com os seguintes Princípios:
> (...)

[92] Nesse sentido, o art. 10 da Carta determinava que os membros estariam obrigados a preservar e respeitar a integridade territorial e independência política uns dos outros contra agressões externas. Interessante observar que, conjugando esse Artigo com as disposições procedimentais acerca do uso da força, pode-se concluir que dentro do regime da Liga das Nações estava vedado o uso da força apenas contra seus próprios membros, haja vista que atos de guerra implicariam violação à integridade territorial e independência política de um outro Estado. Em sentido convenientemente contrário, no entanto, haveria a plena possibilidade de, legalmente, se valer da guerra contra Estados não membros.

> 3. Todos os Membros deverão resolver suas controvérsias internacionais por meios pacíficos, de modo que não sejam ameaçadas a paz, a segurança e a justiça internacionais.
> 4. Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas.
> (...)
> 7. Nenhum dispositivo da presente Carta autorizará as Nações Unidas a intervirem em assuntos que dependam essencialmente da jurisdição de qualquer Estado ou obrigará os Membros a submeterem tais assuntos a uma solução, nos termos da presente Carta; este princípio, porém, não prejudicará a aplicação das medidas coercitivas constantes do Capítulo VII.

Esse regramento, que também possui *status* consuetudinário,[93] foi posteriormente consolidado pelas jurisprudências internacionais, sobretudo pelo já debatido caso *Nicaragua*, através da análise de seus dois principais pilares: o conceito de força e o princípio da não intervenção que, no mais das vezes, são analisados sob uma relação de predominância de um em relação a outro.

Para a primeira corrente, calcada no escopo do conceito de força, pode-se destacar o entendimento de Oliver Dörr, que defende que o escopo de proteção da referida obrigação é construído através da interpretação sistemática da Carta da ONU, sobretudo cotejando o artigo 2º com os arts. 44 e 51 e com o preâmbulo da Carta. Para o celebrado doutrinador, existiria uma razão própria por trás da utilização do termo “força” pela Carta da ONU em coadunação com o conceito de força armada ou mesmo militar. Isso seria, ainda, confirmado pelos *preparatory works* do próprio tratado, em que os representantes dos Estados rejeitaram

[93] INTERNATIONAL COURT OF JUSTICE*.* ***Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)****,* Merits, Judgment. In: ICJ Reports 14, 1986, The Hague, Netherlands, §§187–190; INTERNATIONAL COURT OF JUSTICE**.** ***Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory****,* Advisory Opinion. In: ICJ Reports 136, 2004, The Hague, Netherlands, §87.

veementemente uma proposta brasileira de expandir o alcance da referida proibição às coerções de natureza puramente econômica.[94]

Em sentido similar, destaca-se o entendimento de Malcolm Shaw, que, analisando o artigo 51 sobre direito à auto defesa, conclui que, de fato, a própria Carta da ONU limitou o escopo da noção de força apenas a aqueles mediante ataques armados. Nada obstante, para este doutrinador, essa limitação não deve ser abusiva, devendo englobar, em verdade, qualquer ataque que produza efeitos cinéticos.[95]

Nesse supedâneo, a CIJ, no seu caso *Nicaragua*, dispôs que seria através dos denominados *"scale and effects"* que determinado ato seria, ou não, classificado como ataque armado e, em consequência, como violação da proibição do uso da força.[96]

Cabe ressaltar que essa linha de pensamento não visa, necessariamente, diminuir o escopo de proteção da vedação ao uso da força ao não considerar a violação aos elementos do princípio da não intervenção, (integridade territorial e independência política) como satisfatórios para a configuração de um ato transgressor. Na realidade, aqueles que defendem esta teoria pugnam que os termos "integridade territorial" e "independência política" são meramente a explicitação de parte dos "Propósitos das Nações Unidas".[97] Esse raciocínio acabaria por expandir as possibilidades em que se poderia constatar a existência da violação à vedação ao uso da força, apesar de condicionado à verificação da existência de um ataque armado, cuja constatação é, via de regra, aferida pela presença de *scales and effects* de cunho cinético.

Outra abordagem sobre a presente discussão foca nos quesitos constitutivos do princípio da não intervenção. Para essa corrente, o enfoque concedido não deve ser no meio ou instrumento que ocasionou a violação do uso da força, mas sim

---

[94] DÖRR, Oliver. **Use of Force, Prohibition of.** Max Planck Encyclopedia of Public International Law, Oxford, 2015.
[95] SHAW, Malcolm. International Law. 7 ed. Cambridge: Cambridge University Press, 2014.
[96] INTERNATIONAL COURT OF JUSTICE. ***Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)***, Merits, Judgment. In: ICJ Reports 14, 1986, The Hague, Netherlands.
[97] DÖRR, Oliver. **Use of Force, Prohibition of.** Max Planck Encyclopedia of Public International Law, Oxford, 2015.

quais são os direitos estatais que, uma vez violados, acarretariam na configuração da transgressão da referida obrigação sob comento.[98]

Para essa visão, os elementos moduladores dessa acepção se encontram dispostos no art.2 (4) da Carta da ONU: a integridade territorial e a independência política dos Estados, ambos os elementos diretamente ligados à manifestação da soberania do ente estatal.

Dessa forma, há, aqui, a proposta de uma interpretação evolutiva, e mesmo teleológica, do disposto pela Carta da ONU no seu art. 2 (4).

Essa visão é particularmente relevante quando se analisa o dilema que cerca os chamados ataques cibernéticos.

Como já pontuado, a primeira corrente defende a relação indispensável entre ataques armados e efeitos cinéticos para que se configure o uso da força. Nada obstante, quando transplantado esse raciocínio para o mundo cibernético, percebe-se a sua inadequação, visto que, via de regra, raramente um ataque cibernético acaba por gerar efeitos cinéticos. Ademais, mesmo verificados, ainda haveria a necessidade de se analisar os *scales and effects* exigidos pela CIJ, diante dos quais meros danos físicos a CPUs dificilmente satisfariam tal critério.

De forma diversa, um sistema normativo baseado na verificação da existência de violação de um dos elementos constitutivos do princípio da não intervenção contribuiria para a desnecessidade dessa análise, no mais das vezes, infrutífera e inócua no contexto cibernético. Isso se dá porque, mesmo a doutrina mais afinada com os desenvolvimentos tecnológicos, ao qual este trabalho se alinha, admite que a mera destruição de dados não possui natureza cinética, o que afastaria a possibilidade de classificação dessa medida claramente ofensiva como uso da força.[99] Destarte, ataques que afetem a confidencialidade, a integridade e a

---

[98] BLAY, Samuel K N. **Territorial Integrity and Political Independence.** Max Planck Encyclopedia of Public International Law, Oxford, 2010.

[99] ZIOLKOWSKI, Katharina. General Principles of International Law as Applicable in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. p. 173. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017; SCHMITT N., Michael. Cyber Activities and the Law of Countermeasure In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013, p. 681. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 14 ago 2017.

disponibilização de serviços de computador são poderiam ser tachados como violações ao uso da força.[100]

Nada obstante, apesar do confronto dessas duas teorias, pode-se vislumbrar uma conjugação ente ambas, especialmente para lidar com a questão dos ataques cibernéticos.

Como cediço, as técnicas interpretativas mais recorrentes dos tratados se encontram dispostas na Convenção de Viena sobre o Direito dos Tratados, que possuem, como elemento de similitude, a observância ao princípio da contemporaneidade, que prescreve que determinado tratado deve ser interpretado de acordo com a vontade das partes ao momento de sua conclusão.[101] Entretanto, existe uma técnica interpretativa de alta relevância, que não está codificada na CVDT, mas que possui forte natureza costumeira.[102]

Esse método, chamado de interpretação evolutiva, aplicado de forma mais efetivo a tratados-normativos, tal qual a Carta da ONU, tem como principal característica ser uma exceção clara ao princípio da contemporaneidade.

Destarte, essa técnica prescreve que, para a melhor aplicação e perenidade das normas internacionais, em consonância com o desenvolvimento da comunidade internacional, há a possibilidade de interpretar determinada norma de um tratado sob as condições vigentes ao momento de sua aplicação, fazendo do processo hermenêutico internacional uma atividade não estática e totalmente rígida.[103]

Para que se efetue tal interpretação, a CIJ determinou que devessem ser seguidas duas fases de raciocínio.[104]

Primeiramente, deve ser analisado se, de fato, determinado termo ou previsão do tratado pode ser interpretado à luz das circunstâncias no tempo de sua aplicação,

---

[100] KASTENBERG, Joshua. **Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law**. Air Force Law Review, Washington D.C., Vol. 64, 2009, p. 55.

[101] AUST, Anthony. **Modern Treaty Law and Practice**. 3 ed. Cambridge: Cambridge University Press, 2013.

[102] COSTA, Filipe Gomes Dias; BENN, Verônica Lúcia Hassler. A codificação das normas costumeiras: a interpretação evolutiva no Direito Internacional. **Anais do Congresso Brasileiro de Direito Internacional**, Fortaleza, Vol. 13, 2015, pp. 10-12. Disponível em: <https://uol.unifor.br/oul/conteudosite/F7319182015071708102133018 1/COSTA_BENN_%20A%20codificacao%20de%20normas%20costumeiras%20-%20a%20interpre.pdf> Acessado em: 15 ago. 2017.

[103] É com base nessa técnica que o escopo de proteção do direito à privacidade que, pelos termos do Pacto Internacional de Direitos Civis e Políticos se aplica às "correspondências" abarca, também, as mensagens instantâneas e os *e-mails*.

[104] INGAKI, Osamu. Evolutionary Interpretation of Treaties Re-examined: The Two Stage Reasoning. **Journal of International Cooperation Studies**, Kōbe, Vol. 22, No. 2-3, 2015, p. 134.

e não no período de sua conclusão. Para tanto, observa-se a intenção original das partes refletida nos termos dos tratados, a partir da qual um tratado pode ser interpretado à luz das condições do período da sua aplicação, se as partes assim o desejaram no momento de sua conclusão. Pode-se, ainda, presumir tal intenção a partir da existência de termos genéricos no tratado, mediante os quais as partes aceitaram que o tratado pode evoluir.[105]

Outro mecanismo para apurar a viabilidade da interpretação evolutiva se foca no objeto e propósito do tratado. Essa visão, carregada de elementos teleológicos, considera que mesmo se o termo não refletir a vontade original das partes, ele pode ser interpretado de modo evolutivo de forma que permita a realização efetiva do objeto e do propósito do tratado, o que justificaria a não aplicação do princípio da contemporaneidade ao escolher determinado termo.[106]

No segundo passo do raciocínio de aplicação da interpretação evolutiva, há a apuração da forma como determinado termo evoluiu ao longo do tempo até resultar no entendimento atual conferido a ele. Dessa forma, nessa segunda etapa o termo é analisado à luz das circunstâncias legais e factuais contemporâneas à sua aplicação, por meio da obrigatoriedade da interpretação de boa-fé prevista na CVDT em seu art. 31 (3) (b); do desenvolvimento do direito internacional; e da mudança do significado de termos sob o contexto das novas dinâmicas travadas pela comunidade internacional em suas relações interestatais e também da sociedade como um todo.

Aplicando essa técnica à discussão aqui estudada, denota-se a viabilidade desse processo hermenêutico ao conceito de “força”, sobretudo, através do desenvolvimento do que se denomina o termo “armado” para a comunidade internacional.

De início, cumpre observar que, nos *preparatory works* da Carta da ONU, em que se pode visualizar a intenção dos Estados-partes, a escolha do termo armado foi, de fato, proposital para excluir ações de natureza econômica. Dessa forma, em verdade, a ausência de referência ao contexto cibernético deriva diretamente do fato que inexistia qualquer prática estatal de ataques cibernéticos.

---

[105] Verifica-se essa posição em decisões da CIJ, como no caso *Aegean Sea* e mesmo no Órgão de Resolução de Controvérsisas da OMC no caso United States – Import Prohibition of Certain Shrimp and Shrimp Products.

[106] Essa segunda abordagem foi adotada pelo Corte Permanente de Arbitragem no caso *Iron Rhine*, sendo recorrente em suas decisões.

Ademais conforme se depreende da leitura do preâmbulo da Carta da ONU, compõem os pilares fundamentais da própria Nações Unidas a paz e a estabilidade internacional. Ora, considerando que o princípio da não intervenção derivado do art. 2(4) da Carta da ONU compreende dois dos mais importantes elementos de manifestação da soberania estatal, torna-se viável a compreensão de que ataques que iriam de encontro ao princípio da não intervenção atingiriam, mesmo com graus variados, o objeto e propósito da Carta da ONU, validando a interpretação evolutiva nessa seara.

Tratando-se da evolução dos temos “armed” e “force” dispostos ao longo da Carta da ONU, vale pontuar que a própria CIJ em sua Opinião Consultiva *Legality of the Threat or Use of Nuclear Weapons* de 1996, posteriormente ao caso *Nicaragua*, determinou que a verificação do uso da força e da noção de força armada independe do meio utilizado.[107] Nesse sentido, o próprio *Tallinn Manual* dispõe que determinado ataque cibernético se enquadra no escopo de ataque armado mediante a análise do grau e natureza da violação a partir dos danos causados e do objetivo central da operação cibernética, havendo, aqui, uma visão repaginada do conceito de *“scales and effects”* prescrito pelo caso *Nicaragua.*

Destarte, os termos “armado” e “força”, encontrados em diversos momentos da Carta da ONU e evocados pelos defensores da primeira corrente aqui apresentada como modulador do escopo de proteção ao uso da força, da qual se origina a necessidade de observância de efeitos cinéticos, estaria sujeito a essa técnica interpretativa no sentido de incluir em seus conceitos os ataques realizados pela via cibernética.

Finalmente, é possível notar que, analisando a questão sob o viés cibernético, é plenamente cabível compreender a existência de uma violação ao uso da força por meio de operações conduzidas através do ciberespaço, seja porque elas violam o princípio da não intervenção, seja porque a interpretação evolutiva expandiu o conceito dos termos “força” e “armado” para incluir os ataques cibernéticos.

3.3.2 Uso de ciberestruturas e o dever de devido cuidado

A obrigação de devido cuidado, ou *due diligence,* é um tipo obrigacional de meio, na qual a verificação do regular cumprimento dessa obrigação prestacional se

[107] INTERNATIONAL COURT OF JUSTICE. ***Legality of the Threat or Use of Nuclear Weapons***, Advisory Opinion. In: ICJ Report 226, 1996, The Hague, Netherlands, §39.

dá pela atestação de que o sujeito obrigado adotou determinada conduta que se comprometeu a tomar, servindo, assim, de contraponto à chamada obrigação de resultado.

Esse instituto deriva do desenvolvimento europeu acerca da teoria civilista da responsabilização, sobretudo no que tange aos deveres resultantes da responsabilização objetiva, em que obrigações, como a de vigia, guarda e prevenção, ganharam espaço a partir da consolidação da teoria do risco. Entretanto, conforme ocorre com os institutos do Direito Interno que são transplantados para o Direito Internacional, há certas modificações dessas noções típicas de Direito Civil dignas de nota.

Aplicado à seara do direito internacional, em especial nas relações interestatais, esse tipo obrigacional tem sido entendido como um princípio geral do direito, validando, assim, a possibilidade de que obrigações internacionais prescrevam a obrigatoriedade de observância a determinada conduta que, por sua vez, teria seus planos de execução incumbidos ou ao setor governamental responsável ou, em alguns casos, ao agente público encarregado.[108]

Independentemente, seja devido a um ato estatal ou um ato de terceiros que estejam sob o alcance de sua jurisdição, o cometimento de um ato em contrário a uma obrigação de devido cuidado ativa os mecanismos de responsabilização internacional dos Estados para se verificar, a priori, se o Estado em questão incorreu em atos de negligência ou que, de qualquer outra forma, indique um descaso no cumprimento da obrigação de devido cuidado.[109]

Vale notar que, devido à natureza dessa obrigação, há uma amplificação da importância dos atos de entes privados praticados sob a jurisdição do Estado titular, uma vez que, o *due diligence* compreende também atos de entes não estatais contra a finalidade da obrigação de devido cuidado para que se constate, em termos práticos, indícios de negligência estatal diante de uma obrigação de devido cuidado.

A Corte Internacional de Justiça sedimentou bem essa noção no seu caso *Tehran Hostages*, em que determinou a responsabilização do Irã por violação de obrigações de proteção diplomáticas de natureza de devido cuidado, por, devido à

---

[108] INTERNATIONAL LAW ASSOCIATION. International Law Association Study Group on Due Diligence in International Law. **First Report.** [S.l.], 2014. Disponível em: <https://perma.cc/WX88-SBDX> Acessado em: 18 ago. 2017.

[109] KOIVUROVA, Timo. **Due Diligence.** Max Planck Encyclopedia of Public International Law, Oxford, 2010.

sua negligência ou falta de cuidado, ter falhado em proteger a embaixada americana de ataques de indivíduos.[110]

Ademais, tratando da natureza dessa obrigação, vale asseverar a principal diferença para a práxis internacional de responsabilização no que se refere ao tipo de obrigação analisada: Enquanto que a violação da obrigação de resultado se dá diretamente pela análise se determinado ato ou não ato constitui uma transgressão ao que foi pactuado, violações de obrigações de devido cuidado se dão pela depuração da conduta tomada pelo Estado, independentemente da ocorrência do ato que tal obrigação busca prevenir, sendo o cometimento do ato em si mero indício para que se analise a retidão da conduta estatal.

No mesmo sentido, por ser uma obrigação de meio, distingue-se também da mera obrigação de prevenir. É que o *due diligence* seria o dever de agir com apropriado zelo demandado pela situação. Assim, para que se configure o cumprimento dessa obrigação, basta verificar se o Estado foi atencioso em sua conduta. Dessa forma, a violação da obrigação de *due diligence* diz respeito à falha do Estado em tomar as atitudes para evitar o evento indesejado, não importando se, de fato, o resultado ocorreu. [111] De forma diversa, a obrigação de prevenir requer a ocorrência do evento para ser considerada violada. Assim, a mera falha do Estado em tomar as atitudes necessárias para prevenir o ato não resulta na violação dessa obrigação. De outra forma, ocorrendo o evento, o Estado será responsabilizado, mesmo que tenha tomado as devidas medidas de prevenção, visto que a obrigação de prevenir é de resultado.

Mais notadamente, a principal obrigação de devido cuidado é o dever de natureza costumeiro de não causar dano transfronteiriço, ou *no harm rule,* cuja concepção se desenvolveu a partir do direito internacional ambiental e se expandiu para as demais áreas do direito internacional.[112] Inclusive, alguns doutrinadores entendem que é essa concepção, oriunda do caso arbitral *Trail Smelter* entre EUA e Canadá, que dá origem à obrigação de devido cuidado no direito internacional. Em 1939, nessa arbitragem de suma importância para a evolução e modernização do

---

[110] INTERNATIONAL COURT OF JUSTICE. ***United States Diplomatic and Consular Staff in Tehran***, Judgment. In: ICJ Reports 3, 1980, The Hague, Netherlands.

[111] MAZZESCHI, Riccardo Pisillo. The Due Diligence Rule and the Nature of the International Responsibility of States. **German Yearbook of International Law**, Kiel, Vol. 35, No. 9, 1992, pp. 46-49.

[112] GARVEY, Jack I. Toward a Reformulation of International Refugee Law. **Harvard International Law Journal**, Cambridge, Vol. 26, 1985, pp. 483-495.

direito internacional, cunhou-se o que hoje é denominado *Trail Smelter Rule* ou *Trail Smelter Clause* que, via de regra, consubstancia a essência de todas as obrigações de devido cuidado do direito internacional a partir da noção de soberania, estendendo-se além do certame restrito do direito internacional ambiental:

> under the principles of international law, as well as the law of the United States, no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence.[113]

Inspirando-se nesse preceito, o *Tallinn Manual* em sua regra 5 determina uma obrigação de devido cuidado sobre as ciberestruturas estatais:

> Rule 5 – Control of cyber infrastructure
> A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.[114]

Conforme já pontuado aqui neste estudo, essa regra foi elaborada com o intuito de abarcar quaisquer atos internacionalmente ilícitos em si próprios ou, que de outra forma, ocasionem um dano a outros entes estatais.

Todavia, houve uma falta de consenso acerca da caracterização dessa regra no que diz respeito ao seu escopo de aplicação. Nessa seara, destacam-se como pontos de controvérsia existentes nas discussões do grupo de experts responsável pelo *Manual*: ***i)*** se tal regra seria aplicável apenas às operações cibernéticas que

[113] "De acordo com os princípios do direito internacional e também com o direito norte-americano, nenhum Estado tem o direito de utilizar ou permitir o uso de seu território com vistas a causar danos através de gases poluentes nos territórios de outro Estado ou de propriedades e pessoas alheias, em casos que se tenham consequências severas e sejam estabelecidos por evidências claras e convincentes." (Tradução livre).
[114] "Regra 5 – Controle sobre ciberestruturas. Um Estado não deverá, conscientemente, permitir que sua ciberestrutura, localizada em seu território ou sob o seu exclusivo controle governamental seja utilizada para a consecução de atos que adversamente e ilegalmente afetem outros Estados." (Tradução livre)

estão sendo de fato conduzidas ou também incidiria sobre os atos que indiquem uma mera probabilidade de ocorrerem; ***ii)*** qual a abordagem a ser adotada a respeito do grau de conhecimento esperado do Estado sobre os atos, e se haveria a possibilidade de aplicação da teoria construtivista, a saber, da noção de que o Estado, em certa medida, detém a obrigação de ter ciência da ocorrência de determinados atos sob sua jurisdição e; ***iii)*** se a referida regra seria aplicável apenas a operações cibernéticas travadas no território do Estado ou também se estariam abarcados aquelas atividades meramente roteadas através da ciberestrutura estatal.

Destarte, ciente dessas considerações e desentendimentos ao momento da elaboração da primeira versão do *Tallinn Manual*, o *Tallinn Manual 2.0* possui como um dos seus principais pontos de desenvolvimento o regramento acerca da obrigação de devido cuidado, oportunidade em que propõe uma evolução da regra 5 do *Tallinn Manual* original na figura de sua nova regra 6, devidamente intitulada de *due diligence:*

> Rule 6 – Due Diligence (general principle)
> A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.[115]

Ademais, complementarmente, houve a criação da Regra 7, em que o *Tallinn Manual 2.0* detalha quais são as medidas que os Estados devem tomar em relação a suas ciberestruturas para estarem em conformidade com a norma geral de devido cuidado da Regra 6:

> Rule 7 – Compliance with the due diligence principle
> The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end

[115] "Regra 6 – Devido Cuidado (princípio geral). Um Estado exercerá devido cuidado não permitindo que seu território ou território ou ciberestrutura sob o seu controle governamental seja utilizado para operações cibernéticas que afetem os direitos ou produzam graves consequências adversas para outros Estados." (Tradução livre)

> to cyber operations that affect a right of, and produce serious adverse consequences for, other States.[116]

Esse sistema normativo, mais desenvolvido sobre a matéria, visa, também, encerrar as principais controvérsias existentes à época do Manual original. Nesse sentido, o *Tallinn Manual 2.0* dispõe que:

i) A regra 7 é plenamente aplicável a operações cibernéticas que ainda não foram lançadas, incluindo-se os atos preparatórios que estão sendo tomados e que a partir dos quais o Estado pode razoavelmente concluir que uma operação cibernética ilícita será, de fato, executada. Para ilustrar essa questão, o grupo de experts propõe um caso em que uma agência de inteligência estatal se infiltra em um fórum online fechado, usado por determinado grupo terrorista, baseado no território do Estado. Durante suas investigações, essa agência descobre que esse grupo terrorista instalou um *malware* destrutivo na estrutura cibernética de uma bolsa de ações de outro Estado, e que está sob a iminência de ser ativado. Nessa situação, o sistema normativo proposto pelo *Tallinn Manual 2.0* determina que o Estado em cujo território tal grupo terrorista está baseado deverá impedir e punir essa operação cibernética devido à alta probabilidade de causar dano trasnfronteiriço, de acordo com a chamada *Trail Smelter Rule e a no harm rule.*

ii) Debruçando-se mais uma vez sobre a questão da aplicação da teoria construtivista, o grupo de experts, dessa vez, chegou ao consenso de que o novo escopo da regra 6 inclui a possibilidade de responsabilizar um Estado por falhar em agir com devido cuidado em circunstâncias factuais em que o Estado deveria, objetivamente, ter ciência que seu território e, em especial, suas estruturas governamentais, estavam sendo utilizadas para operações cibernéticas transgressoras. Dessa forma, uma miríade de fatores pode influenciar a verificação dessa presunção de conhecimento por parte do Estado. Incialmente, o fato de que determinado ataque se valeu diretamente da estrutura cibernética governamental praticamente sacramenta a aplicação da teoria construtivista nesse caso concreto.[117] Similarmente, facilita-se a aplicação dessa teoria quando se tratar de *malwares* ou

---

[116] "Regra 7 – Observância do princípio do devido cuidado. O princípio do devido cuidado exige que o Estado tome todas as medidas exequíveis para combater e encerrar operações cibernéticas que afetem o direito de outros Estados ou produzam graves consequências adversas para eles." (Tradução livre).

[117] INTERNATIONAL COURT OF JUSTICE. ***Corfu Channel case***, Merits, Judgment. In: ICJ Reports 4, 1949, The Hague, Netherlands, p. 44 (Separate Opinion of Judge Alvarez).

vulnerabilidades de conhecimento público, a exemplo da brecha *Heartbleed*[118] além de ataques DDoS, facilmente identificados a partir do aumento drástico de uso de banda. Nada obstante, essa teoria é modulada pelas circunstâncias de cada Estado, sobretudo no que se refere ao seu desenvolvimento tecnológico, sendo impossível, via de regra, exigir o mesmo patamar construtivista de responsabilização objetiva de um país com um poderio cibernético como os Estados Unidos e de outro com efetivamente nenhum investimento na área, como é o caso da maioria dos Estados africanos.

iii) Em seu comentário à Regra 6, o *Tallinn Manual 2.0* o grupo de experts propõe a discussão acerca da existência de um dever de devido cuidado de um Estado pela qual há apenas o trânsito de dados, através de cabos de fibra ótica, muitas vezes submarinos. Nesse quesito, os experts concluíram que existe, realmente, a obrigação de devido cuidado dos Estados de trânsito quando suas ciberestruturas funcionam como caminhos ou *proxies* para determinada operação cibernética.[119] Destarte, de acordo com a Regra 7, se esse Estado possuir conhecimento acerca da operação, incluindo-se, aqui, a noção da teoria construtivista, e poder tomar medidas exequíveis para extinguir efetivamente essas operações, ele será considerado titular da obrigação de devido cuidado, a partir da qual poderá ser responsabilizado internacionalmente por atos que se valham de sua ciberestrutura governamental.

Pode-se observar que a comunidade internacional tem tido um cuidado especial com o dever de devido cuidado no contexto cibernético, sendo objeto de intensos estudos dos mais renomados doutrinadores e visto como saída jurídica para combater a atual impunidade internacional de atos cometidos no ou pelo espaço cibernético. Michael Schmitt, organizador das duas versões do *Tallinn Manual* e líder do grupo de experts responsável por tais trabalhos, elucida que o *due diligence* aplicado ao contexto cibernético é, em verdade, um mecanismo jurídico

---

[118] *Bug* recorrente em idos de 2014 em sites utilizadores dos protocolos de segurança SSL e TLS, criados a partir do famoso *software* OpenSSL, a partir do qual é possível ter acesso a dados privados dos usuários a partir de uma interceptação do tráfego de dados existente a partir da conexão do usuário a determinado site que usasse o OpenSSL.

[119] SCHMITT, Michael N. **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, New York: Cambridge University Press, 2017.

extremamente importante para garantir o respeito à soberania dos Estados e ativar o sistema de responsabilização estatal por atos internacionalmente ilícitos.[120]

Entretanto, em que pese o *Taillinn Manual 2.0* proponha uma discussão bastante apurada sobre o tema, essa questão ainda não foi plenamente ou formalmente aceita pelos Estados, os sujeitos por excelência do direito internacional. Isto posto, o debate sobre a abordagem proposta pelo grupo de experts ainda terá que passar pelo crivo da prática estatal para que possa, por ventura, constituir um costume internacional sobre a matéria, vez que a constituição do *opinio juris* não parece ser o principal desafio diante do extenso e contínuo trabalho realizado pelo Centro de Excelência da OTAN para Cooperação em Defesa Cibernética.

[120] SCHMITT, Michael N. **In Defense of Due Diligence in Cyberspace**. The Yale Law Journal Forum, New Haven, 2005. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/SchmittDueDiligence.pdf> Acessado em: 19 ago. 2017.

4. O DIREITO PROBATÓRIO NO CONTEXTO INTERNACIONAL

4.1 O DIREITO PROCESSUAL E AS CORTES INTERNACIONAIS

Um dos fenômenos mais marcantes do Direito Internacional contemporâneo é o que os doutrinadores têm denominado de fragmentação do Direito Internacional.

Essa fragmentação consiste nos efeitos de desuniformização jurídica advinda da diferente abordagem concedida pela grande miríade de cortes internacionais sobre aspectos concorrentes sob os quais, por mais das vezes, possuem, também, jurisdições concorrentes.[121]

Tal fenômeno é mais bem identificado a partir da análise, primeiro, dos diferentes tipos de tribunais internacionais, no que diz respeito ao seu ânimo de permanência e sua competência material e segundo, das regras processuais adotadas por esses tribunais, sobretudo no que diz respeito à práxis probatória, assim como da elaboração de decisões e do valor concedido às práticas processuais de suas jurisprudências.

De início, pode-se observar que as cortes internacionais constituem ou tribunais permanentes, ou cortes *ad hoc* criadas para julgar determinado incidente internacional. Compõem as principais cortes permanentes a Corte Internacional de Justiça, o Tribunal Penal Internacional, o Tribunal Internacional sobre o Direito do Mar, concebido através da Convenção de Montego Bay, e as cortes de direitos humanos dos sistemas regionais, tais qual a Corte Europeia de Direitos Humanos e a Corte Interamericana de Direitos Humanos. Do lado dos tribunais *ad hoc,* destacam-se o Tribunal Penal Internacional Para a Antiga Iugoslávia,[122] o Tribunal Penal Internacional para Ruanda[123] e o Tribunal Especial para o Líbano[124].

Preliminarmente, cumpre observar que a natureza de um tribunal não altera a executabilidade de suas decisões no cenário internacional, tampouco atenua a força de sua jurisprudência como força motriz da evolução do direito internacional[125] ou cria uma hierarquia entre as diversas cortes.

---

[121] WEBB, Philippa. **International Judicial Integration and Fragmentation**. 1 ed. Oxford: Oxford University Press, 2013, p. 141.
[122] Criado pela Resolução do Conselho de Segurança 827 de 1993.
[123] Estabelecido através do Conselho de Segurança por meio de sua Resolução 955 de 1994.
[124] Instituído em 2007 pelo Conselho de Segurança através da Resolução 1757.
[125] Nesse sentido, cumpre destacar o advento do Teste de Controle Geral pela Câmara de Apelação do TPIAI.

Nada obstante, apesar de não figurar como objeto central deste estudo, vale asseverar que a proliferação de tribunais *ad hoc,* sobretudo os de natureza penal, não está imune às críticas dos processualistas internacionais no que diz respeito à violação ao princípio de vedação ao tribunal de exceção, visto que tais cortes foram constituídas posteriormente ao cometimento do ato dito ilícito.[126]

Outra característica particular desses tribunais é o seu caráter necessariamente temporário que, por sua vez, contribuem para a instabilidade da uniformização da jurisprudência internacional.

A prática internacional, lidando com questões como genocídio, imunidades e uso da força tem demonstrado que a natureza permanente de um tribunal contribui diretamente para uma relativa integração, em oposição à existente fragmentação do direito internacional, muito devido à tradição e autoridade que cortes como a CIJ já possui e que o TPI vem adquirindo. Nesse sentido, pode-se encontrar elementos de integração entre as duas cortes, como, por exemplo, na abordagem conferida pelo TPI nos casos *Lubanga* e *Katanga* no que diz respeito à conceituação e classificação de conflito armado, alinhando-se com o posicionamento da CIJ no caso *Armed Activities on the Territory of Congo.*[127]

Em sentido inverso, enquanto que o grau de permanência confere estabilidade e integração ao direito internacional, os tribunais *ad hoc* contribuem para a inovação, visão crítica e, como resultado, fragmentação do direito internacional. Pode-se destacar, nesse sentido, a abordagem conflitante do TPIAI no que diz respeito aos testes de controle com a jurisprudência da CIJ, já alvo de discussão neste trabalho.[128]

Ressalta-se, entretanto, que outro principal elemento que denota o fenômeno de fragmentação é a existência de normas processuais diferentes para cada tribunal, calcadas, primordialmente, nas disposições de seus Estatutos constitutivos.

De forma geral, devido à descentralização inerente do direito internacional diante da falta de um poder soberano superior, não existe um regramento uniforme

---

[126] Nesse sentido, Hugh Thirlway em seu estudo comparativo da CIJ com os demais tribunais internacionais.

[127] INTERNATIONAL CRIMINAL COURT. **The Prosecutor v. Thomas Lubanga Dyilo**, ICC-01/04-01/06, 2012, The Hague, Netherlands; INTERNATIONAL CRIMINAL COURT. **The Prosecutor v. Germain Katanga**, ICC-01/04-01/07, 2014, The Hague, Netherlands.

[128] INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA. **Prosecutor v. Duško Tadic, Appeal against Conviction** , ICTY Case No. IT-94-1- A, Appeals Chamber, 1999, The Hague, Netherlands.

de natureza processual que todas as cortes internacionais devem seguir nem um tratado internacional com função de “código de processo internacional”.

Dessa forma, cada Corte internacional é regida no que se refere às suas normas processuais pelo qual disposto no seu Estatuto e, na maioria das vezes, supletivamente, pelo *Rules of the Court,* instrumento concebido pelo próprio tribunal, mediante autorização expressa de seu Estatuto, para detalhar com mais minúcia, aspectos procedimentais. Verifica-se, ainda, a utilização de práticas pretéritas dos referidos tribunais em suas decisões anteriores como mecanismo de garantir uma uniformidade no que diz respeito ao desenvolvimento do processo judicial dentro da própria dinâmica da corte.[129]

Entretanto, essa forma de aplicação das normas processuais realça, ainda mais, a fragmentação do direito internacional, uma vez que cada tribunal internacional possui um conjunto normativo próprio acerca das regras processuais cabíveis, inibindo a intercalação de entendimentos jurisprudenciais entre as cortes, mesmo no aspecto material, visto que, por exemplo, um mesmo fato pode ser tratado de formas diferentes no que se refere à valoração probatória e, por consequência, ocasionar entendimentos discrepantes no que se refere ao direito material.

Apesar desse cenário, pode-se identificar na prática das cortes internacionais e mesmo nas cortes nacionais, a identificação de princípios gerais do direito de natureza processual que devem ser respeitados enquanto fontes do direito internacional de acordo com o art. 38 do Estatuto da Corte Internacional de Justiça, que, por sua vez, é amplamente utilizado por todo o direito internacional como indicativo do que constitui uma determinada norma aplicável no cenário internacional.[130]

Dessa forma, identificam-se nos julgados de cortes como a CIJ, O Tribunal do Mar, da Corte Europeia de Direitos Humanos a existência de princípios comuns de natureza processual, tal qual o respeito ao princípio ao contraditório, à paridade de armas, o princípio da vedação do *ultra petita* e da *res judicata,* ou coisa julgada. Vale destacar, também, que esses princípios podem ainda serem observados em sede de

---

[129] É justamente devido a esse posicionamento que o *Corfu Channel,* primeiro caso da CIJ, é, até hoje, um dos principais casos do Tribunal de Haia, uma vez que foi nele que muitas bases processuais foram primeiramente delineadas.

[130] ZIMMERMANN, Andreas; OELLERS-FRAHM, Karin; TOMUSCHAT, Christian; TAMS, Christian J. **The Statute of the International Court of Justice: A Commentary**, 2 ed., Oxford: Oxford University Press, 2012, pp. 874-876.

julgados de tribunais *ad hoc*, demonstrando, assim, uma mínima interconexão entre as cortes internacionais, respeitando, evidentemente, o contexto que eles estão inseridos, seja diante da sua natureza de tribunal penal, seja pelo seu grau de permanência, ou mesmo órgão judiciário vinculado a um tratado.

Nesse supedâneo, apesar do fenômeno atual de fragmentação do direito internacional, ainda mais amplificado na seara processual, é possível encontrar círculos concêntricos de entendimento no que diz respeito ao tratamento do processo judicial nas cortes internacionais.

Esse aspecto é especialmente constatado no que diz respeito aos princípios que circundam a prática probatória nas cortes internacionais. De forma geral, percebe-se que as jurisprudências dos órgãos judiciários internacionais, que não possuem natureza penal, adotam uma abordagem bastante similar a respeito da prova, qual seja a existência de liberalidade do tratamento da atividade probatória. Esse comportamento pode ser verificado no caso *Nicaragua,* em que a CIJ, por meio do *principle of free assessment of evidence* dispôs que "dentro dos limites de seu Estauto e das *Rules of the Court,* a Corte possui liberdade na valoração dos diversos elementos de prova."[131] Vale ressaltar, no entanto que, tratando-se de tribunais penais, essa liberalidade é restringida por disposições expressas em seus estatutos, que possuem normas detalhadas sobre a produção e valoração da prova.[132]

No que se refere ao direito probatório nas principais cortes permanentes, percebe-se que o processo de admissão probatória é fortemente inspirado pelos procedimentos do *civil law*, havendo uma prevalência da prova escrita em detrimento daquela fornecida pela forma oral.[133] Devido à essa inspiração, nota-se, também, uma tendência de se evitar uma abordagem restritiva no que se refere a admissibilidade da prova, sobretudo no que tange a licitude da sua origem.

Tratando dessa questão, no caso *Corfu Channel* (Reino Unido v. Albânia) a corte foi provocada para analisar a admissibilidade de provas baseadas na licitude de sua origem. No caso em questão, o Reino Unido conduzira operações de dragagem de minas submarinas nas águas territoriais da Albânia no Canal de Corfu

---

[131] INTERNATIONAL COURT OF JUSTICE. ***Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)****,* Merits, Judgment. In: ICJ Reports 14, 1986, The Hague, Netherlands, §60.

[132] WOLFRUM, Rudger; MOLDNER, Mirka**. International Courts and Tribunals, Evidence**. Max Planck Encyclopedia of Public International Law, Oxford, 2013.

[133] BROWN, Chester. **A Common Law of International Adjudication**, 1 ed. Oxford: Oxford University Press, 2007, pp. 90-92.

mesmo diante de protestos albaneses de que tais operações violariam a sua soberania. O Reino Unido justificou suas ações com base em um suposto direito de um Estado de assegurar a posse de provas localizadas no território de um outro Estado para submetê-las a um processo judicial internacional, reforçando, assim, o arcabouço probatório disponível para essa corte. Nada obstante, ao analisar tal questão, a Corte verificou que, de fato, o Reino Unido violou a soberania albanesa, mas, sem maiores detalhamentos, admitiu a prova apresentada pelos britânicos.[134]

Dessa decisão, extraem-se diversos entendimentos na doutrina buscando entender o motivo por trás da admissibilidade das provas em questão.

Uma primeira visão diz respeito ao fato de que a Albânia, em nenhum momento, questionou a admissibilidade das provas apresentadas pelo governo do Reino Unido, gerando uma espécie de consentimento do governo balcânico no que diz respeito ao uso das referidas provas.

Outra visão baseia-se no fato de que a Corte não considerou a origem ilícita das provas como motivo suficiente para exclui-la do arcabouço probatório disponível para a prolação da decisão.

De qualquer forma, as duas visões comprovam que, de fato, o tratamento conferido à prova no direito internacional se reveste de uma liberalidade marcante o que pode se tornar um empecilho diante das particularidades do espaço cibernético.[135]

Sobre o ônus da prova, percebe-se a prática internacional da aplicação do princípio do *onus probandi incumbit actori*, próprio do modelo adversarial, adotado pela grande maioria das cortes internacionais. Destarte, o ônus de provar determinado fato está com a parte que o alegou, inexistindo, assim, qualquer ônus pré-constituído em favor do *applicant* ou do *respondent*.[136]

Apesar desse princípio, devido à já tão comentada liberalidade das cortes internacionais no que diz respeito ao tratamento da prova, é plenamente viável a

---

[134] INTERNATIONAL COURT OF JUSTICE. ***Corfu Channel case***, Merits, Judgment. In: ICJ Reports 4, 1949, The Hague, Netherlands, p. 22.

[135] Nesse sentido, SPECIAL TRIBUNAL FOR LEBANON. **Decision on the Admissibility of Documents Published on the Wikileaks Website (The Prosecutor v. Salim Jamil Ayyash, Mustafa Amine Badreddine, Hassan Habib Merhi, Hussein Hassan Oneissi, Assad Hassan Sabra)**, STL-11-01/T/TC, 2015, The Hague, Netherlands, em que documentos vazados pelo Wikileaks foram utilizados pela defesa sob o protesto da procuradoria da defesa. Ao final, decidiu-se pela inadimissão dos referidos documentos.

[136] Além de casos da CIJ como do *Temple of Preah Vihear, Genocide e Pulp mills,* pode-se identificar a aplicação desse princípio até mesmo em decisões da OMC, como no caso U*nited States—Measure Affecting Imports of Woven Wool Shirts and Blouses from India.*

inversão do ônus da prova, que, via de regra, é realizada por meio da análise da natureza do que está sendo alegado baseado na gravidade da acusação.[137]

A partir dessa abordagem, surge, então, a relativização da atividade probatória e da sua valoração, sobretudo através da aplicabilidade da chamada evidência circunstancial.

4.2 O NÍVEL PROBATÓRIO NA CORTE INTERNACIONAL DE JUSTIÇA

Em sintonia com os demais tribunais internacionais de natureza não penal, a Corte Internacional de Justiça não possui em seu Estatuto ou *Rules of the Court* normas específicas sobre o procedimento a ser utilizado para a valoração probatória.

Esse silêncio é confirmado ao longo dos principais casos da Corte em que houve a necessidade de abordagem direta a respeito do peso a ser conferido a determinados elementos prova sobre um fato em questão integrante da lide. Nesse sentido, observa-se a atitude da CIJ de adotar uma postura de análise secundária acerca dos fundamentos por trás de determinada valoração probatória. Dessa forma, é possível identificar termos ao longo de sua jurisprudência como *convincing evidence, conclusive evidence* e mesmo *balance of evidence,* denotando, assim, uma ausência de maior uniformidade terminológica sobre qual o nível probatório a ser adotado.[138] Entretanto, a doutrina assinala que, em termos práticos, a utilização desses termos resultou na adoção de um nível probatório nos casos em que foram evocados com flagrantes similitudes com o grau probatório de *clear and convicing evidence*, aplicado pelas cortes dos Estados Unidos.[139] Essa abordagem é mais comum nas hipóteses em que a essência principal do julgamento não está sob discussão.

Em que pese a Corte não possua uma abordagem consistente acerca do nível probatório utilizado de forma geral, pode-se identificar, ao longo dos julgados do Tribunal de Haia a atribuição do nível probatório aplicado utilizando como

---

[137] INTERNATIONAL COURT OF JUSTICE. **Ahmadou Sadio Diallo (Republic of Guinea v. Democratic Republic of the Congo)**, Merits, Judgment. In: ICJ Reports 639, 2010, The Hague, Netherlands, p. 21, § 54

[138] ZIMMERMANN, Andreas; OELLERS-FRAHM, Karin; TOMUSCHAT, Christian; TAMS, Christian J. **The Statute of the International Court of Justice: A Commentary**, 2 ed., Oxford: Oxford University Press, 2012, p. 1237.

[139] TEITELBAUM, Ruth. Recent Fact-Finding Developments at the International Court of Justice. **The Law & Practice of International Courts and Tribunals**, [S.l.], Vol. 6, No. 1, 2007, pp. 119–58.

parâmetro determinante a violação da obrigação internacional discutida, em contraponto com o entendimento mais recorrente dos tribunais nacionais, sobretudo os de cultura de *civil law,* que possuem como principais elementos determinantes da atividade valorativa a natureza dos fatos alegados.

Nos precedentes da CIJ, tal fenômeno destaca-se no julgado acerca do *Bosnian Genocide* de 2015, em que a Corte esclareceu que, devido às alegações e violação de obrigações previstas na Convenção de Prevenção ao Genocídio, em especial a de não cometer genocídio em si, haveria a necessidade de utilização de elementos probatórios *fully conclusive*, imbuídos, em verdade, de uma exigência probatória extremadamente próxima do nível probatório de *beyond reasonable doubt*, sendo vistos, por alguns doutrinadores, como apenas um só padrão de abordagem.[140] Esse entendimento da CIJ aplicou de forma mais explícita uma abordagem passível de ser identificada já no *Corfu* Channel, o primeiro litígio submetido à Corte, quando tratando de violações do uso da força.[141] Dessas decisões depreende-se a imposição de um nível probatório mais rígido quando tratando de *exceptional gravity*. Incluem-se, aqui, violações de normas cogentes, os *jus cogens,* outras graves violações de direitos humanos e também violações da obrigação de não utilização da força.[142]

Mais marcadamente, o caso *Corfu Channel* possui maior relevância no quesito probatório devido à utilização da chamada evidência circunstancial.

Essa técnica valorativa é consequência direta da inviabilidade de uma das partes do litígio de produzir evidências que satisfaçam os graus probatórios de *beyond reasonable doubt* ou de *clear and convicing evidence,* podendo, ainda recorrer a inferências ou provas indiretas que, consideradas em conjunto dentro de um mesmo contexto (circunstância) possuem poderes probatórios sobre determinada matérias. Nesse sentido, a CIJ prescreveu que:

> the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility. Such a

[140] INTERNATIONAL COURT OF JUSTICE. **Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v. Serbia)**, Judgment. In: ICJ Reports 3, 2015, The Hague, Netherlands.
[141] INTERNATIONAL COURT OF JUSTICE. ***Corfu Channel case***, Merits, Judgment. In: ICJ Reports 4, 1949, The Hague, Netherlands.
[142] WOLFRUM, Rudger; MOLDNER, Mirka**. International Courts and Tribunals, Evidence**. Max Planck Encyclopedia of Public International Law, Oxford, 2013.

> State should be allowed a more liberal recourse to inferences of fact and circumstantial evidence. This indirect evidence is admitted in all systems of law, and its use is recognised by international decisions.[143]

Todavia, a Corte asseverou que os fatos a serem utilizados para fins de inferência não podem falhar em cumprir o nível probatório de *beyond reasonable doubt* por si próprios.[144]

Nota-se nesse julgado a admissão da prova circunstancial como princípio geral do direito de natureza processual, devido à sua constatação como técnica probatória utilizada em todos os sistemas jurídicos nacionais e, ainda, por outras cortes internacionais.

Dessa forma, podemos identificar três principais níveis probatórios utilizados pela Corte Internacional de Justiça, que, via de regra, seguem o padrão da natureza do que está sendo alegado para determinar sua utilização: ***i)*** *clear and convicing evidence,* método valorativo usado de forma mais generalista, sobretudo para fatos que não compõem o núcleo duro da fundamentação, ***ii)*** *beyond reasonable doubt*, para fatores que versem sobre violações de obrigações de extrema gravidade, de forma geral e também para elementos factuais que integram a essência da *ratio decidendi* ou e ***iii)*** provas circunstanciais, nível probatório adotado quando se verifica a inviabilidade da produção de provas por uma das partes se aplicado os outros níveis probatórios elencados.

4.3. A VALORAÇÃO PROBATÓRIA E O ESPAÇO CIBERNÉTICO

Indubitavelmente, o maior desfaio da aplicação do sistema normativo ao espaço cibernético debatido aqui neste trabalho diz respeito às consequências da instituição dos níveis probatórios das cortes internacionais, discutidos previamente.

---

[143] "A vítima de uma violação de direito internacional, na maioria das vezes, é incapaz de produzir prova de fatos ensejadores de responsalização interncaional. Esse Estado deve ser autorizado a recorrer a um método mais liberal através de inferências factuais e evidências circunstanciais. Tais provas indiretas são admitidas em todos os sistemas jurídicos, e suas utilizações são também reconhecidas por decisões internacionais." (Tradução livre).

[144] INTERNATIONAL COURT OF JUSTICE. ***Corfu Channel case***, Merits, Judgment. In: ICJ Reports 4, 1949, The Hague, Netherlands.

Isso se dá, pois o ciberespaço é repleto de fatores e elementos extremamente técnicos, que, somado à possibilidade de se atingir relativo anonimato nos ataques.

Diante disso, pode-se verificar o surgimento de um novo tipo de prova perante as cortes internacionais além das já recorrentes provas documentais, testemunhais, produzidas por experts ou pronunciamentos oficiais estatais: a prova digital. A principal característica dessa prova diz respeito à possibilidade de reunir elementos de identificação, armazenamento e análises de dados digitais que posteriormente, serão convertidos em relatórios para melhor acessibilidade valorativa.[145] Vale notar que esse tipo de prova, em si, difere da mera prova documental, visto que requer, devido à sua complexidade e tecnicidade, a interpretação de um forense da área que será encarregado de produzir o relatório final. Evidentemente, essa particularidade pode, por si só, gerar conflitos entre as partes, no que diz respeito à interpretação dos dados compilados, forçando o órgão jurisdicional, no mais das vezes, a nomear um expert independente para produzir um novo relatório.

Embora a prática internacional dos Estados tenha sido de conceder o mesmo poder probatório à prova digital ou eletrônica àquela concedida às provas ditas "físicas",[146] sua aplicação perante os padrões valorativos das cortes internacionais, sobretudo da CIJ se mostra desafiadora, uma vez que, via de regra, tais cortes aplicam o nível probatório da *clear and convicing evidence* ou da *beyond reasonable doubt.* A origem desse questionamento deriva da prática internacional de tratar das questões de atribuição com maior cautela e, de certo modo, hesitação, amplificado justamente quando se abarca o enigmático espaço cibernético.

Desde as primeiras discussões acerca do ciberespaço, mantém-se, ainda hoje, um dos principais dilemas que o permeia quando se trata de operações cibernéticas: a determinação da identidade ou da localização dos ofensores ou de seus intermediários. Esse impasse põe em xeque o verdadeiro propósito da produção de provas perante um tribunal, qual seja o esclarecimento dos fatos e a identificação dos agentes envolvidos.

---

[145] PRESIDENCY OF THE COUNCIL OF MINISTERS,. **National Strategic Framework for Cyberspace Security**, [S.l.], 2013. Disponível em: <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/ uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf>. Acessado em: 19 ago. 2017.

[146] UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Comprehensive Study on Cybercrime: Draft— February 2013, XXIV**, [S.l.], 2013. Disponível em: <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/ CYBERCRIME_STUDY_210213.pdf>. Acessado em: 19 ago. 2017.

O ciberespaço possui, dessa forma, diversos mecanismos de ilidir a possibilidade de se conseguir uma *clear and convicing evidence* e um potencial considerável para gerar uma dúvida razoável e, assim, erodir qualquer tentativa de se ter um fato provado *beyond reasonable doubt*. Marcadamente, a atual arquitetura da internet e das demais conexões possuem diversas brechas e lacunas para mascarar um usuário e sua localização, assim como inteiros servidores e fluxos de pacote de dados. Além disso, há, ainda, a possibilidade de um *hacker* "sequestrar" uma CPU pertencente a alguém inocente e ignorante desse controle remoto, para utilizá-lo como base para efetuar ataques cibernéticos.[147] Em todos esses casos, técnicas como o mero rastreamento são infrutíferas para a consecução de uma prova capaz de encerrar as discussões factuais de um caso judicial.

Predominantemente, a principal atividade forense digital é o rastreamento do endereço IP, identificador existente em qualquer computador em uma sessão em redes ou *online.* Um pacote de dados IP é o elemento mais básico e recorrente na transmissão de dados na internet, ele é formado por dois principais componentes: o *header,* que contém informações sobre a fonte, o destino, o status e a fragmentação do dado em questão, e o *payload,* onde se encontra os dados transmitidos em si.[148] Como principais formas de inutilizar as principais técnicas forenses de rastreamento de IP ou *back-tracking*, tem-se a utilização de servidores *proxies,* Redes Virtuais Privadas, ou VPNs, e a utilização de "Roteadores cebolas" ou *Onion Routers*, como forma de atingir o quase total anonimato na rede.

Os servidores *proxies* funcionam como intermediários entre o usuário e o servidor que ele quer, de fato, acessar na rede. Devido a essa função, esse sistema é capaz de esconder o IP de seus usuários através do direcionamento de todo o tráfego de informações por meio de outro servidor, que ficará encarregado de interagir com o servidor ou rede que o usuário quer acessar.[149] Dessa forma, o

---

[147] GEIß, Robin; LAHMANN, Henning. Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat Prevention. In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 19 ago 2017.

[148] PIHELGAS, Mauno. Back-Tracking and Anonymity in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017.

[149] PIHELGAS, Mauno. Back-Tracking and Anonymity in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International**

servidor *proxy* interage com a rede desejada, expondo o seu próprio IP e repassa o resultado dessa operação ao usuário, que, tecnicamente, não travou qualquer relação com a rede final. Dessa forma, tentativas de rastreamento do IP resultarão na identificação do *proxy*, e apenas dele, possibilitando a segurança, privacidade e, consequentemente, anonimato do usuário. Essa estrutura, apesar de mais rudimentar, já é capaz de ocultar a identidade do usuário, ou, pelo menos, dificultar o trabalho de rastreamento.

Outra ferramenta bastante utilizada são os servidores VPN ou Redes Privadas Virtuais. Seu funcionamento consiste em um aprimoramento dos servidores *proxies.* De forma geral, os VPN criptografam os dados que se originam dos usuários, canalizam-nos para um servidor em outra localidade e, só então, esses dados são transmitidos para o servidor que se quer originalmente acessar. Existem hoje diversos serviços pagos de VPN que se pode contratar para os mais diversos fins. Destacam-se em polos opostos, os serviços existentes nos tribunais e outros órgãos judiciais que possibilitam aos seus usuários o acesso remoto ao sistema interno do órgão por meio do computador pessoal do usuário, localizado em sua casa, e a utilização de VPN com IP de determinados países para poder burlar bloqueios regionais instituídos por certos jogos de computador e sites a alguns países.

Por fim, como aperfeiçoamento substancial ao padrão estabelecido pelos servidores *proxies*, foi criado em idos de 2006, pelo Laboratório de Pesquisa da Marinha Americana, com o propósito de proteger informações governamentais, o hoje lendário Tor, *The Onion Router*. Esse programa constitui na criação de uma rede anônima de comunicação através de uma multiplicidade de servidores *proxies,* públicos e privados que conduzem os dados de forma aleatória, através de uma rota também aleatória, entre o usuário e o seu servidor de destino.[150]

Por exemplo, o Computador pessoal N, quer acessar o site www.camaro.com.br através de um *onion router.* Esse *onion router* é composto dos servidores *proxies* 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12. Dessa forma, a comunicação do PC N com o site em questão pode ser realizado pelo uso de uma combinação

---

Relations and Diplomacy, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017.

[150] THE TOR PROJECT. **Tor: Overview**. [S.l.], [S.d.] Disponível em: <https://www.torproject.org/about/overview.html.en#overview>. Acessado em: 19 ago. 2017.

aleatória dessa rede. Assim, os dados oriundos do PC N podem transitar na ida pelos *proxies* 3, 6, 9, 1 e 11, e na volta pelos *proxies* 8, 5, 2, 9, 3 e 12, escolhidos de forma randômica. Dessa forma, cada servidor desse funciona como uma camada de uma cebola, que deve ser retirada, uma a uma, apara que se chegue ao seu centro. Além disso, assim com uma cebola esse sistema de informação permite que cada camada, ou servidor, apenas interaja com as camadas ou servidores adjacentes, criando, assim, uma barreira de proteção ao centro da cebola, ou no caso do Tor, ao seu usuário.

Definitivamente, o Tor foi um dos principais catalizadores do anonimato na internet, responsável, mesmo que indiretamente, pela proliferação da chamada *deepweb*, parcela da internet acessível apenas por meio do Tor e seus similares, e infestada de páginas obscuras e controversas, em que se pode contratar um assassino profissional anonimamente[151], ou mesmo encomendar drogas ilícitas.[152]

Além das técnicas aqui brevemente analisadas, existem inúmeras outras que ainda não são de conhecimento público, que podem comprometer por completo qualquer tentativa de uma parte de produzir uma prova conclusiva acerca de uma operação cibernética. Ademais, apesar de todo o desenvolvimento tecnológico na área de defesa cibernética, indiscutivelmente aqueles que usam o ciberespaço para fins escusos tem demostrado ter uma vantagem considerável no que esse refere à possibilidade de esconder sua identidade, ou mesmo forjar dados para incriminar outros sujeitos.

[151] SANKIN, Aaron. Searching for a hitman in the Deep Web. **The Daily Dot.** [S.l.], 10 out 2013. Disponível em: <https://www.dailydot.com/crime/deep-web-murder-assassination-contract-killer/>. Acessado em: 19 ago. 2017.

[152] A exemplo do famoso site Silk Road, mercado negro anônimo de drogas ilícitas, hoje desativado pelo governo americano.

5 MECANISMOS DE COMBATE À IMPUNIDADE ESTATAL NO CIBERESPAÇO

5.1 AMPLIAÇÃO DO ESCOPO DA OBRIGAÇÃO DE DEVIDO CUIDADO

Ao momento da feitura do *Tallinn Manual,* o alcance da obrigação de devido cuidado estava condicionado à necessidade de que determinada operação cibernética indevida ocorresse através da estrutura cibernética estatal.[153] Essa abordagem restritiva por natureza do grupo de experts se enquadrava no contexto à época da confecção da primeira versão do Manual, realizada, em verdade, como resposta aos incidentes ocorridos anos antes na Estônia, Geórgia e Irã. Devido a isso, suas disposições tinham como principal enfoque a responsabilização de atos em que a presença e a intervenção estatal eram claramente identificadas, fazendo do dever de devido cuidado uma espécie de obrigação subsidiaria a ser aplicada quando a responsabilização pela violação da vedação ao uso da força fosse inviável.

A esse sistema normativo, enquadrava-se o inevitável uso do teste de controle efetivo,[154] por meio da qual o ato de particulares só seria atribuído ao Estado na circunstância de dependência delineada pela CIJ no caso *Nicaragua,* ou seja, mediante a comprovação do direcionamento estatal da conduta desse ente privado através de sua observância a instruções específicas para a consecução de dado objetivo.[155]

Destarte, devido a esse tratamento, pode-se concluir que o *Tallinn Manual* possuiu como principal finalidade normatizar as hipóteses em que o Estado age explicitamente, mediante operações cibernéticas, contra outro sujeito de direito internacional, o que justifica o seu enfoque substancial no enquadramento da obrigação de vedação do uso da força ao contexto cibernético e análise em segundo plano do dever de devido cuidado.

Inobstante, atualmente, após a primeira grande onda de ataques cibernéticos estatais da qual se resultou a criação do Manual, verifica-se que, cada vez mais, são entes privados que conduzem as principais operações cibernéticas internacionalmente ilícitas, o que gera uma já certa obsolescência das normas do

---

[153] SCHMITT, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warfare**, New York: Cambridge University Press, 2013.
[154] Aplicação do effective control no TM original
[155] INTERNATIONAL COURT OF JUSTICE. ***Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)***, Merits, Judgment. In: ICJ Reports 14, 1986, The Hague, Netherlands, p. 54, §115.

Manual, voltadas, primordialmente, para a responsabilização de ataques cibernéticos conduzidos pelo próprio Estado.

Como principal exemplo, neste ano de 2017 ocorreram ataques cibernéticos mundiais simultâneos utilizando o *ransomware WannaCry,* por meio dos quais dados de importantes empresas e organizações governamentais de diversos países foram criptografados por agentes externos, que exigiam um "resgate" em *bitcoins* para que realizassem a descriptografia, tudo sob a ameaça iminente de que os dados "sequestrados" fossem apagados.[156] O Centro Nacional de Segurança Cibernética do Reino Unido (GHCQ)[157], a Agência de Segurança Nacional dos Estados Unidos (NSA)[158] e empresas privadas especializadas em segurança digital, como a Kaspersky e a Symantec[159] apontam o grupo *hacker Lazarus*[160] como o responsável por esse ataque, e também pelo que acometeu a Sony em meados de 2014[161]. Segundo essas entidades, o *Lazarus* possui relações próximas com a Coréia do Norte, que se encarregava de subsidiar o grupo e facilitar suas operações.

Ora, se aplicado o sistema de normas proposto pelo *Tallinn Manual* original, verificar-se-ia a inviabilidade de responsabilização do Estado norte-coreano por atos internacionalmente ilícitos atos, seja através de alegações de uma eventual violação da vedação do uso da força, ou seja, pela acusação de falha em cumprir com dever de devido cuidado.

Como cediço, para a existência de um ato internacionalmente ilícito, faz-se necessário a atribuição desse ato a um Estado e que o ato em questão constitua

---

[156] PANKOV, Nikolay. WannaCry: o que você precisa saber. **Kaspersky Lab**. [S.l.], 17 mai 2017. Disponível em: <https://www.kaspersky.com.br/blog/wannacry-for-b2b/7324/> Acessado em: 20 ago 2017.

[157] HERN, Alex; MACASKILL, Ewen. WannaCry ransomware attack 'linked to North Korea'. **The Guardian.** [S.l.], 16 jun 2017. Disponível em: <https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group> Acessado em: 20 ago. 2017.

[158] NAKASHIMA, Ellen. The NSA has linked the WannaCry computer worm to North Korea. **The Washington Post**. [S.l.], 14 jun 2017. Disponível em: <https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.d6ba86d1583f> Acessado em: 20 ago 2017.

[159] SOLON, Olivia. WannaCry ransomware has links to North Korea, cybersecurity experts say. **The Guardian.** San Francisco, 15 mai 2017. Disponível em: <https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group> Acessado em: 20 ago. 2017.

[160] GREAT. Lazarus Under the Hood. **Kaspersky Lab.** [S.l.], 03 abr 2017. Disponível em: <https://securelist.com/lazarus-under-the-hood/77908/> Acessado em: 20 ago. 2017.

[161] CORERA, Gordon. NHS cyber-attack was 'launched from North Korea'. **BBC.** [S.l.], 16 jun 2017. Disponível em: <http://www.bbc.com/news/technology-40297493> Acessado em 20 ago. 2017.

uma violação de um obrigação internacional desse Estado.[162] Em matéria de atribuição, conforme já exposto pela CIJ, o mero financiamento e o fornecimento de apoio logístico não constituem elementos suficientes para satisfazer o teste de controle efetivo e, consequentemente, efetuar atribuição dos atos de dado ente privado ao Estado.[163] Seguindo essa linha de pensamento, altamente majoritária no direito internacional público,[164] mesmo que provada a relação em questão do *Lazarus* com a Coréia do Norte, o teor do suporte concedido não caracterizaria a atribuição dos atos cometidos por esse grupo ao estado norte coreano. Destarte, tentativas de enquadrar o país asiático em uma eventual violação da vedação ao uso da força restariam infrutíferas devido aos mecanismos utilizados pela comunidade internacional para fins de responsabilização estatal por atos internacionalmente ilícitos.

Alternativamente, a responsabilização da Coréia do Norte mediante a violação do dever de devido cuidado, conforme estipulado pelo *Tallinn Manual,* também não obteria maiores sucessos. Isso diz respeito à necessidade de comprovar o uso de ciberestruturas estatais com o aval estatal ou devido a negligencia do Estado coreano.[165] Consequentemente, pautando-se na interpretação da Trail Smelter clause e da *no harm rule* proposta pela primeira versão do Manual, a Coréia do Norte não seria titular de uma obrigação de devido cuidado no sentido de tomar as medidas exequíveis para evitar tais ataques afastando, mais uma vez, a existência de um ato internacionalmente ilícito.

Com situações desse tipo em mente, ao momento da elaboração do *Tallinn Manual 2.0* o grupo de experts decidiu pela ampliação do escopo da obrigação de devido cuidado*,* incluindo na obrigação de devido cuidado o dever de vigilância das operações cibernéticas conduzidas em seu território de forma geral,[166] distanciando-se, assim, do escopo reduzido original que apenas abarcava ataques cibernéticos conduzidos através de ciberestruturas governamentais.

---

[162] Como cediço, um ato internacionalmente ilícito é composto de dois elementos: atribuição do ato a um Estado e que esse ato seja um descumprimento de uma obrigação internacional desse Estado.
[163] INTERNATIONAL COURT OF JUSTICE. ***Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)***, Judgment. In: ICJ Reports 43, 2007, The Hague, Netherlands.
[164] Nesse sentido, os principais doutrinadores internacionalistas como Crawford, Shaw, Cassesse e Evans defendem essa visão.
[165] SCHMITT, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warfare**, New York: Cambridge University Press, 2013.
[166] SCHMITT, Michael N. **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, New York: Cambridge University Press, 2017.

Através desse sistema, o envolvimento da Coréia do Norte com o grupo *Lazarus* nos ataques em questão através do apoio geral e da permissão de uso do seu território como base de operações, cumpririam a determinação da regra 7 do *Tallinn Manual 2.0* que prescreve como que o dever de devido cuidado, ou *due diligence,* seria considerado como violado:

> Rule 7 – Compliance with the due diligence principle
> The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States.[167]

Assim sendo, a conduta da Coréia do Norte de negligência ou de aval consciente em relação às operações do *Lazarus* implicaria na sua responsabilização internacional por transgredir o dever de devido cuidado no que diz respeito à obrigação de natureza costumeira de impedir danos transfronteiriços, consubstanciada na *no harm rule* ou na *Trail Smelter Clause*, o que imbui de força vinculante a observância a esse determinado preceito.[168]

Por fim, vale asseverar que a construção dos mecanismos de aplicação do quanto disposto na arbitragem *Trail Smelter* e da *no harm rule* é contínua e influenciada pelo desenvolvimento e variações das relações interestatais travadas por meio do espaço cibernético. O aumento do uso de terceiros para operações escusas na última década implicou na nova redação encontrada no *Tallinn Manual 2.0,* o que comprova a constante e necessária atualização desses trabalhos para se manterem a par com o desenvolvimento tecnológico exponencial do ciberespaço e, assim, evitar a impunidade de Estados que se valem do espaço cibernético para gerar instabilidades na comunidade internacional.

5.2 DA NECESSIDADE DE MITIGAÇÃO DO NÍVEL PROBATÓRIO

[167] "Regra 7 – Observância do princípio do devido cuidado. O princípio do devido cuidado exige que o Estado tome todas as medidas exequíveis para combater e encerrar operações cibernéticas que afetem o direito de outros Estados ou produzam graves consequências adversas para eles." (Tradução livre).
[168] TRAIL SMELTER ARBITRAL TRIBUNAL. **Trail Smelter Arbitration (United States v. Canada)**, Decision of 16 April 1938 and 11 March 1941. In: RIAA Vol. III, 2006, Geneva, Switzerland.

Da análise da jurisprudência da Corte Internacional de Justiça, conforme objeto de estudo no capítulo 3, pode-se depreender a existência de três principais níveis valorativos da prova que a CIJ costuma adotar em seus julgamentos, dentre os quais destaca-se o padrão de exigência de *clear and convicing evidence.*

Todavia, a atividade probatória jurisdicional norteada por esse patamar de valoração tem sido mitigada pela própria CIJ quando barreiras são encontradas na própria produção das provas pelas partes, de acordo com o que foi determinado pela Corte no caso *Corfu Channel*. Diante desse cenário, traz-se à baila as denominadas provas circunstanciais, que, de acordo com o Juiz Padawi Pahsa, constituem fatos que, embora não forneçam provas imediatas da acusação, tornam as alegações em questão prováveis com o auxílio da fundamentação jurídica.[169] Percebe-se que a noção de provas circunstanciais guardam correlação próxima com o uso de inferências e presunções no direito, ambos elementos que a CIJ já se valeu para preencher lacunas probatórias[170]:

> It would be going too far for an international court to insist on direct and visual evidence and to refuse to admit, after reflection, a reasonable amount of human presumptions with a view to reaching that state of moral, human certainty with which, despite the risk of occasional errors, a court of justice must be content[171]

Assim, as provas circunstanciais constituem espécie de provas indiretas que, conjuntamente, são capazes de confirmar determinada inferência ou presunção conforme produto da própria lógica.[172]

Nesse supedâneo, cabe rememorar as dificuldades apresentadas no que se refere à produção probatória no cenário cibernético, em especial devido à dificuldade

---

[169] INTERNATIONAL COURT OF JUSTICE. ***Corfu Channel case***, Merits, Judgment. In: ICJ Reports 4, 1949, The Hague, Netherlands, p. 59 (Dissenting Opinion of Judge Pasha).
[170] INTERNATIONAL COURT OF JUSTICE. ***Corfu Channel case***, Merits, Judgment. In: ICJ Reports 4, 1949, The Hague, Netherlands, pp. 90-91 (Dissenting Opinion of Judge Azevedo).
[171] "Seria indevido que uma corte internacional insista em provas diretas e visuais e que se negasse a admitir, após reflexões, uma quantidade razoável de presunções humanas que visam atingir um patamar de moral e certeza humana que, apesar dos riscos de eventuais erros, uma corte judicial deve se contentar." (Tradução livre).
[172] FRANCK, Thomas M.; PROWS, Peter, The Role of Presumptions in International Tribunals, **The Law & Practice of International Courts and Tribunals**, [S.l.], Vol. 4, No. 2, 2005, p. 2013.

de se conseguir uma prova destituída de dúvidas acerca de seu poder pleno de convencimento, seja devido à possibilidade de burlar o rastreamento de IP, seja devido à abordagem de doutrinadores atinentes às questões cibernéticas de desconsiderar a presença de elementos de código-fonte como indicativos da autoria de determinado *malware* quando idênticos a *softwares* estatais*.* [173]

Destarte, o uso de provas circunstanciais se mostra bastante atraente e, ia de regra, necessária para a atividade probatória no cenário cibernético. Em verdade, os principais meios de prova disponíveis para eventuais partes acabam por se enquadrarem, naturalmente, na noção de prova indireta que, segundo a Corte, diz respeito às provas possíveis de serem produzidas sem violar o controle territorial exclusivo de outro Estado.[174] Ilustrando esse ponto, vale destacar o *Project Grey Goose,* trabalho produzido por experts independetes em resposta aos ataques à Geórgia em 2008, em que, através da análise de tráfego de dados, rastreamento de IP e elementos factuais diversos, como o motivo por trás da Guerra da Ossétia do Sul, determinaram que a Rússia teve um envolvimento direto com os ataques ora conduzidos.[175] Ademais, entidades como o Centro de Excelência da OTAN para Cooperação em Defesa Cibernética, e corporações como a Kaspersky, Symantec, McAfee forneceram relatórios técnicos cruciais para a melhor compreensão de ataques cibernéticos, a exemplo das operações que utilizaram o *Stuxnet* e o *WannaCry,* que se enquadram no contexto de prova circunstancial utilizado pela Corte Internacional de Justiça*.*[176]

Noutro giro, Estados já tem defendido e operacionalizado suas atividades defensivas cibernéticas pautadas na noção de prova circunstancial. Os Estados Unidos em resposta ao secretário geral da ONU, ao tratar das questões de segurança da rede, admitiu que a atribuição altamente confiável de agentes no ciberespaço é bastante improvável de ser atingida por completo, sendo imprescindível para a produção de provas mínimas a ampliação da cooperação

---

[173] ROWE, Neil C. Attribution of Cyber Warfare In: GREEN, James A. Green (ed.). **Cyber Warfare: A Multidisciplinary Analysis**, Routledge: New York, 2015.
[174] INTERNATIONAL COURT OF JUSTICE. ***Corfu Channel case***, Merits, Judgment. In: ICJ Reports 4, 1949, The Hague, Netherlands, p.18.
[175] PROJECT GREY GOOSE. **Project Grey Goose: Phase I Report**, [S.l.] 17 out 2008, Disponível em: <https://pt.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>. Acesso em: 04 ago. 2017.
[176] ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. **Texas International Law Journa**l, Austin, Vol. 50 No. 2, 2015. Disponível em: <http://ssrn.com/abstract=2611753> Acessado em: 23 ago. 2017.

transnacional.[177] Confirmando essa posição internamente, os EUA, através do Chefe do Comando Cibernético Americano, pontou que operações de mitigação e proteção podem ser tomadas mesmo quando não se sabe ao certo quem seria o responsável,[178] elucidando, ainda, que o direito internacional não requer expressamente que um Estado saiba *a priori* quem é o responsável por um ataque armado para que possa tomar as medidas necessárias para se defender de tal ataque.[179]

Igualmente, a própria dinâmica do ciberespaço ao longo das suas décadas de existência tem demonstrado que a ideia do senso comum de que o dilema da identificação de atos no ciberespaço será, eventualmente, resolvido pelos avanços tecnológicos seria uma falácia, visto que, cada vez mais, criam-se novas formas de burlar a atividade probatória determinante no espaço cibernético.[180]

---

[177] UNITED NATIONS SECRETARY GENERAL. **Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General**, 18 U.N. Doc. A/66/152, [S.l.] 15 Jul 2011.

[178] UNITED STATES SENATE. **Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command.** Washington D. C., 15 abr 2010. Disponível em: <https://epic.org/privacy/nsa/Alexander_04-15-10.pdf> Acessado em: 22 ago. 2017.

[179] UNITED STATES SENATE. **Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command.** Washington D. C., 11 mar 2014. Disponível em: <https://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf> Acessado em: 22 ago. 2017.

[180] GEIß, Robin; LAHMANN, Henning. Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat Prevention. In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 19 ago 2017.

6 CONCLUSÕES

O espaço cibernético propõe diversos desafios para o direito contemporâneo, sobretudo para o direito internacional, no que toca em especial o sistema de responsabilização internacional dos Estados.

Ao longo dos anos, cada vez mais o ciberespaço tem sido utilizado de forma indevida para conduzir atos ilícitos contra a estabilidade da comunidade internacional. Os episódios percebidos apenas pontualmente em outrora, como nos incidentes na Estônia, Geórgia e Irã, hoje adquirem feição totalmente global, tendo como mais recente exemplo o ataque que se utilizou do *ransomware WannaCry.* A essa escalada de ataques soma-se o aperfeiçoamento de técnicas de ocultação da identidade dos agentes, através, por exemplo, da sofisticação de instrumentos de burla do rastreamento de IP devido, hodiernamente, à criação dos *onion routers.*

Paralelamente, a comunidade internacional tem amadurecido os mecanismos já existentes de aplicação do direito internacional ao cenário cibernético enquanto não há um desenvolvimento de um projeto de codificação pluriestatal sobre o tema. Notadamente, houve uma redução significativa de defensores da ideia de que o ciberespaço constituiria um domínio público internacional próprio que dependeria da codificação específica de novas normas que, até serem elaboradas, implicaria em um cenário de *non-liquet*.

Contrariamente a essa ideia, constata-se a crescente concepção de que as normas gerais do direito internacional, sejam os princípios gerais do direito ou os costumes internacionais de caráter geral, incidiriam de forma plena no campo cibernético, formando, assim, um sistema mínimo de proteção baseado nos institutos fundamentais do Direito Internacional Público, como a soberania, a responsabilização estatal por atos internacionalmente ilícitos, a obrigação de não causar danos transfronteiriços e o princípio da não intervenção. Nesse sentido, imperioso o destaque do trabalho realizado pelo Centro de Excelência em Defesa Cibernética Cooperativa da OTAN na elaboração do *Tallinn Manual* em 2013 e do *Tallinn Manual 2.0* em 2017, verdadeiros pilares da atividade doutrinária internacionalista sobre o espaço cibernético.

Inobstante, mesmo diante dessa tentativa de adequação das normas já existentes, algumas posições clássicas do direito internacional acabam por implicar

em um cenário de impunidade não desejada, em especial quando analisado o sistema de responsabilização estatal por atos internacionalmente ilícitos.

Em um primeiro momento, tratando do elemento da atribuição do ato praticado por terceiros ao Estado, se pode concluir que, apesar do teste de controle geral ser bastante atrativo devido à sua baixa rigorosidade para fins de atribuição, a posição esmagadoramente majoritária no cenário internacional, traduzida nas decisões da Corte Internacional de Justiça, prega que o teste de controle geral é inadequado para a responsabilização internacional. Assim sendo, o teste de controle efetivo, embora mais rígido e, no mais das vezes, injusto diante de certas condições fáticas, deve ser o sistema aplicado aos atos cometidos através do ciberespaço, devendo a discussão sobre a redução de a atual impunidade ser transplantada para outros fatores da responsabilização internacional.

Como segundo elemento de um ato internacionalmente ilícito está a violação por um Estado de uma obrigação internacional sua. Neste ponto, com base nos trabalhos das duas versões do *Tallinn Manual,* mostram-se com importância eventuais violações da vedação do uso da força e do dever de devido cuidado.

A vedação do uso da força, aplicado ao cenário cibernético, possui certa controvérsia devido à abordagem tradicionalista da comunidade internacional de se exigir danos cinéticos para que se constate a existência da transgressão dessa obrigação. Nada obstante, de acordo com a leitura da Carta da ONU em seu artigo 2(4), conclui-se que uma abordagem mais adequada ao cenário cibernético é a que classifica como uso da força os atos que interferem na integridade territorial ou na independência política de determinado Estado, ambos elementos constitutivos do princípio da não intervenção. Alternativamente, propõe-se aqui, neste trabalho, uma interpretação evolutiva dos termos “armado” e “força”, utilizados pela corrente mais clássica como justificadores da exigência de danos cinéticos, para, assim, compreender, também, danos a estruturas cibernéticas, mesmo que apenas de natureza digital, como o apagamento ou alteração indevida de dados.

Noutro giro, o dever de devido cuidado, outrora relegado à posição de obrigação subsidiária da vedação do uso da força, vem ganhando importância como consequência da utilização do território de determinado Estado, com o consentimento desse, ou devido à sua negligência, para a condução de ataques cibernéticos. Nesse ponto, nota-se a principal evolução da segunda versão do *Tallinn Manual*, que agora busca atingir não apenas os ataques em que era evidente

a presença do Estado como articulador ou mesmo ator principal de atos internacionalmente ilícitos praticados no espaço cibernético. Isto posto, essa ampliação do escopo da obrigação de devido cuidado implicaria na efetiva responsabilização de Estados que dão guarida para grupos de criminosos cibernéticos cujos atos violam o dever de evitar o cometimento de danos trasnfronteiriços originados do território do Estado, de acordo com o preceito da *Trail Smelter Rule* e da *no harm rule.*

Outro importante ponto de discussão de quintessência importância, sobretudo para a viabilidade de um litígio buscando a responsabilização internacional de um Estado diz respeito à forma com que as cortes internacionais e em especial a Corte Internacional de Justiça, tratam de suas questões processuais, particularmente a respeito da valoração probatória. Sobre este tópico, conclui-se que a fragmentação das cortes internacionais pode resultar em diferentes abordagens processuais, sobretudo quando se compraram cortes internacionais por excelência, como a CIJ, com tribunais penais internacionais, sejam eles *ad hoc* ou não. De qualquer sorte, da análise das principais cortes internacionais é possível identificar uma tentativa de coerência no que diz respeito ao nível probatório adotado para que determinado ponto seja considerado provado, embora não haja, na maioria dos estatutos dos tribunais internacionais, nenhuma disposição determinando a utilização específica de um nível probatório em detrimento do outro.

No contexto da CIJ, os níveis probatórios de *clear and convicing evidence* e *beyond reasonable dobut* se mostram mais comuns na práxis desse órgão, sendo o primeiro nível probatório usado de forma mais generalista e o segundo para questões de graves acusações de direito internacional. Como terceiro caminho, há possibilidade de uso de provas circunstanciais, conforme admitido pela CIJ no caso *Corfu Channel* quando houver a inviabilidade jurídica de produção de provas que satisfaçam os níveis probatórios padrões.

Nesse sentido, devido às particularidades da produção de provas no espaço cibernético, torna-se inerentemente inviável a produção de um arcabouço probatório digital incontestável, visto que a efemeridade do ciberespaço faz com que tentativas de atribuição da autoria de ataques cibernéticos sejam facilmente ludibriadas por meio de adulterações e ocultamento de IP, uso de estruturas *botnet* ou mesmo uso proposital de IP alheio como forma de criar um laranja. Dessa forma, conclui-se que a consecução de uma prova cabal capaz de satisfazer os níveis probatórios

normalmente utilizados é virtualmente impossível quando se trata do espaço cibernético, devendo ser adotado o sistema de provas circunstanciais para permitir a valoração conjunta de elementos probatórios como relatórios de empresas de segurança ou órgãos independentes, rastreamentos de IP, indícios de autoria de *malwares* e inferências e presunções que, se analisados isoladamente, não possuiriam o condão de comprovar determinada operação.

Conclusivamente, embora o espaço cibernético não seja a última fronteira do desenvolvimento da humanidade, seus efeitos na sociedade internacional são indiscutíveis, muito devido ao seu desenvolvimento e complexidade de crescimento exponencial. Diante desse cenário, embora a confecção de um tratado multilateral sobre o tema seja uma medida atrativa, a necessidade de atualização do *Tallinn Manual* em menos de cinco anos demonstra que um trabalho de codificação sobre essa matéria seria inócuo ao longo prazo. Em verdade, o principal caminho que o direito internacional no espaço cibernético deveria trilhar é o do estabelecimento, a partir da prática dos Estados, de costumes internacionais específicos, capazes de se adequarem de forma mais efetiva às mudanças tecnológicas sem que se perdesse a essência de suas normas.

Destarte, a presente proposta de ampliar o escopo da proteção do dever de devido cuidado e de mitigar o nível probatório exigido em casos envolvendo o ciberespaço são apenas passos iniciais para a programação de um sistema normativo costumeiro capaz de atualizar o direito internacional ao mundo cibernético. Essa construção talvez seja o principal desafio doutrinário internacionalista do século XXI, que, assim como o funcionamento de um *onion router*, exigirá a transmissão de dados e informações entre diversas mentes pensantes ao redor do mundo para que, juntando cada parcela de estudo e ideias elaboradas, chegue-se ao pacote de normas capaz de deletar, ou, pelo menos colocar em quarentena, a impunidade estatal no ciberespaço.

REFERÊNCIAS

ACCIOLY, Hildebrando; SILVA, G. E. do Nascimento e; CASELLA, Paulo Borba. **Manual de Direito Internacional Público**. 20 ed. São Paulo: Saraiva, 2012.

ANZILOTTI, Dionisio. **Cours de Droit International**. Paris: Panthéon-Assas LGDJ, 1999.

APPELLATE BODY. **United States – Import Prohibition of Certain Shrimp and Shrimp Products**. In: Report of the Appellate body, WTO DS 58, 2005, Geneva, Switzerland.

ASADOVA, Nargiz. *Нам, русским за границей, иностранцы ни к чему*. **Echo of Moscow**, [S.l.], 05 mar. 2009. Disponível em: <http://echo.msk.ru/blog/n_asadova/576689-echo/>. Acesso em: 03 ago. 2017.

AUST, Anthony. **Modern Treaty Law and Practice**. 3 ed. Cambridge: Cambridge University Press, 2013.

BANNELIER-CHRISTAKIS, Karine. Cyber Diligence: A Low- Intensity Due Diligence Principle for Low-Intensity Cyber Operations?. **Baltic Yearbook of International Law**, [S.l.], Vol. 14, 2014. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2550913> Acessado em: 14 ago. 2017.

BLAY, Samuel K N. **Territorial Integrity and Political Independence.** Max Planck Encyclopedia of Public International Law, Oxford, 2010.

BODANSKY, Daniel. ***Non Liquet***. Max Planck Encyclopedia of Public International Law, Oxford, 2012.

BROWN, Chester. **A Common Law of International Adjudication**, 1 ed. Oxford: Oxford University Press, 2007.

BROWNLIE, Ian. **Principles of public international law**. 7 ed. Oxford: Oxford University Press, 2008.

CASSESE, Antonio. **International law**. 2 ed. Oxford: Oxford Univeristy Press, 2005.

COALSON, Robert. Behind the Estonia Cyberattacks. **Radio Free Europe/Radio Liberty**, [S.l.], 06 mar. 2009. Disponível em: <https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html>. Acesso em: 03 ago. 2017.

CORERA, Gordon. NHS cyber-attack was 'launched from North Korea'. **BBC.** [S.l.], 16 jun 2017. Disponível em: <http://www.bbc.com/news/technology-40297493> Acessado em 20 ago. 2017.

COSTA, Filipe Gomes Dias; BENN, Verônica Lúcia Hassler. A codificação das normas costumeiras: a interpretação evolutiva no Direito Internacional. **Anais do**

Congresso Brasileiro de Direito Internacional, Fortaleza, Vol. 13, 2015. Disponível em: <https://uol.unifor.br/oul/conteudosite/F73191820150717081021330181/COSTA_BENN_%20A%20codificacao%20de%20normas%20costumeiras%20-%20a%20interpre.pdf> Acessado em: 15 ago. 2017.

CRAWFORD, James. **Brownlie's Principles of Public International Law**. 8 ed. Oxford: Oxford University Press, 2012.

_____. **Chance, Order, Change: The Course of International Law**. 1 ed. The Hague: Hague Academy of International Law, 2014.

_____. ***State Responsibility*** **The General Part**. Cambridge: Cambridge University Press, 2014.

CZOSSECK, Christian. State Actors and their Proxies in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017.

DANCHEV, Dancho. Georgia President's web site under DDoS attack from Russian hackers. **Zero Day**, [S.l.], 22 jul. 2008. Disponível em: <http://www.zdnet.com/article/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers>. Acesso em: 03 ago. 2017.

DEEKS, Ashley. An International Legal Framework for Surveillance. **Virginia Journal of International Law**, Charlottesville, Vol. 55:2, 2015.

DÖRR, Oliver. **Use of Force, Prohibition of.** Max Planck Encyclopedia of Public International Law, Oxford, 2015.

DUPUY, Pierre-Marie. Part II Interpretation of Treaties, Evolutionary Interpretation of Treaties. In: **Between Memory and Prophecy. The Law of Treaties Beyond the Vienna Convention**. Oxford: Oxford University Press, 2011.

ESPINER, Tom. Georgia accuses Russia of coordinated cyberattack. **CNET**, [S.l.], 11 ago. 2008. Disponível em: <https://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/>. Acesso em: 03 ago. 2017.

EUROPEAN COURT OF HUMAN RIGHTS. **Decision On Admissibility Behrami and Behrami v. France and Saramati v. France, Germany and Norway.** Strasbourg, 12 fev. 1975. Disponível em: <http://hudoc.echr.coe.int/eng-press?i=003-2012546-2140039>. Acesso em 14 ago. 2017.

EVANS, Malcolm D. (ed.). **International law**. 4 ed. Oxford: Oxford University Press, 2014.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric. W32.Stuxnet Dossier Version 1.4, **Symantec Security Response**. [S.l.], fev 2011, Disponível em: <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>. Acesso em: 04 ago. 2017.

FLECK, Dieter. Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual. **Journal of Conflict & Security Law,** Oxford, Vol 18, No. 2, 2013.

FRANCE-NEW ZEALAND ARBITRATION TRIBUNAL. **Rainbow Warrior Affair (New Zealand v. France)**, Decision of 30 April 1990. In: RIAA Vol. XX, 2006, Geneva, Switzerland.

FRANCK, Thomas M.; PROWS, Peter, The Role of Presumptions in International Tribunals, **The Law & Practice of International Courts and Tribunals**, [S.l.], Vol. 4, No. 2, 2005.

GARVEY, Jack I. Toward a Reformulation of International Refugee Law. **Harvard International Law Journal**, Cambridge, Vol. 26, 1985.

GEIß, Robin; LAHMANN, Henning. Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat Prevention. In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 19 ago 2017.

GREAT. Lazarus Under the Hood. **Kaspersky Lab.** [S.l.], 03 abr 2017. Disponível em: <https://securelist.com/lazarus-under-the-hood/77908/> Acessado em: 20 ago. 2017.

HERN, Alex; MACASKILL, Ewen. WannaCry ransomware attack 'linked to North Korea'. **The Guardian.** [S.l.], 16 jun 2017. Disponível em: <https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group> Acessado em: 20 ago. 2017.

HOLANDA. Supreme Court of Netherlands. **The State of the Netherlands v. Hasan Nuhanović Case no. 12/03324, Judgment**. 2013, The Hague, Netherlands. Disponível em: <http://www.asser.nl/upload/documents/20130909T125927-Supreme%20Court%20Nuhanovic%20ENG.pdf>. Acesso em: 14 ago. 2017.

INGAKI, Osamu. Evolutionary Interpretation of Treaties Re-examined: The Two Stage Reasoning. **Journal of International Cooperation Studies**, Kōbe, Vol. 22, No. 2-3, 2015.

INTERNATIONAL COURT OF JUSTICE. ***Aegean Sea Continental Shelf***, Judgment. In: ICJ Reports 33, 1978, The Hague, Netherlands.

_____. ***Ahmadou Sadio Diallo (Republic of Guinea v. Democratic Republic of the Congo)***, Merits, Judgment. In: ICJ Reports 639, 2010, The Hague, Netherlands.

_____. ***Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)***, Judgment. In: ICJ Reports 43, 2007, The Hague, Netherlands.

_____. ***Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v. Serbia)***, Judgment. In: ICJ Reports 3, 2015, The Hague, Netherlands.

_____. ***Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)***, Judgment. In: ICJ Reports 168, 2005, The Hague, Netherlands.

_____. ***Case concerning the Temple of Preah Vihear (Cambodia v. Thailand)***, Merits, Judgment. In: ICJ Reports 6, 1962, The Hague, Netherlands.

_____. ***Corfu Channel case***, Merits, Judgment. In: ICJ Reports 4, 1949, The Hague, Netherlands.

_____. ***Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)***, Merits, Judgment. In: ICJ Reports 7, 1997, The Hague, Netherlands.

_____. ***Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory***, Advisory Opinion. In: ICJ Reports 136, 2004, The Hague, Netherlands.

_____. ***Legality of the Threat or Use of Nuclear Weapons,*** Advisory Opinion. In: ICJ Report 226, 1996, The Hague, Netherlands.

_____. ***Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)***, Merits, Judgment. In: ICJ Reports 14, 1986, The Hague, Netherlands.

_____. ***Rules of Court***, 1978, The Hague, Netherlands. Disponível em: <http://www.icj-cij.org/en/rules> Acessado em: 17 ago. 2017.

_____. ***United States Diplomatic and Consular Staff in Tehran***, Judgment. In: ICJ Reports 3, 1980, The Hague, Netherlands.

INTERNATIONAL CRIMINAL COURT. **The Prosecutor v. Germain Katanga**, ICC-01/04-01/07, 2014, The Hague, Netherlands.

_____. **The Prosecutor v. Thomas Lubanga Dyilo**, ICC-01/04-01/06, 2012, The Hague, Netherlands.

INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA. **Prosecutor v. Duško Tadic, Appeal against Conviction** , ICTY Case No. IT-94-1-A, Appeals Chamber, 1999, The Hague, Netherlands.

_____. **Prosecutor v. Duško Tadic**, ICTY Case No. IT-94-1- T, Trial Chamber, 1997, The Hague, Netherlands.

INTERNATIONAL LAW ASSOCIATION. International Law Association Study Group on Due Diligence in International Law. **First Report.** [S.l.], 2014. Disponível em: <https://perma.cc/WX88-SBDX> Acessado em: 18 ago. 2017.

INTERNATIONAL LAW COMMISSION. **Draft articles on the law of treaties with commentaries**. New York, 1966. Disponível em: <http://legal.un.org/ilc/texts/instruments/english/commentaries/1_1_1966.pdf>. Acesso em: 17 ago. 2017.

_____. **Draft Articles On The Responsibility Of International Organizations, With Commentaries**, Yearbook of the International Law Commission v. II, part 2, [S.l.], 2011.

_____. **Report of the Commission to the General Assembly on the work of its thirty-second session**, Yearbook of the International Law Commission v. II, part 2, [S.l] 1980.

JENNINGS, Sir Robert; WATTS, Sir Arthur. **Oppenheim's International Law Vol. 1: Peace**. 9 ed. Oxford: Oxford University Press, 2008.

KASTENBERG, Joshua. **Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law**. Air Force Law Review, Washington D.C., Vol. 64, 2009.

KEIZER, Gregg. Cyberattacks knock out Georgia's Internet presence. **Computer World**, [S.l.], 11 ago. 2008. Disponível em: <http://www.computerworld.com/article/2532289/cybercrime-hacking/cyberattacks-knock-out-georgia-s-internet-presence.html>. Acesso em: 03 ago. 2017.

KREBS, Brian. Report: Russian Hacker Forums Fueled Georgia Cyber Attacks. **The Washington Post**, [S.l.], 16 out. 2008. Disponível em: <http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html>. Acesso em: 03 ago. 2017.

KOIVUROVA, Timo. **Due Diligence.** Max Planck Encyclopedia of Public International Law, Oxford, 2010.

MARGULIES, Peter. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. Melbourne Journal of International Law, Melbourne, Vol. 14, No. 2, 2013.

MAZZUOLI, Valério de Oliveira. **Curso de direito internacional público**. 9 ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2015.

MAZZESCHI, Riccardo Pisillo. The Due Diligence Rule and the Nature of the International Responsibility of States. **German Yearbook of International Law**, Kiel, Vol. 35, No. 9, 1992.

MELLO, Celso D. de Albuquerque. **Curso de direito internacional público**. 15 ed. rev. e aum. Rio de Janeiro: Renovar, 2004.

NEWLY Nasty. **The Economist,** [S.l.], 24 mai. 2007. Disponível em: <https://www.economist.com/node/9228757>. Acesso em: 03 ago. 2017.

NAKASHIMA, Ellen. The NSA has linked the WannaCry computer worm to North Korea. **The Washington Post**. [S.l.], 14 jun 2017. Disponível em: <https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.d6ba86d1583f> Acessado em: 20 ago 2017.

O'CONNELL, Mary Ellen. Cyber Security without Cyber War. **Georgetown Journal of International Affairs**, Washington D.C., Vol. 17, 2012.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Carta da ONU**. São Francisco, 1945. Disponível em: <http://unicrio.org.br/img/CartadaONU_VersoInternet.pdf>. Acesso em: 10 ago. 2017.

_____. **Convenção de Viena sobre o direito dos tratados**. Viena, 1969. Disponível em: <http://www.cedin.com.br/wp-content/uploads/2014/05/Conven%C3%A7%C3%A3o-de-Viena-sobre-o-Direito-dos-Tratados-entre-Estados-e-Organiza%C3%A7%C3%B5es-Internacionais-ou-entre-Organiza%C3%A7%C3%B5es-Internacionais.pdf>. Acesso em: 17 ago. 2017.

_____. **Convenção das Nações Unidas sobre o Direito do Mar.** Montego Bay, 1982. Disponível em: <http://www.iea.usp.br/noticias/documentos/convencao-onu-mar> Acessado em: 08 ago. 2017.

_____. **Convention on International Civil Aviation**. Chicago, 1944. Disponível em: <https://www.icao.int/publications/Documents/7300_cons.pdf> Acessado em: 08 ago. 2017.

_____. **IV Geneva Convention Relative to the Protection of Civilian Persons in Time of War**. Geneva, 12 ago 1949. Disponível em: <http://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.33_GC-IV-EN.pdf> Acessado em: 15 ago. 2017.

PIRKER, Benedict. Territorial Sovereignty and Integrity and the Challenges of Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 14 ago 2017.

PERMANENT COURT OF ARBITRATION. **Award in the Arbitration regarding the Iron Rhine ("Ijzeren Rijn") Railway between the Kingdom of Belgium and the Kingdom of the Netherlands**, Decision of 24 May 2005, In: Report of International Arbitral Awards, Vol.27, 2005, The Hague, Netherlands.

PERMANENT COURT OF INTERNATIONAL JUSTICE. **The Case of the S. S. Lotus**. In: Publications of the Permanent Court of International Justice Series A. No. 10, 1927, The Hague, Netherlands.

PRESIDENCY OF THE COUNCIL OF MINISTERS. **National Strategic Framework for Cyberspace Security**, [S.l.], 2013. Disponível em: <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/ uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf>. Acessado em: 19 ago. 2017.

PIHELGAS, Mauno. Back-Tracking and Anonymity in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017.

PROJECT GREY GOOSE. **Project Grey Goose: Phase I Report**, [S.l.] 17 out 2008, Disponível em: <https://pt.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>. Acesso em: 04 ago. 2017.

PANKOV, Nikolay. WannaCry: o que você precisa saber. **Kaspersky Lab**. [S.l.], 17 mai 2017. Disponível em: <https://www.kaspersky.com.br/blog/wannacry-for-b2b/7324/> Acessado em: 20 ago 2017.

PORTELA, Paulo Henrique Gonçalves. **Direito internacional público e privado**. 3 ed. rev. ampl. e atual. Salvador: juspodivm, 2011, p. 706.

RAMOS, André de Carvalho. **Curso de direitos humanos**. 2 ed. rev., atual. e ampl. São Paulo: Saraiva, 2015.

RBN – Georgia CyberWarfare – 2 – Sat 16 00 East Coast, 20 00 GMT. **RBNExploit**, [S.l.], ago. 2008. Disponível em: <http://rbnexploit.blogspot.com.br/2008/08/rbn-georgia-cyberwarfare-2-sat-16-00.html>. Acesso em: 03 ago. 2017.

REZEK, José Francisco. **Direito internacional público**: curso elementar. 14 ed. rev., aum. e atual. São Paulo: Saraiva, 2013.

ROBERTSON, Jordan; RILEY, Michael. Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar. **Bloomberg**, [S.l.], 10 dez. 2014. Disponível em: <https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>. Acesso em: 03 ago. 2017.

ROHAN, Brian; PEARCE, Tim. Georgia says Russian hackers block govt websites. **Reuters**, [S.l.], 11 ago. 2011. Disponível em: <http://uk.reuters.com/article/us-georgia-ossetia-hackers-idUKLB2050320080811>. Acesso em: 03 ago. 2017.

ROSCINI, Marco. **Cyber Operations and the Use of Force in International Law**, 1 ed. Oxford: Oxford University Press, 2014.

_____. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. **Texas International Law Journa**l, Austin, Vol. 50 No. 2, 2015. Disponível em: <http://ssrn.com/abstract=2611753> Acessado em: 23 ago. 2017.

ROWE, Neil C. Attribution of Cyber Warfare In: GREEN, James A. Green (ed.). **Cyber Warfare: A Multidisciplinary Analysis**, Routledge: New York, 2015.

SANKIN, Aaron. Searching for a hitman in the Deep Web. **The Daily Dot.** [S.l.], 10 out 2013. Disponível em: <https://www.dailydot.com/crime/deep-web-murder-assassination-contract-killer/>. Acessado em: 19 ago. 2017.

SCHMITT N., Michael. Cyber Activities and the Law of Countermeasure In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 14 ago 2017.

_____. **In Defense of Due Diligence in Cyberspace**. The Yale Law Journal Forum, New Haven, 2005. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/SchmittDueDiligence.pdf> Acessado em: 19 ago. 2017.

_____. **Tallinn Manual on the International Law Applicable to Cyber Warfare**, New York: Cambridge University Press, 2013.

_____. **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, New York: Cambridge University Press, 2017.

SCHMITT, Michael N.; WATTS, Sean. Beyond State-Centrism: International Law and Non-state Actors in Cyberspace. **Journal of Conflict & Security Law,** Oxford, Vol. 21, No. 3, 2016.

SHAW, Malcolm. International Law. 7 ed. Cambridge: Cambridge University Press, 2014.

SOLON, Olivia. WannaCry ransomware has links to North Korea, cybersecurity experts say. **The Guardian.** San Francisco, 15 mai 2017. Disponível em: <https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group> Acessado em: 20 ago. 2017.

SPECIAL TRIBUNAL FOR LEBANON. **Decision on the Admissibility of Documents Published on the Wikileaks Website (The Prosecutor v. Salim Jamil Ayyash, Mustafa Amine Badreddine, Hassan Habib Merhi, Hussein Hassan Oneissi, Assad Hassan Sabra)**, STL-11-01/T/TC, 2015, The Hague, Netherlands.

TEITELBAUM, Ruth. Recent Fact-Finding Developments at the International Court of Justice. **The Law & Practice of International Courts and Tribunals**, [S.l.], Vol. 6, No. 1, 2007.

THE Meaning of Stuxnet. **The Economist,** [S.l.], 30 set. 2010. Disponível em: <http://www.economist.com/node/17147862>. Acesso em: 04 ago. 2017.

THE TOR PROJECT. **Tor: Overview**. [S.l.], [S.d.] Disponível em: <https://www.torproject.org/about/overview.html.en#overview> Acessado em: 19 ago. 2017.

THIRLWAY, Hugh. **The International Court of Justice**. ed 1.Oxford: Oxford University Press, 2016.

TRAIL SMELTER ARBITRAL TRIBUNAL. **Trail Smelter Arbitration (United States v. Canada)**, Decision of 16 April 1938 and 11 March 1941. In: RIAA Vol. III, 2006, Geneva, Switzerland.

TRAYNOR, Ian. Russia accused of unleashing cyberwar to disable Estonia. **The Guardian**, [S.l.], 17 mai. 2007. Disponível em: <https://www.theguardian.com/world/2007/may/17/topstories3.russia>. Acesso em: 03 ago. 2017.

US and Israel were behind Stuxnet claims researcher. **BBC**, [S.l.], 04 mar. 2011. Disponível em: <http://www.bbc.com/news/technology-12633240>. Acesso em: 04 ago. 2017.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Comprehensive Study on Cybercrime: Draft— February 2013, XXIV**, [S.l.], 2013. Disponível em: <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>. Acessado em: 19 ago. 2017.

UNITED NATIONS SECRETARY GENERAL. **Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General**, 18 U.N. Doc. A/66/152, [S.l.] 15 Jul 2011.

UNITED NATIONS SECURITY COUNCIL. **Resolution 827**. U.N. Doc. S/RES/827, [S.l.], 25 mai, 1993.

_____. **Resolution 955**. U.N. Doc. S/RES/955, [S.l.], 08 nov, 1994.

_____. **Resolution 1757**. U.N. Doc. S/RES/1757, [S.l.], 30 mai, 2007.

UNITED STATES SENATE. **Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command.** Washington D. C., 15 abr 2010. Disponível em: <https://epic.org/privacy/nsa/Alexander_04-15-10.pdf> Acessado em: 22 ago. 2017.

_____. **Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command.** Washington D. C., 11 mar 2014. Disponível em: <https://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf> Acessado em: 22 ago. 2017.

VALENCIA-OSPINA, Eduardo. Evidence Before the International Court of Justice. **International Law FORUM Du Droit Internationa**l. The Hague, Vol. 1, 1999.

VERHULST, Stefaan. Estonian plan for 'data embassies' overseas to back up government databases. **New York University GovLab**, New York, 02 jun. 2012. Disponível em: <http://thegovlab.org/estonian-plan-for-data-embassies-overseas-to-back-up-government-databases>. Acesso em: 03 ago. 2017.

VON HEINEGG, Wolff, Heintschel. Legal Implications of Territorial Sovereignty in Cyberspace In: CZOSSECK, Christian; OTTIS, Rain; ZIOLKOWSKI, Katharina. (eds.). **2012 4th International Conference on Cyber Conflict**., NATO CCD COE Publications, Tallinn, 2012.

WEBB, Philippa. **International Judicial Integration and Fragmentation**. 1 ed. Oxford: Oxford University Press, 2013.

WOLFRUM, Rudger; MOLDNER, Mirka**. International Courts and Tribunals, Evidence**. Max Planck Encyclopedia of Public International Law, Oxford, 2013.

ZIMMERMANN, Andreas; OELLERS-FRAHM, Karin; TOMUSCHAT, Christian; TAMS, Christian J. **The Statute of the International Court of Justice: A Commentary**, 2 ed., Oxford: Oxford University Press, 2012.

ZIOLKOWSKI, Katharina. General Principles of International Law as Applicable in Cyberspace In: ZIOLKOWSKI, Katharina (ed.). **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**, NATO CCD COE Publications, Tallinn, 2013. Disponível em: <https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf>. Acesso em: 04 ago 2017.

_____. **Stuxnet – Legal Considerations**, NATO CCD COE Publications, Tallinn, 2012. Disponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf>. Acesso em: 07 ago. 2017.