FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ
CURSO DE DIREITO

MAURÍCIO DE MORAIS PONCELL FILHO

GUERRA CIBERNÉTICA:
Adaptação do Direito Internacional em seu sistema a esse novo domínio público

Recife
2018

MAURÍCIO DE MORAIS PONCELL FILHO

GUERRA CIBERNÉTICA:
Adaptação do Direito Internacional em seu sistema a esse novo domínio público

Monografia apresentada à Faculdade Damas da Instrução Cristã como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Henrique Weil Afonso.

Recife
2018

Ficha catalográfica
Elaborada pela biblioteca da Faculdade Damas da Instrução Cristã

Poncell Filho, Maurício de Morais.
P739g Guerra cibernética: adaptação do direito internacional em seu sistema a esse novo domínio público / Maurício de Morais Poncell Filho. - Recife, 2018.
68 f.

Orientador: Prof. Dr. Henrique Weil Afonso.
Trabalho de conclusão de curso (Monografia - Direito) – Faculdade Damas da Instrução Cristã, 2018.
Inclui bibliografia

1. Direito internacional. 2. Guerra cibernética. 3. Espaço cibernético. I. Afonso, Henrique Weill. II. Faculdade Damas da Instrução Cristã. III. Título

341 CDU (22. ed.) FADIC (2018-163)

FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ

MAURÍCIO DE MORAIS PONCELL FILHO

GUERRA CIBERNÉTICA: Adaptação do Direito Internacional a esse novo domínio público

Defesa Pública em Recife, _____de_____ de 2018.

BANCA EXAMINADORA:

Presidente: Orientador: Prof. Dr. Henrique Weil Afonso

_____

Examinador (a): Prof.

_____

Examinador (a): Prof.

_____

AGRADECIMENTOS

Agradeço primeiramente ao meu avô, Ateniense, pessoa que tenho profunda admiração me estimulando desde pequeno sempre a pesquisar e procurar o conhecimento para satisfação pessoal, assim como minha avó, Maria de Lourdes, pelos carinhos e orações.

Agradeço por agora aos meus pais que diariamente desde o início do curso vêm acompanhando minha luta diária, me dando forças e motivações, assim como minha cadela Pituca, que apesar de ser um animal, possui uma sensibilidade incrível de absorver minha concentração e dedicação nas vastas horas de estudos ao meu lado.

Agradeço também a Faculdade Damas com todos os seus professores que passaram do 1º ao 10º período, me proporcionando um pensamento cada vez mais crítico sobre nossa sociedade.

Agradeço a todos os meus amigos que sempre estiveram ao meu lado em todos os momentos que precisei.

Por fim mais uma vez agradeço a todos os meus familiares pelo carinho e pelo apoio!

RESUMO

Esta monografia trata de um estudo sobre a guerra cibernética, a respeito de vários assuntos que permeiam o Direito Internacional e a adaptação de seus instrumentos jurídicos voltados para esse novo domínio. É observado que o propósito desse estudo visa entender as modificações que a comunidade internacional vem suportando de acordo com os possíveis atos de guerra (como espionagem de dados sigilosos, ataques a sistemas financeiros e manipulações de informações) provocados no espaço cibernético, trazendo um novo cenário mundial nas relações. O Direito internacional por ter bases principiológicas e doutrinárias bastantes abrangentes traz várias respostas para a resolução desse problema jurídico que se enfrenta, sempre baseado na soberania e na jurisdição dos Estados, assim como nos princípios norteadores do próprio Direito Internacional e nas convenções da ONU, assessoradas por seus respectivos órgãos especializados no controle da segurança cibernética. Toda essa conjectura visa uma normatização jurídica mais segura para as consequências da guerra cibernética. A metodologia hipotético-dedutiva utilizada em conjunto com a pesquisa descritiva e bibliográfica traz uma investigação cientifica que crie uma nova visão como o Direito Internacional pode adaptar e atualizar seu sistema jurídico ao novo mundo da guerra cibernética contida na esfera do ciberespaço, se utilizando das fontes, princípios e doutrinas como analise de testes e estudos para essa regulação jurídica. Destarte, o trabalho ainda se utiliza da metodologia de direito comparado, valendo-se das resoluções da ONU para compor a base cientifica dos demais conteúdos. Por fim a monografia traz temas inovadores como o da constitucionalidade internacional, o regime jurídico de condomínios globais, a corrente doutrinaria do direito transnacional e o sistema de verificação de um ataque armado ser enquadrado como um ataque cibernético. Esses principais pontos abordados possibilitam uma visão que o Direito Internacional dispõem de grande potência de se legislar os efeitos de uma guerra cibernética, contudo este precisará entrar em um profundo debate que tratam de temas como relações políticas internacionais, economia e tecnologia, sendo um estudo sempre continuado e constante quando é falado de guerra cibernética.

Palavras chave: Direito Internacional. guerra cibernética. espaço cibernético.

ABSTRACT

This monograph deals with a study on cyber warfare, about various issues that permeate international law and the adaptation of its legal instruments aimed at this new field. It is observed that the purpose of this study is to understand the changes that the international community has been taking in accordance with possible acts of war (such as espionage of secret data, attacks on financial systems and manipulation of information) caused in cyber space, bringing a new scenario relationship. International law, because of its broad principles and doctrines, provides a number of answers for solving this legal problem, which is always based on the sovereignty and jurisdiction of States, as well as on the guiding principles of International Law itself and the UN conventions, which are advised by their respective specialized agencies in the control of cyber security. All this conjecture aims at safer legal regulation for the consequences of cyber warfare. The hypothetical-deductive methodology used in conjunction with the descriptive and bibliographical research brings a scientific investigation that creates a new vision as the International Law can adapt and update its legal system to the new world of the cyber war contained in the sphere of the cyberspace, if using of the sources , principles and doctrines such as analysis of tests and studies for this legal regulation. Thus, the work is still using the methodology of comparative law, using UN resolutions to compose the scientific basis of the other contents. Finally, the monograph introduces innovative themes such as international constitutionality, the juridical regime of global condominiums, the current doctrine of transnational law, and the system for verifying an armed attack to be framed as a cyber attack. These main points allow a view that international law has great power to legislate the effects of a cyber war, but this will need to enter into a deep debate that deal with issues such as international political relations, economics and technology continuous and constant when it comes to cyber warfare.

Keywords: International Law. cyber warfare. cyber space.

SUMÁRIO

1. INTRODUÇÃO

Com o avanço tecnológico pós-segunda guerra mundial temos um novo palco no século XXI para as guerras. A chamada guerra cibernética é uma nova preocupação para o Direito Internacional, na medida em que o ciberespaço se tornou um novo domínio público internacional. Observamos que as noções clássicas de soberania e jurisdição entre os Estados acabam por ter sua barreira territorial/política ultrapassada pela tecnologia, resultando uma corrida armamentista cibernética de aprimoramentos tecnológicos, com base na espionagem entre os próprios Estados no ciberespaço, além de atos de guerra provocados como intervenções nos sistemas financeiros, atentados a sistemas reguladores de matrizes nucleares e até mesmo manipulações de dados nas eleições.

Todos esses fatos ocorrentes no âmbito do ciberespaço se torna um novo objeto de estudo no Direito Internacional e adaptação de seu sistema jurídico a nova realidade da sociedade internacional diante da evolução tecnológica.

O trabalho tem como finalidade trazer ao público a importância do novo cenário mundial através dos atos de guerra provocados no espaço cibernético, pois muda os costumes da comunidade internacional, como por exemplo, o ataque cibernético a um programa nuclear do Irã em que foi instalado um vírus no sistema eletrônico da planta de enriquecimento de urânio com objetivo de extrair as informações de controle desta matriz energética.

Diante deste caso observamos a preocupação do Direito Internacional modificar seus instrumentos jurídicos aperfeiçoando as noções básicas de soberania e jurisdição voltadas a esse novo paradigma da guerra cibernética, em que os Estados atacam uns aos outros por meios tecnológicos.

As consequências podem ser as mais diversas desde danos econômicos até danos políticos, sendo justificados por uma mera legitima defesa, pois se sentiram ameaçados aos ataques a suas informações e decidiram contra-atacar utilizando esse mesmo viés cibernético. Sendo assim o ciberespaço acaba se tornando um ambiente hostil que precisa de uma séria regulação jurídica a fim de evitar e punir os entes internacionais que deram causa a esses conflitos tecnológicos e ás demais repercussões no mundo físico/real. Uma segurança maior à rede de informações garante a integridade da comunidade internacional em seu equilíbrio jurídico, prosperando assim uma melhor regulação deste novo domínio público que é o ciberespaço.

Ainda nesta linha de pensamento se tem diversas pesquisas cientificas que abordam o

tema, sendo exposto no trabalho da autora Barros (2015), intitulado de Guerra cibernética: os novos desafios do Direito Internacional, falando a respeito que a guerra cibernética possui um bom alicerce principiológico do Direito Internacional, de acordo com a preservação da paz e da segurança, respeitando a soberania dos Estados e não se utilizando da força. Contudo essa nova realidade do domínio virtual deve ser pensada nas relações internacionais não como uma justificação que viole o próprio Direito Internacional, mas que o mesmo crie uma realidade sistêmica interativa, rompendo os paradigmas lineares do direito aplicando uma ótica democrática e interativa da soberania, elevando uma participação maior dos Estados na escolha de alternativas no campo de atuação internacional.

Assim como Saldan (2012) intitulado de: Os desafios jurídicos da guerra no espaço cibernético, que também aborda esse novo domínio público de maneira alarmante, pois os ataques cibernéticos possuem uma capacidade destrutiva tão significativa que podem ser comparados como armas, razão pela qual se traduz perfeitamente a uma agressão ou uso da força segundo a carta da ONU.

É necessário que se identifique o agressor para que a legítima defesa ou o sistema de segurança coletivo sejam autorizados, todavia, qualquer reação deve ser sopesada de acordo com os princípios da necessidade e proporcionalidade, que precisam ser sazonados para o ciberespaço.

Com base na problematização e justificação apresentados nos parágrafos supracitados, como o Direito Internacional pode adaptar seu sistema jurídico ao novo domínio público internacional no âmbito da guerra cibernética?

Tendo em vista a grande e complexa problemática da guerra no ciberespaço, apresentamos caminhos a serem percorridos e desenvolvidos para possível solução desta incógnita. O Direito Internacional por ser um instituto jurídico bastante flexível e maleável em relação à soberania e jurisdição dos Estados, composta por uma estrutura de vários princípios gerais como: igualdade soberana dos Estados, independência e respeito à jurisdição internacional, a não intervenção nos assuntos da competência interna de outros Estados; Assim como as convenções da ONU sobre segurança no espaço cibernético, fazendo com que essas convenções e princípios vissem uma possível regulação e impedimento dos demais atos provocados pelos Estados soberanos no ciberespaço geram uma possível guerra no âmbito cibernético**.**

Por seguinte o trabalho tem como objetivo geral analisar como o Direito Internacional pode adaptar seu sistema jurídico para a regulação da guerra cibernética, voltada para a finalidade de uma segurança jurídica mais sólida nesse novo domínio público sendo orientada

por princípios e fontes basilares do Direito Internacional. Já os objetivos específicos são: descrever o que é a soberania dos Estados em sua modalidade clássica e a transformação que este instituto jurídico irá com o surgimento do ciberespaço e o novo palco das guerras cibernéticas no século XXI; Desenvolver a modificação do instituto jurídico da jurisdição, assim como as doutrinas que estudam formas de normatizações que ultrapassem as fronteiras dos Estados, pois o ciberespaço é um domínio presente desde a esfera nacional ate a esfera internacional; Caracterizar o espaço cibernético explicando sua delimitação no direito internacional, seu funcionamento e sua hostilização pós-segunda guerra como um novo meio bélico dando uma nova face à guerra, que seria a guerra cibernética.

Observamos a utilização da metodologia hipotético-dedutiva aliada ao tipo de pesquisa descritiva e bibliográfica, visando à investigação científica na construção de uma nova visão de adapte os instrumentos jurídicos do Direito Internacional ao novo paradigma da guerra cibernética no âmbito do ciberespaço, testando as demais fontes e princípios do Direito Internacional na regulação da punição e prevenção de determinados atos de guerra provocados através do espaço cibernético.

O trabalho também possui a utilização da metodologia de direito comparado analisando as resoluções da ONU de acordo com as políticas legais de segurança cibernética e a convenção do Conselho Europeu sobre crime cibernético.

Na abordagem teórica será apresentado o primeiro capítulo tratando da soberania no ciberespaço. Conceitua-se a soberania em dois tipos, interna e externa, na primeira é observado que é o poder supremo que o Estado possui de tomar suas próprias decisões dentro de seu território. Já a soberania externa é explicada como uma atuação da personalidade jurídica do Estado no âmbito internacional, como por exemplo, o direito a uma igualdade jurídica (MAZZUOLI, 2011, p.509). Com base nesses conceitos expostos de soberania, é reparado que o ciberespaço para ser acessado necessita de uma estrutura física o que geraria uma série de consequências e efeitos jurídicos advindos deste novo domínio público atuante na esfera soberana dos Estados.

No segundo capítulo é exibida a jurisdição, que é um elemento integrante da soberania dos Estados sendo na maioria das vezes executada nos limites de seu próprio território, portanto é função do Estado delimitar até que ponto seu ordenamento jurídico poderá atingir tanto no âmbito interno como no externo. Fazendo uma contraposição com o conceito clássico de jurisdição ligado ao território e seus limites, o ciberespaço apesar de ser um território não físico (virtual), as matrizes que mantêm a operação deste espaço são físicas como foi explicado no capítulo anterior, ocorrendo uma interação entre o real e o virtual,

submetendo-se à jurisdição de algum Estado e suas respectivas leis.

Por fim no terceiro capítulo é tratada a abordagem do ciberespaço, pois com a virada para o século XXI, presenciamos uma profunda e rápida evolução da tecnologia, possibilitando um grande número de interações, comunicações, no palco internacional. Joseph Nye Jr., traz o conceito de ciberespaço em que é um ambiente operacional delimitado pela utilização de meios eletrônicos para explorar a informação por meio de sistemas interconectados. (NYE JR., 2010, p.122). Este novo domínio público chamado de ciberespaço é formado de uma rede complexa que contém diversas conexões interativas pelo mundo entre os entes internacionais, trazendo inúmeras incertezas sobre a atuação do Direito internacional no futuro.

2. OS CONTORNOS CLÁSSICOS DO PRINCÍPIO DA SOBERANIA E SUAS TRANSFORMAÇÕES NA SOCIEDADE INTERNACIONAL CONTEMPORÂNEA

Conforme foi apresentado na introdução os tipos de soberania e seus demais conceitos sendo consolidados pela comunidade internacional, por inicio, neste capítulo será estudado de forma mais aprofundada a parte doutrinária, que sustenta a ideia de soberania para contextualização dentro da temática do ciberespaço poder ser feita.

Seguindo a doutrina de Mazzuoli (2011), o conceito contemporâneo de soberania traz o entendimento que o Estado detém o poder de tomar suas próprias decisões dentro do seu território, seja aplicação ou criação de suas próprias leis. Sendo assim o Estado não reconhece nenhum poder maior ou mais alto que o seu internamente, de maneira que não se admite a atuação de poder superior ao próprio Estado que dite suas competências internas.

Na mesma linha de pensamento é notado que em outra definição a soberania se trata de um poder incontestável, pois dentro do seu território nacional a validade jurídica de normas e atos não são passíveis de intervenções externas de poderes maiores que as modifiquem, tendo em vista o poder que produz o Direito positivo é o próprio direito na qual não há direito, não podendo o mesmo ser contestado (TELLES JUNIOR, 2001 apud MAZZUOLI, 2011).

A soberania por seguinte fora dos limites internos dos Estados demonstra uma situação de ‘’ igualdade soberana’’ em suas relações internacionais de acordo com o art.2º,§ 1º da Carta da ONU[1] de forma que o fator diferenciador entre os tipos de soberania é justamente o seu fator interno/territorial que atribui efeitos jurídicos diferentes para cada situação.

A partir do momento que o Estado deixa os limites de suas competências nacionais e passa a atuar nas relações externas, a ideia de soberania deixa de ser constituída na ótica de não se poder relativizar-la entre Estados, já que a soberania traduz o sentido de algo supremo, predominante e diante do contexto internacional os Estados devem estar em pé de igualdade, porque não se teria lógica aplicar a soberania de todos os Estados ao mesmo tempo em uma relação internacional (MAZZUOLI, 2011).

A relativização de alguns direitos inerentes à personalidade do Estado na comunidade internacional remonta a comparação com o pensamento de Luigi Ferrajoli que não está tão destoante do nível de complexidade internacional que se chegara. O direito internacional levado a sério e a crise do Estado nacional trazido por Ferrajoli (2002, p. 46) nos explica que

[1] Artigo 2: A Organização e seus membros, para a realização dos propósitos mencionados no artigo 1, agirão de acordo com os seguintes Princípios: 1. A Organização é baseada no princípio da igualdade soberana de todos os seus membros.

‘’ repensar o Estado em suas relações externas à luz do atual direito internacional não é diferente de pensar o Estado em sua dimensão interna á luz do direito constitucional. ’’

Ao analisar essa passagem posta pelo autor e sendo comparada com as explicações que serão abordadas, observa-se que o direito internacional não é um instituto que esta à parte dessa realidade constitucional dos Estados, mas que parte dessa realidade é objeto do direito internacional planejar garantias jurídicas que se encaixem e equilibrem essas relações complexas políticas e jurídicas que os Estados têm com a comunidade internacional. É percebida que a crise do Estado nacional é real, nas devidas proporções, quando é feita uma retrospectiva na qual a humanidade passou há quatro séculos desde quando surgiu o Estado moderno na Europa e os Estados soberanos na comunidade internacional.

O poder altamente destrutivo das armas nucleares, as disparidades econômicas entre os países gerando a miséria, conflitos de cunho étnicos intranacionais, como por exemplo, o caso dos ataques cibernéticos contra a Estônia realizados pela Rússia que será melhor explicado, tornam a convivência internacional na manutenção da paz e seu equilíbrio internacional cada vez mais difícil. Todos os Estados da comunidade internacional no século XXI estão em uma crescente interdependência econômica, política e principalmente tecnológica/informacional formando a humanidade um tipo de aldeia global com relações totalmente complexas e frágeis.

Toda essa gravidade factual atrai com certo peso a responsabilidade do Direito Internacional em realizar uma espécie de integração mundial que embora exista, possui alguns pontos em aberto, principalmente na questão da regulação da guerra cibernética. Portanto a soberania externa do Estado se preocupa principalmente com a sua defesa contra os inimigos externos, porém, com essa crescente interdependência internacional do século XXI acaba por diminuir a forte presença desse conceito. Surge então uma crise de legitimação dessa sistemática de soberanias desiguais, já que temos países com uma tecnologia muito avançada para atuar no ciberespaço em detrimento de países que sequer tem tecnologia suficiente para se defender contra esses ataques, além dos vários fatores de ordem econômica e política, transformando a longo prazo um sistema insustentável que visa igualdades meramente formais do ponto de vista jurídico dispostos na carta da ONU.

Segundo Ferrajoli (2002) no tema sobre a soberania, é enfatizada a sua construção doutrinária principalmente na segunda aporia que sustenta a mesma:

> A segunda aporia diz respeito à história, teórica e sobretudo prática, da ideia de soberania como *potestas* absoluta *superiorem non recognoscens.* Essa história

> corresponde a dois eventos paralelos e divergentes: aquele da soberania interna, que é a história de sua progressiva limitação e dissolução paralelamente á formação dos Estados constitucionais e democráticos de direito; e aquele da soberania externa que é a história de sua progressiva absolutização que alcançou seu ápice na primeira metade do século XX com as catástrofes das duas guerras mundiais. Nem mesmo cronologicamente as duas histórias coincidem: a da soberania externa iniciou-se primeiro e, diferentemente daquela da soberania interna, ainda está longe de concluir-se e continua a mostrar-se como uma ameaça permanentemente de guerras e destruições para o futuro da humanidade (FERRAJOLI, 2002, p.3).

De acordo com essa passagem o poder absoluto não reconhece qualquer outro superior, confirmando o que já foi exposto em parágrafos passados, já que a soberania interna dos Estados em suas próprias formações constitucionais e democráticas de direito provocaram uma inconsistência na soberania externa. É importante destacar que a soberania externa projeta a personalidade jurídica do Estado, principalmente na questão do não envolvimento de um Estado na esfera de competência do outro. Entretanto esse impasse entre garantir um poder supremo estatal e manter em pé a igualdade soberana, trouxe o apogeu que desencadeou as duas guerras mundiais, por terem sido acompanhadas pela concentração e a ampliação do poder de maneira gradual vindo da própria soberania interna.

É observada de maneira evidente e atual a ideia do referido autor no âmbito da guerra cibernética, porque os Estados criam novas tecnologias e desenvolvem meios cibernéticos em seu próprio território, sendo legitimados por toda uma estrutura normativa vinda de uma Constituição que favorece de maneira progressiva um aumento de poder do Estado. A legitimação interna feita pelos Estados de um poder cibernético, desencadeia por consequência a violação de outros Estados seja por espionagem cibernética ou ate mesmo ataques cibernéticos (por meios de *hackers* ou vírus), para manter a garantia de seus direitos adquiridos pela soberania interna. A razão do Estado em progredir em seu poder soberano, seja em razão da segurança nacional para não ficar desprotegido dos outros Estados ou aprimoramentos tecnológicos de cunho bélico/informacional para não ficar para traz em seus armamentos dos demais, podem extrapolar o próprio poder soberano interno e atingir outro Estado sendo capaz resultar em uma guerra cibernética.

Contudo, na comunidade internacional os Estados vivem se monitorando nessa questão cibernética, como por exemplo, a China habitualmente mapeando os sistemas informacionais do pentágono nos Estados Unidos para se atualizar em seus sistemas

cibernéticos de capacidade militar e de defesa, os aprimorando caso os americanos os tentem contra-atacar se utilizando do mesmo vetor cibernético (ULTIMO SEGUNDO IG, 2013).

Isso acaba resultando uma confusão jurídica e até mesmo uma lacuna na carta da ONU, pois a limitação, proteção e ate mesmo a punição dentro da utilização da soberania fica um ponto de discussão para se verificar em que ocasiões houve violação da soberania, atos de guerra, legítima defesa, e outras séries de efeitos jurídicos internacionais que merecem ter destaque aos olhos da comunidade internacional e principalmente pela ONU.

Fazendo um paralelo, Ferrajoli (2002) em sua proposta final apresenta a ideia de um constitucionalismo de direito internacional que leve um respeito efetivo pelas cartas internacionais de direitos humanos e o reconhecimento das faltas de garantias para que as cartas sejam executadas, pois é obrigação da ONU e dos respectivos Estados suprir essas lacunas.

Ora, esta concepção não é diferente quando falamos da normatização de possíveis lacunas na carta da ONU sobre a temática da guerra cibernética, atuando os Estados de forma democrática ao lado da ONU para por em pauta quais as possíveis faltas de garantias que os demais entes internacionais têm quando se trata do uso e de sua violação da soberania em decorrência do meio cibernético.

Continuando os desdobramentos sobre a conceituação de soberania, ainda existem outras duas formas: a negativa e a positiva. Na soberania negativa foi trilhado o mesmo caminho lógico de uma fundamentação jurídica que tem como base a independência e a igualdade de maneira formal entre os Estados, ou seja, esse instituto não necessita de um caráter ativo dos Estados na comunidade internacional, mas sim o exercício do direito de não intervenção em seus assuntos internos respeitando os demais membros que fazem parte da sociedade internacional. Diferentemente da soberania positiva, que prega um ativismo dos Estados em seu governo na prestação de bens de natureza coletiva a todos os cidadãos, em outros termos, seria uma aptidão do Estado em declarar e executar políticas públicas tanto em seu âmbito interno como no âmbito internacional objetivando uma satisfação de necessidades das mais variadas formas (legais e sociais) dos seus cidadãos (MAZZUOLI, 2011).

Observa-se que essas duas formas caracterizam o Estado, pois todos eles possuem soberania negativa, contudo a soberania positiva depende de ativismo Estatal que por meio de seus atributos políticos implementem governos que criem efetivações internas e externas que sejam reconhecidos pela comunidade internacional (JACKSON, 1990 apud MAZZUOLI, 2011).

O retrato da doutrina que foi exposto, trás outra visão da guerra cibernética, porque todos os Estados ao possuírem a soberania negativa estão no exercício do direito a não intervenção. Em consequência, isso reflete quando um Estado por meio do ciberespaço se utiliza de meios cibernéticos para entrar na esfera do outro e obter determinadas informações sigilosas ou confidenciais, restando por desrespeitar a relação de igualdade e independência que todos os entes da sociedade internacional possuem.

No que toca a soberania positiva, esse ativismo Estatal tanto internamente como no âmbito internacional deve ser levada a reflexão do ciberespaço em discussões governamentais internas se tratando de legislações, e postas à comunidade internacional para que protejam seus cidadãos. É destacado o exemplo, dos ataques cibernéticos advindos da Rússia em manifestação contra a retirada da estátua de um soldado soviético que lutou contra os nazistas na capital da Estônia em Tallin, atuando a Rússia através de *harckers* em ‘’bombardear’’ de informações que ultrapassem um limite máximo suportado de servidores de empresas e bancos Estonianos gerando um transtorno na sociedade (BBC BRASIL, 2007).

A estátua é vista pelo povo Estoniano como um símbolo de opressão soviética e em contra partida a comunidade étnica russa considera a retirada da estátua um insulto. A situação é deveras preocupante do ponto de vista internacional, tendo em vista que o ministério da defesa da Estônia alega ataques partindo de várias partes do mundo, porém com uma concentração maior vindo de sites baseados na Rússia. Identifica-se que a soberania positiva quando é exercida, leva em conta toda uma discussão governamental em torno de como o país deve se comportar e tomar medidas que protejam seu status político através de implementações jurídicas. Entretanto a sociedade internacional tem um dever de atuação em conjunto trazendo respaldos também jurídicos a respeito do ciberespaço e desses atos de guerra que violam a soberania dos Estados. Da mesma maneira que os próprios Estados em seu exercício de Soberania externa, por meio da sua personalidade jurídica internacional, trazerem a sociedade internacional um debate que deságue em uma possível regulação da guerra cibernética (BBC BRASIL, 2007).

De qualquer forma não se pode falar de soberania sem falar do direito a igualdade que apesar de ser muito parecido e próximo do direito a liberdade e a soberania, está estritamente ligado como uma relação lógica doutrinária imprescindível para a sustentação de todas essas garantias internacionais. A base principiológica do Direito Internacional deve ser compreendida como uma teia de conceitos interligados que de fatos em fatos tendem a se flexibilizar, e tornar possível a resolução de vários problemas internacionais. O fundamento

em uma larga doutrina jurídica, permitindo diferentes interpretações, pode garantir o objetivo de uma segurança jurídica que é proposta pelo Direito Internacional.

Quando falamos do direito a igualdade voltamos ao início do capítulo sendo mencionado o Art. 2º,§1º da Carta da ONU, sendo assim em decorrência dessa norma é importante frisar a igualdade jurídica entre todos os Estados em virtude da soberania, ou seja, falamos de igualdade jurídica e não de fato. Segundo Garner, o princípio da igualdade,

> Não implica ou não deveria implicar outra coisa senão a igualdade perante o direito internacional, isto é, o direito de todos os Estados, grandes ou pequenos, à mesma proteção do direito e à igualdade de tratamentos quando se apresentam perante as jurisdições internacionais, como querelantes ou querelados (GARNER, 1931 apud MAZZUOLI, 2011, p.510).

É de suma importância reparamos a aplicabilidade do princípio da igualdade jurídica absoluta entre os Estados no Art.4º da Convenção Panamericana sobre os Direitos e Deveres dos Estados, afirmando que todos os Estados são ‘’juridicamente iguais’’, possuindo as mesmas prerrogativas de direitos e tendo a mesma competência para a realização de seus exercícios.

Ainda comentando sobre o artigo acima, o simples fato de o Estado surgir como sujeito de Direito Internacional já consubstancia o próprio direito a igualdade independente do poder que possua para assegurar seu exercício. A resolução nº2625 (XXV) promulgada pela Assembleia-Geral da ONU expressa: ‘’ Todos os Estados gozam de igualdade soberana’’. Os Estados possuem direitos e deveres iguais porque todos compõem como membros da comunidade internacional, embora sejam existentes as relações de disparidades econômicas, políticas, sociais entre outras (GENERAL ASSEMBLY, 1970 apud MAZZUOLI, 2011)[2].

A mesma resolução traz seis elementos caracterizadores que fazem parte da igualdade entre os Estados: a) a igualdade em direitos; b) o gozo dos direitos inerentes á plenitude da soberania; c) o respeito à personalidade dos outros Estados; d) a integridade territorial e a independência política; e) a livre escolha do Estado de seu sistema político, social, econômico e cultural; f) o dever dos Estados em respeitar seus compromissos e de viver em paz com os outros Estados (GENERAL ASSEMBLY, 1970 apud MAZZUOLI, 2011)[3].

---

[2] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations; Preamble: *Reaffirming*, in accordance with the Charter, the basic importance of sovereign equality and stressing that the purposes of the United Nations can be implemented only if States enjoy sovereign equality and comply fully with the requirements of this principle in their international relations, […]

[3] The principle of sovereign equality of States: […] a. States are judicially equal; b. Each State enjoys the rights

Em ponto negativo, é presente um problema inerente ao direito à igualdade e que posteriormente justifica boa parte da política internacional na questão da guerra cibernética, porque a igualdade jurídica acaba por não ser suficiente na atuação efetiva desse principio, surgindo às desigualdades de facto. Essa desigualdade factual é um dos maiores desafios jurídicos do direito internacional quando o sistema jurídico internacional observa a violação dos direitos dispostos na carta da ONU e atua por consequência na defesa e na tutela dos mesmos.

Acaba por ser um ponto delicado, porém a própria carta da ONU tenta por reequilibrar os Estados desigualando alguns deles visando essa proteção da desigualdade de facto, resultando em contrapesos entre os Estados permanentes que fazem parte do Conselho de Segurança (França, Estados Unidos, Reino Unido, China e Rússia), detentores do poder de veto que serve como um fator para desigualar os poderes entre os Estados.

Diante do direito a igualdade juntamente com as desigualdades de facto, a função do Conselho de Segurança sofre de uma parcialidade no tema da guerra cibernética na medida em que os próprios Estados do Conselho como, por exemplo, a Rússia no suposto ataque contra a Estônia, quebram a igualdade e uma série de garantias inerentes à soberania dos Estados de maneira que o direito internacional está diante de uma complexidade além de jurídica, política no controle interno da ONU (BBC BRASIL, 2007).

Uma possível regulação da guerra cibernética por desvantagem se teria um favorecimento dos países mais fortes economicamente e politicamente do globo, botando em vulnerabilidade a integridade da comunidade internacional. Sendo assim o que está disposto no art.24º da carta da ONU dá ao Conselho de Segurança como único órgão das Nações Unidas, o poder decisório em manutenção da paz e da segurança internacional.

Não obstante mesmo todos os países sabendo das atrocidades às avessas dos países mais fortes economicamente e politicamente, a comunidade internacional não pode deixar de debater e começar a trazer em pauta as legislações internas e programas governamentais em defesa das garantias como a soberania, o princípio da não intervenção, o princípio da igualdade entre outros direitos inerentes ao Estado decorrentes de sua personalidade jurídica internacional.

---

inherent in full sovereignty; c. Each State has the duty to respect the personality of other States; d. The territorial integrity and political independence of the State are inviolable; e. Each State has the right freely to choose and develop its political, social, economic and cultural systems; f. Each State has the duty to comply fully and in good faith with its international obligations and to live in peace with other States.

2.1 Questionamentos sobre a equalização do poder soberano

Em continuidade na questão de normatizações e discussões a respeito da regulação da guerra cibernética se tem o primeiro guia internacional, sem caráter vinculativo, como uma tentativa de direcionar uma visão apurada sobre a lei aplicável às operações cibernéticas hostis, sendo chamado o manual de Tallin (GUIA DE ESTUDOS..., 2016).

A produção deste manual em parceria entre o Centro de Excelência de Ciberdefesa Cooperativa da OTAN (CCDCOE) e a universidade de Cambridge, contando com a ajuda de organismos observadores como o Comitê Internacional da Cruz Vermelha, o USCYBERCOM e a OTAN desenvolveram um trabalho na análise de leis gerais existentes com a finalidade de entender como poderiam ser aplicadas no contexto da guerra cibernética, tendo em vista o desencadeamento dos ataques cibernéticos à Estônia em 2007. O manual contêm noventa e cinco encaminhamentos, que no caso de uma vivência em conflitos cibernéticos, devem ser seguidos (GUIA DE ESTUDOS..., 2016).

Questões essenciais como soberania, ‘’*jus in bello*’’(direito que rege a maneira como a guerra é conduzida), ‘’*jus ad bellum*’’(direito do uso da força), responsabilidade dos Estados, lei da neutralidade e direito humanitário internacional são trabalhados ao longo do tratado visando formar uma possível base jurídica que trazem diversas visões de especialistas para a interpretação do âmbito cibernético no século XXI. Toda essa conjuntura de temas e esforços dos especialistas tem o propósito de contestar como e quando um Estado pode declarar a guerra cibernética para se defender de possíveis ataques, quais leis serão aplicadas ao caso concreto entre outras situações, porque dentro do ciberespaço ainda não foi definido o que seriam considerados crimes de guerra ou atos de guerra diferidos de uma legítima defesa (GUIA DE ESTUDOS..., 2016).

Tem-se um risco existente em se confundir um ato realizado por um Estado dentro do ciberespaço para se defender de um ataque cibernético e um ato de guerra ou crime de guerra que pode desencadear uma guerra cibernética ou uma guerra clássica, porém com motivações advindas de questões violadas no ciberespaço.

O manual de Tallin não só traz situações de guerra cibernética ou a sua eminência, mas também versa sobre o direito cibernético em tempos de paz, buscando normatizar as atividades cotidianas no meio cibernético realizados pelos entes internacionais que estão abaixo do nível de um ataque cibernético propriamente dito (GUIA DE ESTUDOS ..., 2016).

Esse parâmetro de convivência funciona como um termômetro para se evitar um caos total na sociedade internacional na medida em que um mínimo ato de um Estado no meio

cibernético com uma interferência não tão relevante para outro Estado já se caracterizaria uma motivação para a guerra, gerando uma dinâmica totalmente desproporcional levando em conta a hiperconectividade que possuímos entre os Estados ao redor do globo. É manifesto, que principalmente os Estados mais fortes da comunidade internacional e consequentemente os que fazem parte do Conselho de Segurança diariamente monitoram o meio cibernético e adentram dentro de áreas de informações que são pertencentes a outros Estados.

Contudo um dos pontos mais delicados acaba por ser este, pois a mera investigação e monitoramento do ciberespaço para a proteção da comunidade internacional justificaria o Estado investigador a adentrar em áreas de informações de competência interna, ou o princípio da não intervenção nos assuntos internos dos Estados para mantermos de pé o direito a soberania dos Estados e a suas igualdades do ponto de vista jurídico na sociedade internacional?

Certamente que os Estados ao aderirem um tratado internacional sobre guerra cibernética ou ate mesmo hipoteticamente falando de uma constitucionalização de algum código de guerra cibernética, acabam-se por falar de algumas relativizações de direitos inerentes à personalidade do Estado no meio internacional para determinados casos. Fazendo uma comparação que está muito distante do tema abordado no trabalho, mas que idealiza uma linha de pensamento válida é quando se relativizam os direitos constitucionais em determinados casos em nossa Carta Magna, como a quebra de sigilo telefônico para fins de investigação.

Ora, o direito a privacidade de informações existe, porém ao se investigar um fato relevante e autorizado por entidades superiores vemos a relativização deste direito. A aplicação desta ideia, só que de maneira bem mais complexa e delicada, seria o inicio de uma exegese jurídica na construção de aplicações normativas nos casos que envolvam o âmbito da guerra cibernética.

O Conselho de Segurança da ONU serviria justamente para essa interpretação levando em conta fatores econômico, políticos, jurídicos e outros para decidir se tal ato realizado por determinado Estado no ciberespaço estaria violando a soberania ou até mesmo se o Estado estaria realizando um ataque cibernético.

Segundo Ferrajoli (2002), o Estado nacional como sujeito soberano está em uma crise que vem dos dois lados, uma crise de cima quando os Estados transferem parte de seu poder para entidades supra estatais ou extra estatais (como a ONU, OTAN, Comunidade Europeia entre outras), como parte das suas funções bélicas de defesa militar e combate a criminalidade entres outras funções que no passado tinha sua gênese e seu desempenho dentro da soberania

Estatal. De baixo temos um desmembramento interno do Estado levando em conta as comunicações internacionais gerando conflitos políticos internos alterando a pacificação interna nacional.

Por fim chega-se ao constitucionalismo do direito internacional como um tipo de superação a crise dos Estados por conta de sua soberania esta sendo compactada em razão de diversos fatores internos e externos. Em caráter gradativo observamos que a superação da crise Estatal se dá no plano e uma despotencialização e do deslocamento para o âmbito internacional das bases do constitucionalismo ligadas de maneira tradicional aos Estados, que vai além daqueles princípios de ordem internacional que se conhece, juntamente com o que ocorreu nas Declarações e Convenções, e principalmente com a Carta da ONU que versam sobre essas garantias de caráter internacionais.

Não se está propondo uma forma de governo mundial, mas em um ideal levantado por Kelsen intitulado de '' A paz através do direito'', limitando de uma forma efetiva a soberania dos Estados através de uma implementação de garantias jurisdicionais, contra as violações dos direitos humanos de maneira interna e contra violações da paz de maneira externa (FERRAJOLI, 2002).

Da mesma forma que foram tratadas as limitações à soberania do Estado através de algum ideal próximo ao constitucionalismo internacional, levando em conta a crise soberana do Estado nacional, é vista a relativização da soberania totalmente atrelada à atribuição em segundo plano certos poderes inerentes a personalidade do Estado na comunidade internacional e de maneira específica aos poderes que sustentam a soberania.

Emer de Vattel ao dar o conceito clássico de soberania também traz em contra ponto uma semente da relativização ao falar que "(...) ao Estado mais poderoso é dada mais honra e ao Estado mais fraco mais ajuda" (VATTEL, 2004, p.16 apud MARTINS, 2009, p. 2), sendo assim é notório, apesar de ser utópica, a presença de um substrato que se reflete na carta da ONU disposta em seu Art. 1º,§2º e no Art. 2º, §1º. Contudo ainda sim precisamos de uma normatização e uma política internacional da comunidade em cada vez mais dar olhos a constitucionalidade em detrimento da ordem e da autoridade que a soberania pura e clássica traz. Segundo Colombo (2008, p. 7),

> Em outras palavras, o conceito de soberania, da doutrina francesa, encontra na doutrina contemporânea do direito internacional público seu principal contraponto. Para começar, a soberania é um conceito relativo, por conseguinte, um elemento não essencial do Estado. Segundo, pelo princípio da soberania absoluta não seria possível enquadrar os Estados que se

> submetessem às normas de Direito Internacional como entidades soberanas, já que a soberania significa autoridade suprema.

De acordo com a autora citada acima se retorna a um ponto já trabalhado, sobre o modelo internacional da comunidade em sustentação dos Estados soberanos, pois acaba por ser insustentável múltiplas soberanias presentes ao mesmo tempo no plano internacional. Isso resultaria novamente uma guerra mundial e que não é diferente dos atos realizados pelos Estados no meio cibernético.

Umas das grandes celeumas é o fato de que os Estados exploram o ciberespaço violando a soberania dos demais e justificam a sua atuação no próprio exercício da soberania, ocorrendo uma antinomia entre o instituto jurídico da soberania e o direito. Segundo Ferrajoli (2003) temos a seguinte afirmação:

> Isto porque a soberania, sob a ótica do direito, revelou-se uma categoria antijurídica, porque ela é uma negação do direito, da mesma forma que este é a sua negação. Ou seja, há uma antinomia entre direito e soberania, justamente pelo fato de que o poder soberano dos Estados é desprovido de regras e limites (apud COLOMBO, 2008, p. 8).

Ora, a antinomia instalada entre soberania e direito traz justamente a ideia da relativização já que o direito garante o sopesamento da própria soberania e qualquer outro instituto jurídico que faça parte da personalidade jurídica do Estado perante a sociedade internacional. Contudo a própria defesa da soberania pode ser posta em relação ao direito quando determinados Estados tem esse instituto violado e precisam se reafirmar perante aos demais.

A interpretação na aplicação da soberania também pode ser um contraponto interessante, pois o Estado quando se utiliza da soberania na efetivação dos direitos humanos diante de violações advindas do ciberespaço, mostrando que esse instituto tem dois lados em determinadas situações.

Em 2012 foi aprovado na Assembleia Geral das Nações Unidas através do Conselho de Direitos Humanos, o chamado *Human Rights Council Resolution on Human Rights on the Internet* -A/HRC/20/L.13- traz uma proteção dos direito humanos no ciberespaço, dispondo a seguinte passagem:

> Os mesmos direitos que as pessoas possuem off-line devem ser protegidos on-line, especialmente a liberdade de expressão, a qual é aplicável independentemente de fronteiras e através de qualquer mídia escolhida, de acordo com o artigo 19 da declaração universal dos direitos humanos e o

> Pacto Internacional sobre Direitos Civis e Políticos (apud GUIA DE ESTUDOS ..., 2016).

É mister apresentar não só as consequências diretas de uma guerra cibernética ou atos de guerra advindos do ciberespaço, mas apresentar consequências indiretas que afetam direitos e garantias jurídicas inerentes ao indivíduo. Nesse caso quando determinado Estado através do seu poder de soberania suprimi através do ciberespaço manifestações de opiniões públicas e acaba por modificar de maneira arbitrária a postura política da comunidade internacional ao omitir de maneira totalitária determinadas informações.

O campo de estudo do ciberespaço e as consequências das atuações dos Estados seja através do seu poder soberano, seja través a relativização ao se aplicar ou não a defesa da soberania nos traz um grande alargamento doutrinário em que pontos o Direito Internacional ainda não se firmou ou ainda possui pontos de fragilização.

Toda a sequência de temas trazidos à cima de maneira ou outra desencadeia na responsabilidade internacional, já que se permanece com um foco no Estado em si e na sua soberania, é devido analisar questões além para algo de caráter societário internacional.

Quando se fala de um ato atentatório feito por um Estado a outro, está sendo tratado de um ato que compromete a comunidade internacional como um todo, pois o ilícito internacional ocasionado merece uma responsabilização específica e uma reparação dos danos sofridos pelo Estado violado.

A responsabilidade internacional tem o objetivo de manter a igualdade soberana entre os Estados, e seu tema é regulado pela *Draft articles on Responsibility of States for Internationally Wrongful Acts* – ARSIWA, ou em português, Projeto da Comissão de Direito Internacional das Nações Unidas, trazendo em seu art. 2º a definição de responsabilidade internacional dos Estados (LIMA, 2017).

A obrigação internacional do Estado é um dos fatores que vincula essa responsabilização, porque o ato ilícito, a culpa, o dano, e o nexo causal de certa forma ainda são meios difíceis em se identificar, utilizando provas palpáveis, quando estamos diante de ataques cibernéticos. Governos como o da Rússia no caso da Estônia podem contratar hackers de variadas partes do mundo, especializados em determinados tipos de ataques e encobrir rastros que levem esse tipo de responsabilização a ser apurado na sociedade internacional.

3. NOVOS PARADIGMAS DOUTRINÁRIOS SOBRE A APLICAÇÃO DA JURISDIÇÃO

Foi comentado ao começo do trabalho sobre a incidência da jurisdição na aplicação das leis de um Estado soberano nos limites do seu território estando intimamente ligado ao poder da soberania. Segundo Mazzuoli (2011, p. 665) temos o seguinte conceito de jurisdição: ‘’ o Estado, como se sabe, possui jurisdição sobre todos aqueles que se encontram em seu território. Tal jurisdição é aqui tomada no sentido da extensão espacial em que o Estado exerce sobre os indivíduos a sua autoridade, e não em outro’’.

Com base na citação acima, a extensão espacial acaba sendo um elemento perceptível e palpável, diferentemente quando iniciou-se o estudo no relacionamento do ciberespaço com esse instituto jurídico. Sendo assim a primeira percepção, em parte errônea, que é observada do ciberespaço é de ter uma anarquia, permitindo uma ampla liberdade de atitudes e interações, já que ainda não se teria uma divisão exata jurisdicional/soberana dos Estados gerando um domínio universal. É exposto também o conceito de jurisdição em que Accioly (2012, p. 465) afirma:

> O direito do estado sobre o território e os respectivos habitantes é exclusivo, ou seja, nenhum outro estado pode exercer a sua jurisdição sobre o território, a não ser com o consentimento do primeiro. É bem verdade que a legislação do estado pode prever o exercício de sua jurisdição em país estrangeiro sobre os respectivos nacionais, o que significa que a jurisdição do estado em relação aos estrangeiros não é exclusiva’.

Nota-se que o dever de não intervenção na competência interna dos Estados está perfeitamente conectado com a ideia de vedar e interferência de poder jurisdicional em territórios pertencentes a outros Estados a não ser que os mesmos consintam. A jurisdição por ter um conceito secular e ter sido criada no momento de ascensão soberana na formação nacional dos Estados, tem seu objetivo para solucionar possíveis disputas políticas internacionais naquele século e, aliás, até o século XX antes do surgimento do ciberespaço, esse conceito em seu modelo clássico ainda era aplicável e efetivo para as resoluções das lides.

É importante nos atentarmos que alguns autores utilizam o termo *competência* no lugar de jurisdição. De acordo com Rousseau a competência territorial remete “a competência do estado em relação aos homens que vivem em seu território, às coisas que nele se encontram e aos fatos que aí ocorrem” (ACCIOLY, 2012, p. 465-467). Com o advento do ciberespaço a realidade do Direito Internacional começou a funcionar de outra forma, pois o a

lógica tradicional de aplicação da jurisdição está necessitando de novas linhas doutrinarias para se adequar de forma mais efetiva a esse novo domínio. O elemento físico de território e suas delimitações para possibilitar a aplicação normativa dos Estados ficou em uma zona cinzenta no contexto cibernético. É justamente esse ponto em aberto que o Direito Internacional irá se debruçar para reconstruir uma ligação mais atualizada entre a jurisdição e a sua aplicação no ciberespaço levando em conta uma vasta explicação teórico-doutrinária que será exposta as linhas abaixo.

Embora a área de atuação do ciberespaço obviamente seja em um meio virtual e em função dessa virtualidade resultar falta de limites físicos, a utilização e interação dos entes com este meio é de certa forma real e físico, pois independente de ser uma pessoa jurídica de personalidade de direito público ou privado e de ser uma pessoa física, estes estão vinculados à jurisdição de um Estado que está localizado em um dado continente do globo podendo ser especificado. Com base no que foi dito, deu-se o primeiro passo para possibilitar o entendimento na ligação da jurisdição com o ciberespaço, já que o mesmo faz parte de um meio não real, contudo para manter-se em operação e ser acessado é necessário ter servidores e uma infraestrutura física edificada em algum país (BARROS, 2015).

Existem dois elementos importantes para ser aplicada a responsabilização de maneira apropriada aos Estados assim como os demais violadores de direitos que se utilizaram do ciberespaço como meio. O primeiro elemento seria a localização física dos atores internacionais e o segundo elemento os *links* que conectam as vítimas, entretanto é compreendida a dificuldade para investigar essas violações de direitos através do ciberespaço levando em conta o encobrimento das pistas como qualquer crime. Por isso que o Direito Internacional deve se preocupar em uma cooperação internacional entre os Estados, pois se está deixando o espaço físico e suas limitações, no combate dos crimes virtuais no palco da Era Cibernética (KANUCK, 2010 apud BARROS, 2015).

Cada fração de informação que trafega no ciberespaço está submetida aos interesses do próprio Estado soberano ou as empresas privadas que são proprietárias daquela infraestrutura que sedia e movimenta aquela informação. Não existe um espaço virtual desprovido de uma infraestrutura física que o mantenha sem o patrocínio e gestão de algum ente, e que esteja estabelecida em algum continente do globo, gerando assim um dos pontos cruciais dessa linha de pensamento. Essa estrita limitação física em sua estrutura abre o campo para ser iniciada as primeiras ligações jurídicas entre o ciberespaço, que seria o mundo virtual, e a jurisdição propriamente dita que faz menção ao território dos Estados, sendo o mundo real (BARROS, 2015).

Todos os entes proprietários de aparatos e instrumentos que sejam utilizados para adentrar e compor o espaço cibernético como satélites, cabos de fibra ótica, torres de transmissão, roteadores de *Wifi* entre outros, de maneira implícita ou explícita, quando produzidos e geridos esses proprietários esperam que tenham uma proteção jurídica normativa do Estado soberano que se beneficiou dessa infraestrutura criada. Cai por terra a ideia de uma completa anarquia ao caracterizar o ciberespaço, sendo o mesmo pensado erroneamente como apenas alvo de despejo de informações desprovidas de interesses específicos, que muito pelo contrario tanto as empresas privadas como os Estados soberanos tem um grande interesse de investir economicamente nesse meio. Grandes valores monetários são gastos nos equipamentos mais sofisticados e de ponta para ter-se o maior controle e conquista deste território virtual (BARROS, 2015).

Sendo assim quando é possuido esse caráter físico das infraestruturas que mantém o ciberespaço tanto nas áreas territoriais e aéreas marítimas, é possível uma delimitação mínima de atuação nesses espaços avocando aos Estados soberanos que estejam sediando essas estruturas o seu poder de atuação. Porventura se ultrapassar este dado limite territorial mínimo Estatal é notória a utilização das regras e princípios de direito internacional que irá intermediar possíveis lides (KANUCK, 2010 apud BARROS, 2015).

Citando novamente de maneira rápida o princípio da soberania dos Estados, é observado que sua organização territorial foi realizada com o aval da ONU. Por conseguinte como foi explicado supracitadamente, o liame específico da infraestrutura que compõem o espaço cibernético, como o conceito de jurisdição propriamente dito, gera um déficit organizacional na divisão dos territórios no ciberespaço de maneira exata. Dado que é presente nos indícios mínimos de delimitações, levando em conta infraestruturas físicas estabelecidas em um dado país.

Isso acaba por gerar o principal problema na aplicação das leis dos respectivos Estados soberanos envolvidos em uma guerra cibernética, ou atos de guerra em meio cibernético. Pontualmente essa divisão territorial é altamente complexa e envolve uma série de entraves políticos internacionais, assim como a própria atuação da ONU no meio desse contexto envolvendo a Era cibernética.

Conquanto ainda que o delineamento específico de maneira reconhecida pela ONU e os demais entes internacionais não seja possível efetivamente como um território de um Estado, as transmissões de mídia e os sinais de comunicações sem fio podem contribuir como indícios limítrofes para um mapeamento estatístico futuro, de qual Estado está tendo aquele quantitativo de informações sendo trocados no meio cibernético. Em outros termos serve

como um molde para ter-se uma noção gráfica do globo dentro do ciberespaço. É importante perceber que a União Internacional de Telecomunicações (UIT), agência da ONU especializada em tecnologias de comunicação e informação, possui diretrizes que estabelecem determinadas frequências eletromagnéticas de comunicação e proíbe a prática de qualquer ato de interferência não autorizada.

Observa-se que o reconhecimento de determinada região do ciberespaço ainda não é concedida como território de um Estado soberano, mas a ONU já começou a implementar mesmo que de maneira embrionária uma noção inicial de introdução a uma organização mínima no ciberespaço.

3.1 O poder soberano e jurisdicional do estado nas violações dos direitos humanos presentes no ciberespaço

Abre-se um pequeno tópico para tecer comentários sobre a violação de direitos humanos que ocorre no espaço cibernético, começando do próprio Estado soberano que sedia aquela infraestrutura e mantém tal campo do ciberespaço em operação. À vista disso, a soberania assim como a jurisdição, que se tem trabalhado neste capítulo, é um poder que o Estado detém na aplicação de suas leis nos limites do seu território.

Essa violação inicia-se quando alguns Estados em nome da segurança tomam a decisão de ingerir-se no conteúdo de certas informações eletrônicas e controlando de forma absolutista o que pode ser acessado pela população. A título de exemplo temos na China o projeto Escudo Dourado que é subdividido em 12 programas governamentais, com um grande investimento de capital humano especializado, visando criar um ‘’Grande *Firewall*’’ para fazer uma triagem de conteúdos informacionais que poderão adentrar no espaço cibernético chinês, impedindo a população de ter um acesso maior aos conteúdos do ocidente (CEIRI NEWSPAPER, 2017).

É notório que o instituto da soberania e da jurisdição é utilizado de maneira arbitrária como justificação para violação dos direitos garantidos por um Estado Democrático de Direito em prol da segurança de informação internacional restando contraditório e oportunista certos privilégios de poder que o Estado possui. Apesar de não ser o foco do trabalho, estudar violações dos direitos humanos através do ciberespaço, é importante ter noção de que tipo de bandeira está sendo levantada para a defesa de uma ameaça cibernética e até que ponto a restrição de maneira autoritária de conteúdos cibernéticos podem ser limitados á população com base na soberania e jurisdição dos Estados.

Segundo Barros (2015), um dos maiores desafios para o direito internacional é possibilitar que a execução e o controle da soberania sejam eficientes para que as normas jurídicas tenham a capacidade de responder adequadamente aos atos violadores de direitos realizados no ciberespaço, que consequentemente, seria a guerra cibernética. De maneira bastante pragmática podemos dizer que a proibição do uso da força assim como a utilização da guerra, por exemplo, servem como princípios dentre vários outros no direito internacional nos casos de dificuldade na aplicação da jurisdição nacional.

3.2 A interpretação dos condomínios globais no âmbito do ciberespaço

Com base no pensamento acima construído, uma delimitação mínima no ciberespaço geraria uma aplicação melhor e mais acertada da soberania e jurisdição, devendo ser olhada a ideia do ciberespaço como um domínio público *su generis*. Portanto é possuída uma vinculação dos Estados soberanos a esse meio e ao mesmo tempo esse viés cibernético é tão vasto que vai além dos próprios Estados, se transformando em um elemento que faz parte da comunidade internacional, vital para o globo no século tecnológico que vivenciamos. O ciberespaço se tornou um grande meio de interação entre os indivíduos, tornando-se um meio de profunda interdependência entre os Estados e uma grande interferência dos atores não estatais (BARROS, 2015).

Por efeito, Posen (2003 apud BARROS, 2015, p. 115-116):

> [...] define os espaços comuns mundiais, como o mar, o espaço e o ar, pela expressão em inglês de ‘global commons’, aqui traduzida como ‘condomínios globais’. Essas áreas “não pertencem a nenhum Estado e fornecem acesso para grande parte do globo”.

De acordo com a citação a cima resta a dúvida se o ciberespaço pode ser caracterizado ou não como um condomínio global, já que em certos pontos é possível visualizar uma ligação com os entes internacionais e em determinados momentos é observada uma grande abertura como se fosse de um domínio público pertencente à comunidade internacional. É visto a defesa de Stein no posicionamento do ciberespaço ser um condomínio global, justamente porque os Estados soberanos tentam delimitar áreas de atuação pertencentes a sua jurisdição dentro do ciberespaço (STEIN, 2003 apud BARROS, 2015).

No caso de Glenny, se entra em uma discussão mais aprofundada, porque o ciberespaço para ser entendido como condomínio global, acaba necessitando de um conceito formado de maneira bastante delineada para o direito internacional. Isso significa que o conceito de espaço global é um principal alicerce na formação das características do condomínio global para assim ser possível o apontamento do ciberespaço inserido no contexto do Direito Internacional (GLENNY, 2011 apud BARROS, 2015).

Barros (2015, p.116) afirma da seguinte maneira sua visão do ciberespaço nessa temática:

> Provavelmente, pode-se perceber características de um espaço global, mas um domínio global diferenciado dos outros domínios do mar, espaço e ar. Os domínios comuns globais geralmente são regulados pelo Direito Internacional, de forma satisfatória, dentre os Estados.

Dessa maneira o condomínio global seria uma junção de conceitos na formação de um híbrido entre aquilo que é regulado pelo Direito Internacional, sendo as áreas comuns no globo ou espaços globais (os espaços aéreos, marítimos e cósmicos), e as áreas que são submetidas à jurisdição e soberania dos Estados.

O elemento habitualidade explica bem essa característica híbrida na elucidação do condomínio global, pois a título de exemplo se tivermos em mente de forma singular que cada indivíduo não utiliza essas áreas internacionais como viajar de avião ou de navio todas as horas, e de fato ocorrendo algum tipo de problema quem em primeira mão irá ditar as normas desses espaços será o direito internacional. No caso do ciberespaço é observada uma grande diferença porque este meio é utilizado todos os dias, todas as horas por vários entes internacionais que possuem diversas características (BARROS, 2015).

É tão forte a característica *sui generis* do ciberespaço que sua composição é dotada por regulações nacionais dos Estados soberanos e internacionais pelo direito internacional preconizado principalmente pela ONU. Toda essa multiplicidade de normas e atores internacionais nos dá um ponto forte na característica do ciberespaço, já que toda a sua regulação ainda não sofreu uma legitimação cristalizada diante de inúmeros fatores políticos internacionais que levantam essa complexidade.

Na medida em que se abre o acesso a Internet para realização dos direitos humanos, de fato está sendo definindo o ciberespaço como um condomínio global. Contudo o preço que se paga, em sua heterogeneidade, é alta levando em conta vários tipos de problemas, como

ameaças de diversos pontos, vindo de empresas privadas contratadas, *hackers* e o próprio governo.

Diante disso a reprimenda mais objetiva e fácil é a restrição e controle dos usuários que utilizam o ciberespaço, violando-se os direitos humanos. A segurança cibernética pode ter tanto efeitos positivos como negativos, porém sempre dever ser observado uma democracia mínima para um bom convívio, permitindo que o ciberespaço seja um domínio que efetive essas garantias a todos os usuários

O condomínio global no ciberespaço deve ser um instituto reinventado, analisando as pluralidades tanto dos Estados soberanos como sua relação com a comunidade internacional. A humanidade é o principal interessado para gerir esse condomínio global, sendo os Estado soberanos, usuários do ciberespaço, empresas privadas, ONGS entre outros.

Em um grande resumo toda a comunidade internacional foi beneficiada pelo advento do ciberespaço, nada seria mais justo e equilibrado que um controle menos concentrado em mãos de poucos. Contudo nota-se que a luta pelo poder sempre é constante e não termina, Estados soberanos como os Estados Unidos da América galgam a todo custo uma hegemonia em quase todos os domínios e isso não seria diferente no ciberespaço.

A característica *sui generis* do ciberespaço resulta em atuações legitimadas pela soberania e jurisdição dos Estados em áreas do ciberespaço que tiveram as bases das suas infraestruturas físicas fincadas mantendo esse espaço em operação. Entretanto as áreas limítrofes, sendo os condomínios globais, possuem a incidência de poder dos Estados de forma lacunosa, justificando grande parte da problemática do Direito Internacional no estudo na sua aplicação normativa e concedendo uma efetivação mais acertada desses poderes.

A busca pelo controle do *global commons* são um dos fatores principais que movimentam a expansão do investimento tecnológico dos Estados para ganhar mais poder hegemônico na comunidade internacional. Sendo assim, atingidos os controles dos espaços comuns, consequentemente os Estados acabam por ter em mãos o comando político, econômico e militar na escala internacional mantendo sua força hegemônica.

É visto que o resultado dessa adição de fatores inevitavelmente desagua na guerra cibernética, já que os Estados que seriam adversários não teriam um controle efetivo e bem condensado da economia, da política internacional e da força militar, ficando em ponto de desvantagem, tendo que se curvar a atuação do Estado hegemônico. O controle dos condomínios globais sem dúvidas será um lugar de destaque na Era da informação, onde a guerra cibernética será um grande palco de disputas pelo poder e sua influência pelo ciberespaço (POSEN, 2003 apud BARROS, 2015).

Segundo Barros (2015), no ponto de vista da economia política a ausência de normas reguladoras e a anarquia sistemática são totalmente contrárias a um modelo que o direito internacional propõe de legalização do ciberespaço como um condomínio global sem resultar em um excessivo combate pelo poder buscando uma hegemonia política.

Notam-se duas conjecturas que o direito internacional necessita ter como sustentação para esse domínio global: a primeira é a inevitabilidade protetiva dos recursos físicos que difundem as informações, sendo consequentemente protegidos pelos direitos de propriedade privada. A segunda é a indispensabilidade na identificação positiva de quais são os tipos de usuários que utilizam o espaço cibernético sendo legítimos ou não, contando no caso de ilegítimos temos a sua exclusão sempre levando em conta o cuidado com a proteção dos direitos humanos (BARROS, 2015).

É observado que esse tipo de sistemática para uma operação harmônica do condomínio global, necessita de investimentos econômicos vindo de diversos entes, para que não tenhamos um único investidor beneficiário de seus próprios investimentos. O ideal seria um condomínio global com gastos de manutenções acessíveis, para que todos os entes internacionais possam participar desse controle sem se submeter de maneira econômica ao mando de Estados mais fortes que exploram essa fraqueza dos Estados mais fracos. Infelizmente uma das grandes objeções do ciberespaço é essa, uma área em que poucos investem muito por terem um poder econômico e político elevado, e que muitos não investem ou investem pouco por dependerem economicamente, politicamente e tecnologicamente de Estados mais fortes impedindo a difusão dessas novas tecnologias de maneira mais democrática.

Sendo assim mesmo existindo todas essas complexidades que envolvem os *global commons* podemos fazer analogias a determinados fatos que apareceram para o Direito Internacional como um norte na orientação sobre como conceituar os condomínios globais e como o Direito Internacional poderá resolver os conflitos inseridos dentro desse novo domínio que é o ciberespaço.

No primeiro exemplo tem-se o arquipélago polar de Svalbard localizado ao norte da Noruega situado no oceano ártico. O arquipélago é ordenado pela soberania norueguesa em função do Tratado de Svalbard, sendo assinado em Paris após a primeira guerra mundial no dia 9 de fevereiro de 1920, pretendendo diminuir tensões políticas pós-guerra principalmente com a União Soviética (KANUCK, 2010 apud BARROS, 2015).

O tratado reconhecia a soberania da Noruega sobre Svalbard, porém a mesma era mitigada em alguns pontos, uma vez que o regime jurídico específico permitia que os demais

países signatários do tratado pudessem ter acesso aos recursos naturais do arquipélago, assim como realizar pesquisas científicas beneficiando a comunidade internacional.

Por outro lado a Noruega tem a responsabilidade jurídica e o dispêndio econômico de administrar grande parte do território como: cobrar taxas para a manutenção do arquipélago, entretanto o orçamento desta manutenção é feito à parte da Noruega continental; Proibir a discriminação, pois todos os indivíduos e empresas dos países vinculados ao tratado podem ter acesso e se estabelecer no arquipélago, contudo atos de discriminação a estrangeiros são acobertados pela jurisdição norueguesa; E por ultimo a desmilitarização, sendo vedada a utilização de armas e qualquer tipo de atividade militar nas ilhas, sendo um território neutro. Observamos que todos esses direitos e obrigações atribuídas à Noruega fazem parte de uma soberania incompleta com o objetivo de preservação dos recursos naturais e equilíbrio político entre os Estados soberanos que fazem parte do tratado mantendo de pé os interesses da sociedade internacional (MINIONU, 2018).

Com base no exemplo acima, Ferrajoli (2002, p.52) traz em seu livro o capítulo nomeado de ‘’a crise hodierna da soberania’’, tecendo o seguinte comentário:

> [...] acreditamos que cabe à cultura jurídica e política apoiar-se naquela ‘’razão artificial’’ que é o direito, e que já no passado moldou o Estado em suas relações internas, para indicar as formas e os percursos: os quais passam, evidentemente, através da superação da própria forma do Estado nacional e através da reconstrução do direito internacional, fundamentando não mais sobre a soberania dos Estados, mas desta vez sobre as autonomias dos povos.

Uma nova reflexão da soberania na visão de Ferrajoli toma forma, pois a mesma ao invés de ser uma satisfação absoluta e plena do poder Estatal sobre os demais começa a sofrer limitações em função de inúmeras complexidades políticas, econômicas e históricas (no caso do arquipélago de Svalbard), com o principal objetivo de se atingir a autonomia dos povos. Por consequência chegando até a temática do estudo do ciberespaço.

Ferrajoli (2002) também traz outra consideração com base no paradigma do velho Estado soberano. Pois o mesmo em relação a pequenas coisas é grande demais e em contrapartida, para coisas grandes é demasiadamente pequeno. Destarte, a sua função de administrar, legislar e julgar demonstram essa grandiosidade, como foi elucidado no exemplo prático acima. Entretanto o cerne dessa explicação está no seu seguinte posicionamento:

> Mas sobretudo, o Estado é pequeno demais com respeito às funções de governo e de tutela que se tornam necessárias devido aos processos de internacionalização da economia e às interdependências cada vez mais sólidas que, na nossa época, condicionam irreversivelmente a vida de todos os povos da Terra (FERRAJOLI, 2002, p.50).

A complexidade de inúmeros fatores que envolvem o arquipélago forçou o Estado norueguês a reformular o funcionamento de sua soberania, dividindo seu poder com a sociedade internacional. Esse instituto começando a ser sopesado com diferentes escalas satisfativas, levando em conta a questão multilateral de interesses globais, inicia uma revitalização das visões que o Direito Internacional pode ter em relação ao poder soberano. Entretanto, existe uma série de questões melindrosas que envolvem esse processo de relativização de um poder tão forte e senão o mais supremo de um Estado.

No segundo exemplo temos o domínio marítimo sendo assemelhado a um condomínio global e sua sistemática de funcionamento no tráfego marítimo internacional parecido com o ciberespaço. Os Estados possuem o poder da soberania, apesar disso os mesmos não possuem um controle absoluto desse meio, ocorrendo uma equalização de poderes entre os entes, pois a navegação internacional precisa ser mantida um nível de pacificidade. Essa balança constante põem de um lado o peso do poder absoluto dos Estados e de outro a utilização do espaço marítimo por toda sociedade internacional de maneira ordeira por um bem comum de todos, resultando a essência do que seria um condomínio global (KANUCK, 2010 apud BARROS, 2015).

De acordo com os exemplos citados a cima, o objetivo de se investir na segurança e desenvolvimento do ciberespaço é parecido com a dinâmica dos condomínios globais, se tornando um grande desafio para uma organização desse domínio. Entretanto os Estados e organizações internacionais mais fortes sempre buscam de forma sedenta aumentar a sua escala de poder perante a sociedade internacional, conquistando e anexando novos domínios ou territórios para a sua atuação soberana e jurisdicional. Sendo assim afastando o propósito e obrigação internacional de proteger, administrar e investir nesse meio tão essencial no século XXI que é o ciberespaço.

Em outro giro segundo Barros (2015), as ameaças realizadas através de ataques cibernéticos ou a guerra cibernética propriamente dita, podem induzir esses Estados mais fortes e investidores desse meio a se protegerem e consequentemente proteger uma boa parcela da sociedade internacional, resultando querendo ou não a efetivação da obrigação internacional de proteção.

Posto isto, o conceito de condomínio global sendo relacionado com o ciberespaço tende a abrir uma nova visão, como por analogia ao direito de propriedade em que temos vários poderes inerentes a mesma e que podem ser divididos de acordo com determinada ocasião, da mesma forma com a relativização da soberania. Essas formas de compartilhar o poder e atuação dos Estados em diferentes jurisdições é o que forma o *global commons*, como ocorre nos espaços marítimos, aéreos, espaciais e que devemos começar a inserir e ampliar este conceito para o ciberespaço.

3.3 A aplicação do direito transnacional nas relações que permeiam o ciberespaço

Assim como os condomínios globais, é abordada também outra visão doutrinária no Direito Internacional a fim se ter uma normatividade jurídica voltada à nova realidade da globalização que é vivenciada no século XXI.

Essa nova visão que está sendo estudada no Direito Internacional é chamada segundo Gunther Teubner (2003) de direito transnacional ou *global law*. Contempla-se que esse fenômeno da globalização formou os UNO's ("*unidentified normative objects*") ou objetos normativos não identificados como, por exemplo, o Manual de Tallin explicado anteriormente no trabalho.

As relações jurídicas cada vez mais complexas entre vários entes internacionais causam uma série de interferências multilaterais de ordens normativas diferentes, restando fragmentar paulatinamente a aplicação do direito nas questões de soberania e jurisdição através de um Estado-Nação, se tornando cada vez mais difícil a sua aplicação. Os UNO's são fruto de uma convergência normativa de diferentes atores no mundo globalizado possuindo uma imparcialidade na sua criação de regras em relação aos reflexos políticos advindos dos Estados ou grupos político-econômicos controlados por esses Estados (BARBOSA E MORSCHEN, 2016).

O direito transnacional vai além da soberania e jurisdição dos Estados, abandonando a ideia de que os Estados-Nação seriam umas das únicas instituições com atribuições de criar, ordenar e aplicar o direito. O paradigma do estado-centrismo necessita ser quebrado dando lugar a uma nova visão jurídica da globalização e as consequências complexas que o ciberespaço traz para o direito internacional e transnacional. Segundo Gunther Teubner implantamos ‘’uma guerra de crenças a respeito da transnacionalização do direito’’, gerando uma corrente ideológica que o direito pode prescindir a qualquer Estado soberano, e outra corrente que afirma a impossibilidade de o direito existir sem um Estado (BARBOSA E MORSCHEN, 2016).

Isso resulta e uma longa retrospectiva jurídica pela história do direito que reflete nas doutrinas baseadas no ‘’contrato social’’, porém o advento de novas formas de poder global como o ciberespaço está começando a modificar os comportamentos dos entes internacionais, e os conduzindo a adotar medidas que permitem conceber a existência de normas jurídicas transnacionais indo além das fronteiras jurisdicionais e dos poderes soberanos dos Estados (BARBOSA E MORSCHEN, 2016).

Teubner explica que a Teoria do Pluralismo jurídico é um dos principais pontos de apoio para a sustentação do *global law*, ressaltando o termo redes de comunicação. Vejamos a seguinte passagem que demonstra esse pensamento:

> Claramente, o mundo da vida de diferentes grupos e comunidades não é a principal fonte do direito global. Teorias de pluralismo jurídico terão que reformular seus conceitos fundamentais, mudando seu foco de grupos e comunidades para discursos e redes de comunicação (ver Teubner, 1992:.1456ff). A fonte social do direito global não é o mundo da vida das redes pessoais globalizados, mas o proto-direito de redes especializadas, organizativa e funcional que estão formando uma identidade global, mas fortemente limitado. O novo direito vivo do mundo é alimentado a partir da auto-reprodução contínua de altamente técnica, altamente especializada, muitas vezes formalmente organizadas e bastante restritas, redes globais de natureza económica, cultural, académica ou tecnológica (TEUBNER, 2003 apud BARBOSA E MORSCHEN, 2016, p.152).

As mudanças na sociedade ou em grupos sociais deixam de ser a força motriz que modifica o direto global, e a tecnologia que nesse caso está sendo analisada como o ciberespaço, abre uma nova realidade vivenciada pelos atores internacionais, ocasionando em uma criação jurídica que se preocupe em uma sistematização altamente técnica e especializada com o fito de respaldar de maneira eficiente as inúmeras incertezas que ainda possuímos diante do surgimento do ciberespaço na sua utilização pelos Estados como um poder global que tem várias faces.

Não só o ciberespaço, mas a *lex mercatória* é um exemplo nas formas de comunicações de redes especializadas, que são utilizadas no comércio internacional deixando de lado a aplicação extremamente limitadora das normas jurídicas Estatais e dando espaço a um sistema normativo jurídico independente da jurisdição e soberania, como se fosse um sistema que transita pelo direito legitimado pelo Estado e pelo direito internacional.

Por consequência essas redes especializadas na esfera transnacional forçam os Estados soberanos a se curvarem diante da nova realidade. Sendo assim a perda de sua soberania é aparente, e Benoit Frydman, em “*A Pragmatic Approach to Global Law*”,afirma:

> Em um mundo sem um soberano, os Estados são obrigados a se comportar como atores, entre os demais. O Estado, soberano (até certo ponto) no seu próprio

> território, perde toda a soberania (apesar do que diz o direito internacional público) assim que atravessa fronteiras e deve comprometer-se com outras forças. Estas forças são de outros Estados, é claro, mas também de outros tipos de atores da sociedade do mundo, como as organizações internacionais e as organizações não governamentais, ou empresas de transição e suas redes (FRYDMAN, 2013 apud BARBOSA E MORSCHEN, 2016, p.153).

Percebe-se que o pluralismo jurídico trás uma nova visão do que é o direito transnacional superando a ideia soberana como escala unanime dos atores na sociedade internacional, formando um painel composto de vários sistemas jurídicos inter-relacionados. A Teoria do Pluralismo Jurídico transnacional é o elemento vital que faz o *global law* ou o direito transnacional se conectar com os demais fatos ocorrentes com a gênese do ciberespaço e seus demais debates a respeito da possibilidade de uma normatização e uma superação de institutos jurídicos seculares como a soberania e jurisdição.

De acordo com Teubner, as normas produzidas pelo direito transnacional assim como a ideia de condomínio global, são sistemas jurídicos *sui generis*. Nesta particularidade de gênero próprio se tem três teses que validam esse ordenamento, na primeira tese que já foi exposta, a Teoria do Pluralismo Jurídico, dá ênfase nas formas de comunicação e redes especializadas (TEUBNER, 2003 apud BARBOSA E MORSCHEN, 2016).

Na segunda tese é constatado que por o direito transnacional possuir uma característica *sui generis* não pode ser conjecturado levando em conta pressupostos normativos de sistemas jurídicos nacionais, de maneira que quando é criada a norma jurídica baseada no direito transnacional a mesma não deve partir de uma construção nacional através de processos legislativos e uma série de atribuições estatais que legitimem aquela norma no Estado-Nação. Por fim na terceira tese levando em conta a política internacional, é defendido a ideia do direito transnacional ser desprendido de qualquer tipo de política, pois como foi comentando anteriormente no trabalho o Direito Internacional especificamente na guerra cibernética sofre um grande problema de os Estados violadores dos direitos de outrem no ciberespaço fazerem parte do conselho de segurança da ONU, restando à parcialidade nas decisões políticas que envolvam alguma regulação cibernética que passe pela chancela da ONU. É apresentada a seguinte passagem realizada por Teubner:

> A relativa distância à política internacional e ao direito internacional não preservará o “direito mundial sem Estado” de uma repolitização. Muito pelo contrário: justamente a reconstrução de (trans) ações sociais e econômicas como atos jurídicos globais solapa o caráter apolítico do direito global e fornece dessarte o fundamento da sua repolitização. Ela, porém, ocorrerá previsivelmente sob novas formas, pouco conhecidas até agora. Suspeito que o direito mundial não será repolitizado por

> instituições políticas tradicionais, e.g. de natureza por assim dizer parlamentar, mas justamente pela via daqueles processos nos quais o direito mundial se "acopla estruturalmente" a discursos altamente especializados, isolados (TEUBNER, 2003 apud BARBOSA E MORSCHEN, 2016, p.155).

Os elementos de discursos altamente especializados são um dos pontos mais fortes que afastam a influência política na manutenção de uma imparcialidade internacional na criação dessas normas jurídicas do direito global. Em outras palavras a repolitização do sistema internacional só será permitido levando em conta a essas novas formas de regulações ao redor do globo, nesse caso, por exemplo, a *lex mercatória* e a dinâmica do ciberespaço que está em formação.

Permanecendo nessa mesma linha observamos que tanto para a aplicação do direito transnacional como a ideia de regulação jurídica do ciberespaço temos elementos que os identificam, segundo a classificação de Viellechner:

> O direito transnacional deve ser entendido como direitos (1) transfronteiriços, ainda que não se refiram necessariamente a questões globais, (2) tanto às relações de indivíduos como também de objetos regidos pelo interesse comum, pelo qual geralmente se restringem a áreas individuais (*Sachbereiche*), e (3), predominantemente, mas não exclusivamente, é definido por atores não-estatais em forma de contrato (TEUBNER, 2015 apud BARBOSA E MORSCHEN, 2016, p.155).

A reflexão que fazemos desses elementos é que eles estão à frente tanto da criação sistemática normativa vinculadas a um Estado, como a sua aplicação está fora do alcance efetivo das mãos do Estado, levando em conta a descontinuação da soberania e jurisdição como fatores únicos e essenciais de controle, tomando como base a cultura de um Estado como centralizador e legitimador de sistemas jurídicos.

O direito transnacional e o ciberespaço passam a serem fatores que são de interesse de todos os entes da comunidade internacional, porém a sobreposição de poderes absolutos e politizados dos agentes internacionais não se sustentam mais, de acordo com a necessidade de se criar uma normatização especializada e global voltada para a nova realidade tecnológica na globalização e os reflexos políticos e econômicos que essa complexidade traz.

4. O CIBERESPAÇO E OS JOGOS DE PODERES NO DIREITO INTERNACIONAL

Neste capítulo será iniciada uma série de análises que partem de diferentes pontos de estudo sobre o ciberespaço e seu poder. Como foi mostrado na introdução do trabalho, é apresentado um breve conceito sobre este novo domínio, sendo assim no intuito de reforçar uma explicação mais profunda e direcionada trazemos outros conceitos de diferentes autores.

Segundo Kuehl o ciberespaço é explicado como:

> Um domínio operacional dentro do ambiente de informação cuja distinta e única característica é enquadrada pelo uso de eletrônicos e espectros eletromagnéticos para criar, armazenar, modificar, trocar e explorar informações via redes interdependentes e interconectadas usando tecnologias de informação/comunicação (KUEHL, 2009, apud GARDINI, 2014)[4].

Tem-se em vista que o elemento informação é o fator importantíssimo como movimentador, estruturador e alimentador desse sistema de comunicações, composto por elementos tecnológicos. É ressaltado o fator informação para o ciberespaço porque aquele acaba por formar no século atual uma nova forma de poder global, já que o mesmo ultrapassa fronteiras físicas e modifica de maneira muito rápida a percepção jurídica do direito internacional a respeito desse domínio.

Essa rápida evolução do ciberespaço é constatada pela redução drástica de custos na fabricação de itens tecnológicos, levando em conta a globalização no comércio internacional e a instalação de empresas multinacionais nos países emergentes, favorecendo um capitalismo agressivo na produção massificada dos componentes vetores ao ciberespaço.

Como consequência, é aberto um leque formando uma multiplicidade de atores internacionais utilizadores desse domínio cibernético, porém ao contrário do que o senso comum idealiza a internet não é o ciberespaço propriamente dito, porque o fator informação é o que caracteriza este domínio, ou seja, o mesmo já existia muito antes da internet em razão de telefones móveis ou fixos, rádio, sistemas de comunicações aéreas e marítimas, redes de telégrafos, televisão via satélite e outros, já faziam a função de transmitir informações. Destarte a internet teve seu surgimento atrelado à criação da computação eletrônica interligando os computadores e suas respectivas redes entre si em uma escala mundial, de forma que a sua estrutura e funcionamento é formada por várias camadas sendo estas:

---

[4]Tradução livre do original: "Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."

> A camada inferior é composta pelos elementos físicos que dão suporte às conexões, ao fluxo e ao armazenamento de dados que circulam em formato digital. São componentes da camada inferior, por exemplo, as linhas telefônicas, os cabos de conexão, as antenas de transmissão, os satélites, os servidores, etc. A camada superior, por sua vez, é composta por informação. A informação é codificada e decodificada por padrões técnicos e lógicos que compõem a camada intermediária da Internet. Em outras palavras, a informação é traduzida na camada intermediária, de padrões compreensíveis por seres humanos para padrões computacionais, e vice-versa. O uso e a partilha da informação por diferentes usuários através de diferentes aplicações (e-mail, sítios Web, telefonia VoIP, troca de arquivos P2P, entre outras) gera ainda uma quarta camada, um espaço vastíssimo de interações e formação de redes sociais, econômicas e políticas que se desenvolve de forma transnacional e impõe múltiplos desafios aos processos de governança política nos planos nacional e internacional (EISENBERG E CEPIK, 2002, MUELLER, 2002; MALCOLM, 2008 apud CANABARRO E BORNE, 2014).

Deste modo entendemos que a internet é um conjunto de camadas que tem características físicas e informacionais altamente complexa, possuindo inúmeras funções que ampliam o ciberespaço ao redor do globo. Essas junções das camadas combinadas com o ciberespaço consolidam seu poder na escala internacional resultando no século atual uma busca desenfreada por esse novo poder pelos Estados e demais organizações pelo mundo.

Ainda nessa linha segundo Starr (2009 apud GARDINI, 2014, p.11), o "poder cibernético é definido como a habilidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e através de instrumentos de poder.[5]" Essa passagem traduz perfeitamente o porquê dos entes internacionais atualmente buscarem tanto ter o domínio potencial do ciberespaço, visto que a manipulação de informações através desse meio controlam os sistemas econômicos, políticos e cultuais, desencadeado um novo conceito de poder visto no direito internacional que é o *smart power*.

Antes se falar do *smart power* propriamente dito deve-se ter noção das proporções que foram tomadas para se chegar a essa escala de poder que transformou completamente a dinâmica das relações internacionais. O fenômeno da globalização reflete o progresso do conhecimento humano no aperfeiçoamento científico e tecnológico, fazendo o homem obter conquistas jamais imaginadas pela humanidade, transformando completamente a maneira como se vive na sociedade e principalmente as relações complexas que a sociedade internacional tem e passa a ter com o impacto dessas evoluções tecnológicas.

As sucessivas e inúmeras interações efetivadas pelo aperfeiçoamento tecnológico restam por abrir diversos questionamentos sobre o sistema normativo tradicional sustentado pelo Direito Internacional. Pois sua construção, que foi concebida com base no poder

[5] Tradução livre do original : "[…] the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."

soberano dividido e tolerado pelos Estados na comunidade internacional, tal qual sua centralização como legisladores, executores e julgadores das normas em comum acordo no Direito Internacional, necessitam de uma revitalização normativa e doutrinária com base nas evoluções tecnológicas presentes no século atual.

Entretanto essa ideia de Estado legitimador dessa ordem jurídica no direito internacional começa a cair por terra com base nas novas correntes doutrinarias que estudam a transnacionalidade do direito quebrando essa lógica linear clássica que observamos no mundo jurídico. Atrela-se essa preocupação do Direito Internacional com a globalização e suas transformações na sociedade internacional, porque cada vez mais os Estados investem no aperfeiçoamento de novas tecnologias que interferem diretamente nessas relações internacionais, de forma que essas tecnologias somadas com o vetor informação caracteriza o ciberespaço como uma nova fonte de poder. Segundo Barros (2015) observamos a seguinte passagem:

> As grandes potências raramente estão satisfeitas com a distribuição de poder; pelo contrário, enfrentam um incentivo permanente para a alterarem o equilíbrio de poder ao seu favor. Têm, quase sempre, intenções revisionistas e usam de todos os meios necessários para a obtenção de mais poder, caso concluam que isso pode ser realizado com um custo razoável. Por vezes, os custos e os riscos de tentar alterar o equilíbrio de poder são muito elevados, ao forçar as grandes potências a aguardar circunstâncias mais favoráveis, ou tentar aumentar a sua influência sem o uso do poder militar (MEARSHEIMER, 2007 apud BARROS, 2015, p.70).

Com base na passagem acima nota-se que o ciberespaço como uma nova forma de poder é constatada perfeitamente, pois levamos em conta o capitalismo agressivo na produção massificada de componentes eletrônicos acessíveis em função de um custo baixo que viabilizam o acesso ao ciberespaço. Isso se torna um incentivo nos investimentos realizados pelas grandes potências em aperfeiçoar esse vetor cibernético na utilização de informações que os favoreçam.

É muito mais rentável uma grande potência investir no ciberespaço e ter o poder informacional de coagir determinados entes internacionais a contribuir com seus interesses, do que presenciarmos um grande impacto internacional de um Estado coagir outrem ou ameaçar diretamente por meios militares.

De acordo com Nye (2010), ter poder é sinônimo de possuir habilidade para influenciar outros atores internacionais para atingir determinado objetivo dentro nas relações internacionais. Existem duas maneiras de afetar esses atores internacionais: temos a utilização de procedimentos de persuasões culturais e ideológicas que são chamados de *soft power* e o uso da força militar ou econômica chamados de *hard power*. Esses são os principais meios

(persuasão, coerção e suborno) utilizados nas relações internacionais para ter-se a dominação de determinado interesse em relação aos outros entes internacionais (BARROS, 2015).

Em vista disso o *soft power* ou o poder brando é utilizado de uma forma mais suavizada sem criar muitas polêmicas politicas no meio internacional, impondo a vontade do Estado a outros entes internacionais ou os próprios Estados nas suas relações. A diplomacia, os mecanismos de parcerias e assistências econômicas, reuniões entre os representantes dos Estados promovendo uma comunicação pacífica, são praticas adotadas nesse tipo de poder sendo consideradas vitais levando em conta que o *hard power* por si só é incapaz de promover a defesa de ideologias e interesses dos Estados na esfera internacional (NYE JR, 2010 apud BARROS, 2015).

A carta da ONU traz logo em seu artigo 1º a promoção da paz nas relações internacionais, sendo este proposito um ‘’dever ser’’ na doutrina do Direito Internacional efetivando o *soft power* com uso especial da diplomacia. Sendo assim na realidade da política internacional que se vivencia, os Estados se utilizam tanto do *hard power* como do *soft power* ao mesmo tempo para influenciar e alcançar seus objetivos perante aos demais Estados soberanos.

Contudo muito antes de ser notada a incidência de um poder brando nas relações internacionais, no século passado era o poder militar que trilhava essas relações já que naquele tempo as outras formas de poder (econômico e informacional) não eram muito visualizadas. Com o avanço das tecnologias, aperfeiçoamento das relações econômicas e a várias outras mudanças que a humanidade vivenciou, é de se notar que o poder militar foi descentralizado dando espaço no século atual a outras formas de poder atuantes pelo globo.

Segundo Nye (2010 apud BARROS, 2015), essa distribuição de poderes em decorrência da descentralização do poder militar pode ser equiparada a um jogo de xadrez tridimensional. Sendo primeiro plano caracterizado pela incidência do poder militar, como foi falado anteriormente, nas relações internacionais possuindo como principal exemplo da atualidade os Estado Unidos da América como o único Estado com potencial militar para atuar no globo inteiro.

No segundo plano temos o poder econômico formado por vários blocos como a União Européia por meio de unificação de moeda sendo o euro, a China se utilizando modelo socialismo de mercado e sua política econômica de produção massificada, no oriente médio tendo países como os Emirados Árabes Unidos detendo umas das principais *commodities* que controlam a economia sendo o petróleo. No terceiro plano temos todos aqueles fatores que vertem o controle de feitio eficaz dos Estados, como ataques terroristas, desastres ambientais,

crises econômicas impremeditáveis e outros eventos que são imprevisíveis. Reunindo todos esses planos, temos por observar que sua distribuição é complexa de maneira que um se debruça sobre o outro casuisticamente, descaracterizando a visão militar que se tinha no século passado das relações internacionais.

Por mais que os demais Estados tenham um fortíssimo poder influente em um desses planos, nada adianta se o mesmo não possui habilidade suficiente para jogar esse jogo de xadrez organizando adequadamente e objetivamente o direcionamento desses elementos planificados (*hard power e soft power*) na obtenção de resultados.

Com base nesse direcionamento de maneira objetiva dos poderes citados no paragrafo anterior, tem-se a ideia inicial do *smart power* ou poder inteligente. Os Estados Unidos em sua política internacional é um grande exemplo desse tipo de poder, estando suas relações internacionais pautadas na utilização dos meios militares, sanções econômicas e nos meios mais pacíficos como cooperações internacionais, ou seja, existe uma aplicação mesclada do *hard power e o soft power*. Enfatiza-se que para a consecução do *smart power* seja feita, deve ser observada sempre a estratégia entre esses dois poderes, pois segundo Nye, (2010 apud BARROS 2015) a vinculação do poder na escala internacional não se dá apenas na análise do poder militar/bélico de um Estado, já que o poder brando é essencial e um importante meio de ampliar os interesses estatais em virtude da sociedade internacional ser complexa e interdependente em vários fatores políticos, sociais e econômicos.

O conceito de *smart power* segundo uma alta autoridade do Departamento do Estado americano afirmou: ‘’... a inteligente integração e ligação em rede de diplomacia, defesa, desenvolvimento, e outras ferramentas dos chamados poderes ‘duro’ e brando...’’, é observada de maneira clara a essência de uma proporcionalidade na utilização do poder inteligente (NYE JR., 2012, p. 264).

No entanto, o Direito Internacional não permite a legitimação no emprego do *hard power*, em razão de condena-lo como um meio de resolução de conflitos. O *soft power* é o principal meio para a resolução de conflitos que vem sendo adotado pelo legalismo internacional, uma vez que segundo Nyer (2010 apud BARROS 2015) ‘’ a promoção da democracia, direitos humanos, e desenvolvimento da sociedade civil não é melhor administrada com o cano de uma arma’’.

Á vista disso, a utilização do poder militar vem sofrendo algumas desvantagens no século atual, de modo que principalmente Estados grandes em função do custo, vêm se utilizando desse recurso com mais cautela e estudo (NYE, 2012).

Segundo Nye (2012) temos a seguinte afirmação:

> Embora a força permaneça um instrumento crítico na política internacional, não é o único instrumento. O uso da interdependência econômica, da comunicação, das instituições internacionais e dos atores transnacionais às vezes desempenha um papel maior do que a força (p. 56).

Foi realizada uma remissão a esse comentário, pois o uso do poder duro tem o seu nível de eficácia no meio internacional, porém o risco de retaliações dos Estados lesados e a credibilidade perante a comunidade internacional do Estado, que se utilizou deste meio agressivo, acabam por ficar em jogo, já que a economia é um fator que pesa muito no equilíbrio das relações internacionais e basta ocorrer um conflito militar significativo para alterar o *in statu quo ante bellum*. Um grande exemplo desse risco no emprego do *hard power* foi a guerra do Afeganistão que teve como resultado na vitória dos americanos na derrubada do governo do Talibã, e ocasionando uma represália por parte dos terroristas no ataque das torres gêmeas no dia 11 de setembro de 2001 aos Estados Unidos. Com base nesse fato histórico é observado que pós o ataque das torres gêmeas, o governo americano mudou completamente sua política imigratória e sua comercialização com os países do oriente médio, constatando as consequências e o risco da utilização do poder militar.

Fato interessante a ser estudado também neste capítulo é a relação que o *soft power* tem com o *smart power*, e diante disso, Nye (2012) comenta que ao criar o conceito de poder inteligente, acaba se existindo uma contraposição equivocada na perspectiva de que o poder brando por si só pode atingir uma política externa efetiva, caso este na tentativa ineficaz que o poder brando teve em evitar o apoio do governo Talibã a Al Qaeda nos anos 90. Existem vantagens e desvantagens quando o poder brando é utilizado casuisticamente. Essa efetivação do poder brando varia porque existem três recursos essenciais que são conceituados segundo Nye (2012) como: ‘’sua cultura (em locais onde ela é atrativa), seus valores políticos (quando ele os cumpre interna e externamente) e suas políticas externas (quando os outros as veem como legítimas e possuindo autoridade moral). ’’ É observado que o poder brando depende muito dos Estados que incorporam aquela cultura e aqueles valores políticos, já que a persuasão do Estado se utilizando desse poder vai partir de como o alvo pensa a respeito daquele conjunto de fatores vindo do *soft power*.

Entrando no ponto sobre cultura, esta pode ser um recurso de grande valia para o poder propriamente dito. O termo ‘’cultura’’ é conceituado como comportamentos sociais padronizados, transmitido conhecimentos e valores por determinados grupos. Essas

padronizações de comportamentos sociais podem chegar a níveis universais, havendo interações culturais entres diferentes sociedades, fazendo a cultura ser sempre transmuta. Estamos falando da cultura em específico porque se tem o exemplo de estudantes chineses irem passar uma temporada de estudos nos Estados Unidos, e ao voltarem para o seu país, trazerem uma visão multicultural de que as coisas na China podem ser implementadas de maneiras diferentes. Em outras palavras isso que dizer que o poder brando torna-se uma importante ferramenta no jogo de influencias perante a comunidade internacional. Contudo o emprego de recursos militares podem, em certos casos, coadjuvar com o poder brando, já que algumas pessoas são atraídas pela força e um poder militar forte e atuante, podendo ser uma fonte de atração para a expansão do poder brando, e em contraposição caso os recursos militares sejam empregados de maneira desorganizada, sua consequência pode ser o enfraquecimento do poder brando. Vimos como exemplo o caso do Brasil e Estados Unidos aumentando seu *soft power* investindo seus recursos militares na ajuda dos haitianos, posteriormente ao terremoto no ano de 2010 (NYE, 2012).

4.1 Os deslocamentos de poderes

Superadas as explicações sobre os tipos de poder e seus efeitos perante o Direito Internacional, presenciou-se no século atual uma grande revolução da informação que de acordo com Nye (2012), traz dois tipos de deslocamentos de poder: transição de poder e difusão de poder.

A transição de poder de certo modo é um evento tanto quanto mais antigo e já vivenciado pela comunidade internacional, principalmente quando um Estado dominante transmite para o outro esse poder, porém a difusão do poder é um procedimento completamente novo e característico das consequências de se ter uma disseminação de informações em uma velocidade e quantidades altíssimas pelo globo. O que é alarmante para todos os Estados, é o fato da era informacional global ter chegado a um nível fora de controle até dos Estados mais influentes. Nye (2012) traz o seguinte comentário de um ex-diretor de planejamento político do Departamento de Estado: ‘’A proliferação da informação é tanto uma causa de não polaridade quanto a proliferação das armas’’. É visto que as informações são tão poderosas e capazes de influenciar atores internacionais como a proliferação de armas tendo esse mesmo intuito de controlar os atores internacionais e atingir seus objetivos. Possui-se outra passagem trazida por Nye sobre o comentário de um analista Britânico:

> Encaramos cada vez mais riscos, ameaças e desafios que afetam as pessoas de um país, mas que se originam sobretudo ou inteiramente nos outros países [...] crise financeira, crime organizado, migração em massa, aquecimento global, pandemias e terrorismo internacional, para citar apenas algumas [...] Uma das principais razões para a dificuldade é que o poder tem sido difundido vertical e horizontalmente. Temos não somente um mundo multipolar, mas também um mundo não polar (NYE JR., 2012, p.151).

De acordo com o comentário acima todos os riscos exemplificados de certa maneira estão ao controle dos Estados nas respectivas políticas, legislações, tratados e práticas internacionais permitidas pela comunidade internacional que geram inúmeras interpretações e formações de opinião, formando o mundo multipolar em todos os sentidos. Entretanto a apolaridade internacional é o resultado de consequências incertas geradas pela tecnologia e a circulação massificada e veloz de informações.

Já foi elucidada no trabalho a corrente ideológica do Estado soberano estar decaindo, vez que essa instituição global exercia sua imposição desde a Paz de Westfália, no ano de 1648. Com base nisso, Nye (2012) diz que alguns estudiosos preveem que a revolução da informação vai sufocar as hierarquias burocráticas e substituí-las por organizações em rede, em razão da própria rede de informações trazidas pelo ciberespaço possuir inúmeras funções e conhecimentos que sejam mais eficientes que os meios legitimados pelos Estados.

Os mercados privados e as entidades não lucrativas terão uma participação relevante ao assumir determinadas funções governamentais, tendo em vista que as comunidades virtuais ao se desenvolverem na internet conseguirão atravessar as jurisdições territoriais e desenvolver seus próprios padrões de governanças. Esse será um ponto chave, trazendo a linha ideológica do Direito Transnacional, que foi tratado anteriormente. Nye (2012) traz o seguinte trecho: ‘’O novo padrão de comunidades e governança entrecruzadas vai se tornar um análogo moderno e mais civilizado do mundo feudal que existia antes da ascenção do Estado Moderno’’. O Estado não vai parar de existir, porém vai ter um destaque fora da centralidade nessa nova forma de ver e avaliar o funcionamento das relações internacionais pós-revolução da informação e elevação do ciberespaço como elemento do Direito Internacional, tornando-se mais operativo do que nas instituições de base estatais.

A revolução da informação, principalmente nas transformações cibernéticas revela um dos pontos principais no aumento da difusão do poder. Segundo Nye (2012), ‘’ os estados continuarão sendo os atores dominantes no palco mundial, mas encontrarão o palco bem mais povoado e difícil de controlar’’. Tanto empresas privadas como pessoas físicas hoje em dia

tem acesso a um mundo de informações na internet, sendo o poder da informação. Os governos sempre tiveram a preocupação de filtrar e avaliar o tipo de informação que chega a população, porém com a consolidação do ciberespaço no século atual tornou mais difícil esse controle integral por parte do Estado.

Alguns estudiosos preferem chamar a revolução da informação de ‘’terceira revolução industrial’’, baseadas nas rápidas inovações tecnológicas nos *softwares*, computadores e outros dispositivos de comunicações, ocasionando uma grande redução de custos ampliando o acesso de muitos indivíduos a esses materiais que permitem o acesso ao ciberespaço. Apresentam-se no trabalho informações interessantes sobre a construção dessa revolução, demonstrando que o poder do computador duplicou a cada dezoito meses ao longo de trinta anos, e no início do século XXI, ele tinha o custo de um milésimo que no início da década de 1970, mostrando que a evolução dos componentes tecnológicos alinhada a um custo em constante barateamento, apresenta um resultado jamais visto em termos de acesso a informação. Outro dado interessante, foi constatado em 1993 algo em torno de 50 *sites* ao redor do mundo, no ano 2000 esse número ultrapassava 5 milhões. (NYE, 2012).

Mira-se que a característica fundamental da revolução informacional, não é a velocidade das comunicações, principalmente entre os ricos e poderosos, mas sim a gigantesca redução de custo na transmissão e acesso a informação. No século XIX já existia uma comunicação instantânea através do telégrafo em especial entre o continente europeu e o continente norte americano, porém nem todos tinham acesso a esse tipo de comunicação e esse tipo de estrutura que não era conectada a todos os continentes. Sendo assim o custo atual em relação acesso e transmissão da informação se tornam ínfimos possibilitando um fluxo infinito de informações para o ciberespaço. Como resultado, dispomos de uma explosão informacional, sendo exemplificado em uma pesquisa feita em 2006, estimando 161 bilhões de *gigabytes* de informações digitais criadas e captadas, ou seja, isso significa aproximadamente 3 milhões de vezes os conteúdos e informações trazidas em todos os livros já escritos. Esse exemplo nos dá ideia de que a velocidade na informação não é tudo e sim o número cada vez mais crescente de indivíduos tendo acesso à informação tanto na sua criação como em sua disseminação, sucedendo uma aceleração na difusão do poder e mudando a própria natureza dos Estados (NYE, 2012).

Nye faz um comentário bastante interessante sobre essa redução de custos:

> Quando o custo da computação e da comunicação abaixou, as barreiras à entrada começaram a declinar. Tanto os indivíduos quanto as organizações privadas,

> variando desde corporações até ONGS e terroristas, estão capacitados para desempenhar papéis diretos na política mundial (NYE JR., 2012, p.154-155).

Isso significa que a propagação da informação como uma forma de poder é distribuída pelo ciberespaço de uma maneira muito ampla, influenciando diretamente no monopólio de poder que os Estados têm na política internacional, podendo ser acessada desde civis até grupos e organizações com diferentes objetivos na presença da comunidade internacional. Essa é a parte que a velocidade nas comunicações entra na questão da informação, pois quando um maior número de indivíduos possui um amplo acesso a essas informações, todos ao mesmo tempo, os governos passam a ter um controle menor sobre suas agendas políticas. Logo os líderes políticos irão usufruir de uma liberdade reduzida em suas decisões porque seu tempo de reação aos demais acontecimentos será bastante limitado e terá que ser feito com muitas análises, já que o palco internacional está mais complexo possuindo um número maior de atores nesse novo cenário político no Direito Internacional.

Outro ponto interessante na redução de custos, na medida em que as barreiras de acesso à informação e ao ciberespaço começam a serem diminuídas, a revolução informacional diminui o poder dos Estados maiores e aumenta o poder dos Estados menores assim como os atores não estatais, ou seja, mais uma consequência da difusão de poder. Não é tão simples afirmar que obrigatoriamente os Estados menores irão ter poder suficiente e retirar poder suficiente para disputar com os Estados maiores, mas mesmo diante dessas relações internacionais complexas pode ser afirmado que a revolução da informação ajuda os pequenos, porém também ajudam cada vez mais os Estados grandes e poderosos. Podem existir tanto *hackers* dispostos a roubar, explorar e criar informações no ciberespaço para diminuir o poder dos Estados ou atacar os Estados poderosos. O próprio governo também pode distribuir milhares de agentes treinados com profundo conhecimento em computação dispostos a romper códigos de segurança ou se infiltrar em outros Estados para garantir sua hegemonia internacional gerando o cerne da guerra cibernética (NYE, 2012).

A busca desenfreada por informações pelos Estados muda completamente o emprego dos poderes (*soft power, hard power e smart power*) diante de determinadas situações na política internacional. Por mais que o custo de ter acesso às informações seja baixo, a busca e criação de novas informações no ciberespaço com regularidade necessitam de um investimento considerável. Em um contexto completamente concorrente, as informações que são novas tem um poder mais efetivo e são mais importantes. Embora a informação seja um bem público, seu consumo não se esgota. É visto o seguinte trecho que Nye (2012, p.156) traz

em seu livro: ‘’Thomas Jefferson usava a analogia de uma vela: se eu lhe dou uma luz, isso não diminui minha luz. Mas, em uma situação competitiva, pode fazer uma grande diferença se eu tenho a luz primeiro e vejo as coisas antes de você’’. Isso quer dizer que aquele ator que tiver primeiro uma informação que possa mudar, seja qualquer setor da economia, posturas na política internacional, conhecimento sobre a cura de determinada doença, entre outros, pode influenciar diretamente todas as relações de poderes que os entes internacionais possuem entre si.

Países poderosos como Estados Unidos, China, Rússia e França detêm de grandes servidores que buscam, armazenam e produzem essas informações valiosas que são ocultadas e podem colocar em desvantagem os Estados concorrentes. Em contrapartida atores não governamentais como *Wikileaks* também possuem informações confidenciais sensíveis de determinados Estados e até mesmo países com recursos cibernéticos avançados podem chantagear grandes Estados em troca de poder e benefícios. Como resposta os Estados algumas vezes patrocinam ataques cibernéticos realizados por *freelance*, piratas e *hackers* para não manchar sua imagem perante a sociedade internacional.

Percorrida uma vasta explicação e toda uma construção do que é o poder, das subdivisões que o poder possui e sua ligação com o ciberespaço, passa-se a entrar de fato no assunto que envolve um dos principais temas do trabalho.

4.2 Um estudo analítico do ciberespaço

Foi relatado em partes anteriores desse capítulo que o poder baseado na informação por si só não é novo, porém a aplicação dessas informações através dos meios cibernéticos é. O conceito de ciberespaço volta aparecer, já que Nye (2012, p.161) afirma existir ‘’dúzias de definições de espaço cibernético, mas, em geral, ‘’cibernético’’ é um termo ligado a atividades eletrônicas e relacionadas a computador’’. Em outras palavras podemos dizer que o espaço cibernético contem múltiplos recursos e funcionalidades que não só criam e difundem a informação, mas possui sua própria estrutura organizacional de funcionamento, permitindo uma ampla conceituação desse espaço.

Por definição ‘’espaço cibernético é um domínio operacional formado pelo uso da eletrônica para [...] explorar informações via sistemas interconectados e sua infraestrutura associada’’ (NYE, 2012). Os meios eletrônicos passaram a serem os principais condutores e os criadores da informação, formando diversas conexões interativas entre vários atores internacionais.

Para ficar mais claro o entendimento do que veio a se tornar o espaço cibernético, temos inicialmente em 1969, a criação de conexões entre computadores, chamada Arpanet, pelo Departamento de Defesa dos Estados Unidos, e posteriormente em 1972 à criação de códigos para permuta de informações digitais (TCP/IP). O sistema de endereços na internet que conhecemos atualmente só veio surgir em 1983, junto com os primeiros vírus de computador, sendo assim a *World Wire Web* ou simplesmente a famosa sigla WWW que veio a aparecer em 1989. Por seguinte o maior e famigerado dos *sites* de busca foi o *Google* em 1998 que hodiernamente controla inúmeras empresas no setor eletrônico/cibernético e publicitário. Foi no final da década de 1990 que inúmeras empresas começaram a investir nessa nova tecnologia criando e fornecendo informações para o resto do globo, já que a semente do ciberespaço veio de infraestruturas militares e só depois foram abertas para utilização dos civis. Com base nisso em 1998 foi criada a Icann (*Internet Corporation for Assigned Names And Numbers*), uma entidade sem fins lucrativos vinculada ao governo americano, que desenvolve planos nacionais solenes para uma melhor segurança cibernética. Para se ter uma noção da importância de programas e políticas internacionais que regulem e tragam ao menos uma segurança mínima cibernética, em 1992 existia o numerário de 1 milhão de indivíduos utilizando a internet, e um pouco mais que uma década esse número passou para 1 bilhão de usuários. É observado um crescimento e evolução acelerados do ciberespaço, sem falar das próprias complexidades que foram geradas nas relações entre os entes internacionais, nas infraestruturas que operam esse espaço virtual, no quantitativo de agentes especializados que manuseiam e mantém em organização essa grande rede informacional (NYE, 2012).

O ciberespaço acaba sendo um meio de interação entre o físico e o virtual, formando um regime híbrido que possui várias camadas de atividades. Dessa forma temos a seguinte divisão:

> A camada de infraestrutura física segue as leis econômicas dos recursos rivais (ou exclusivos) e os crescentes custos marginais e as leis políticas de jurisdição e controles soberanos. A camada virtual, ou informacional, tem características da rede econômica de aumentos das receitas em função da escala e práticas políticas que dificultam a realização de controle jurisdicional (NYE.JR, 2012, p.162).

Isso acaba sendo um jogo de controle dessas camadas que envolvem aspectos econômicos, políticos, normativos e tecnológicos. Estados que sabem controlar esses elementos podem realizar ataques cibernéticos a baixo custo e com ampla margem de proteção para encobrir a sua autoria por falta de normas jurídicas tanto nacionais como

internacionais a respeito do ciberespaço e ainda mais ter um poder econômico manipulador desse domínio para ameaçar ou deixarem subordinados os Estados mais fracos.

Pode-se dizer também que o poder cibernético é determinado por uma reunião de recursos relacionados ao controle, formação de *softwares* e redes, assim como habilidades humanas voltadas ao computador. Contudo tecnologias *intranets* como redes internas de uma Empresa ou comunicações via satélites também fazem parte desse tipo de poder. Nye (2012) comenta que ‘’ o poder cibernético é a capacidade para obter resultados preferidos mediante o uso dos recursos de informação eletronicamente conectados do domínio cibernético’’. Os resultados buscados através da utilização do poder cibernético podem trazer repercussões tanto dentro como fora desse domínio, sendo uma moeda de dois lados. Esses efeitos levam os Estados a investirem tanto na defesa cibernética para garantir seus bancos de informações e estudos a respeito de aperfeiçoamentos tecnológicos como no ataque cibernético para retaliar os demais agressores que tentaram interferir ou espionar os demais planos sigilosos que os Estados possuem.

Os Estados Unidos são umas das nações que já vem investindo amplamente no espaço cibernético através dos meios militares, vejamos a seguinte afirmação do secretário de defesa americana, Willian J. Lynn III:

> Nesse momento, mais de 100 organizações de inteligência estrangeiras estão tentando hackear as nossas redes digitais que organizam as operações militares norte-americanas. O Pentágono reconhece a ameaça catastrófica criada pela guerra cibernética, e está se coligando a governos aliados e empresas privadas para se preparar. (LYNN III, William J. 2010, p.1, apud BARROS, 2015).

Esse comentário revela o real envolvimento tanto dos Estados assim como entidades não estatais com o objetivo de roubar informações militares, já que são informações extremamente valiosas fazendo a diferença em uma tensão pré-guerra surtindo um efeito mais eficaz que um conflito armado. Toda essa problemática que impulsiona a guerra cibernética é realizada apenas nas pontas dos dedos nos botões de um teclado e um *mouse*. Isso leva aos Estados estudarem e traçarem uma vasta criação e desenvolvimento de estratégias de defesa cibernética que podem levar anos para ser em grande parte segura contra uma legião de ataques vindos do mundo inteiro.

4.3 Retrospectiva na formação do domínio cibernético e a análise da legítima defesa de acordo com a Carta das Nações Unidas

A guerra cibernética propriamente dita é justamente o reflexo de todas essas mudanças e avanços que as formas de poderes sofreram (*hard power, soft power, smart power, cyberpower*), fazendo o conflito cibernético ser um fenômeno multifacetado e em determinadas proporções, e não ser uma simples guerra como é conhecido no sentido tradicional/clássico. Logo no inicio da criação da internet e consequentemente do ciberespaço, dois americanos, John Arquilla e David Ronfeldt, na década de 90 lançaram o seu livro *cyber war is comming!* (1993) tratando de uma maneira futurista as consequências e efeitos que esse novo domínio iria trazer nas relações internacionais (FERNANDES, 2012).

Os dois autores americanos iniciaram essa temática abordando a infoguerra (*netwar*) como um confronto dentro do âmbito informacional nas sociedades, na tentativa de remodelar ou até prejudicar o saber que a população possui do mundo ao seu redor. A *netwar* pode visar informações de caráter político, informações que tragam um tumulto a respeito de uma visão cultural que seja diferente ,e a principal que o trabalho está estudando, acessos ilegais a redes e bases de dados relacionadas a computadores (FERNANDES, 2012).

É visto que a realidade da guerra cibernética naquele tempo já era prevista logo no inicio da computação e da internet, sendo até hoje uma questão que continua atualíssima. Por mais que nessa conceituação inicial, do que veio a se tornar a guerra cibernética, não trate de maneira específica a respeito de sistemas eletrônicos e as praticas que são feitas diretamente nesse meio, o fator informação que interliga todo o ‘’saber’’ de uma sociedade tal como as informações que pautam as relações entre Estados e entes não-estatais, se manipuladas de maneira arbitrária, um conflito cibernético está estabelecido.

Destarte Arquilla e Ronfeldt trouxeram um conceito específico sobre a guerra cibernética, vejamos:

> [...] conduzir e preparar para conduzir, operações militares de acordo com os princípios da informação [...] Esta forma de guerra pode envolver diversas tecnologias – nomeadamente C3I[6]; recolha de informação, posicionamento e identifi cação de amigos ou inimigos (IFF)[7]; e sistemas de armas “inteligentes” – para dar apenas alguns exemplos. Pode também envolver interferência electrónica, falseamento, sobrecarga e intrusão nos circuitos de informação e comunicação de um adversário. [...] Poderá também implicar o desenvolvimento de novas doutrinas sobre o tipo de forças necessárias, onde e como deslocá-las, e saber o quê e como atacar no lado do inimigo. Como e onde posicionar determinados tipos de computadores e sensores relacionados, redes, bases de dados, etc., pode-se tornar tão

[6] Communications, Command, Control and Intelligence.
[7] Identification – Friend - or – Foe.

> importante como a questão que costumava ser efetuada sobre deslocação de bombardeiros e as suas funções de suporte. A ciberguerra pode também ter implicações para a integração dos aspectos políticos e psicológicos com os aspectos militares de fazer a guerra (ARQUILLA E RONFELDT, 1993 apud FERNANDES, 2012, p. 16).

Nota-se que o conceito evoluiu se tornando mais complexo e abrangendo mais elementos ligados a tecnologia, como situações análogas a um *hack* da mesma maneira que o desenvolvimento de novas doutrinas, vertendo perfeitamente as situações das formas de poder e a difusão do próprio poder no meio cibernético, como foi estudado anteriormente. É interessante observar também que o componente informação sempre está ligado desde a inexistência e criação do ciberespaço, até a própria manipulação do espaço cibernético de como chegam ou são criadas essas informações, entrando na temática mais inerente a tecnologia e a rede de computadores.

No entanto tem-se também o conceito de ciberguerra trazido na visão do *Institute for Advanced Study Information Warfare* dos Estados Unidos:

> [...] o uso ofensivo e defensivo da informação e dos sistemas de informação para negar, explorar, corromper, ou destruir a informação de um adversário, processos baseados na informação, sistemas de informação e redes baseadas em computadores, enquanto se protegem as próprias. Tais ações são projetadas para atingir vantagens sobre adversários militares (SINKS, 2010 apud FERNANDES, 2012, p. 17).

Analisa-se que os Estados unidos optaram por um direcionamento do ciberespaço de maneira ostensiva em estratégias militares, garantindo desde já uma segurança cibernética em suas redes, além de garantirem uma nova forma de guerra adquirindo vantagem militar antecipada em caso de um ataque físico ou mesmo um ataque cibernético com prévia analise nos sistemas informacionais do inimigo.

Passando agora para um revés jurídico, é o questionamento se os Estados com base no *jus ad bellum* podem se utilizar da ciberguerra levando em conta o plano normativo do Direito Internacional. É tida uma leve impressão de sentir um vazio jurídico quando é falado da adequação dessa nova realidade aos padrões normativos do Direito Internacional, que regula o uso da força legitimados antes do surgimento do ciberespaço. Na verdade é existente um problema que pode vir a ser resolvido com vários tipos de respostas, mas que todas resultam no mesmo objetivo que é regular e tornar juridicamente mais seguro o ciberespaço e os efeitos que uma guerra cibernética nesse meio pode trazer (FERNANDES, 2012).

Quando se fala no uso da força, contido o teor da normatividade utilizada pelo Direito Internacional, a Carta das Nações Unidas vem por ser o principal meio a ser consultado diante de um problema na comunidade internacional. Na verdade a Carta tem como regra geral a proibição do recurso à guerra, ou seja, o *jus contra bellum*, sempre adotando uma resolução de conflitos por meios diplomáticos. Em relação a essa regra geral o documento possui o seguinte conteúdo em seu artigo 2º nº 4:

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

Dessa maneira os objetivos da ONU como a paz internacional, garantir os direitos humanos, promover o desenvolvimento econômico e social das nações entre outros, são como barreiras para impedir um retrocesso da humanidade através da guerra e de ameaças bélicas.

Contudo como toda regra é aplicada temos a existência de exceções, e estas a própria carta também prevê. O seu artigo 39º cominado com os artigos 41º e 42º dizem a respeito do funcionamento do Conselho de Segurança que poderão autorizar ou não a utilização da força. Vejamos o artigo 39°:

> O Conselho de Segurança determinará a existência de qualquer ameaça à paz, ruptura da paz ou ato de agressão e fará recomendações ou decidirá que medidas deverão ser tomadas de acordo com os artigos 41º e 42º, a fi m de manter ou restabelecer a paz e a segurança internacionais.

Serão feitas uma série de análises primeiramente tomando medidas sem envolver o emprego de forças armadas, como a utilização de sanções econômicas, até ao corte nas relações diplomáticas como preconiza o artigo 41°. Se por ventura as medidas previstas no artigo passado não surtam efeitos, o Conselho de Segurança poderá se utilizar das demais forças para garantir ou restabelecer a paz e a segurança internacionais.

Contempla-se outra exceção disposta no artigo 51º a respeito da admissão, em seu teor legal do direito a legítima defesa, coletiva ou individual (FERNANDES, 2012):

> Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva, no caso de ocorrer um ataque armado contra um membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para

> a manutenção da paz e da segurança internacionais. As medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer momento, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais.

Esse é o ponto de questionamento se com base nesse dispositivo, os Estados poderão se utilizar do ciberespaço para se defenderem gerando uma guerra cibernética, respaldado na autorização do Conselho de Segurança. Certamente é axiomático que se houver uma hostilização ameaçando a paz ou uma real agressão, de maneira lógica será valido à utilização desse meio segundo o artigo 39º. Contudo, David Graham relata a dificuldade nas relações internacionais de se aplicar esse dispositivo sem controvérsias:

> A maioria das decisões apenas chega após extensas e morosas deliberações, e, mesmo então, estão sujeitas ao veto de qualquer membro permanentes do Conselho de Segurança. Assim, dada a natureza nebulosa e com *nuances* dos ciberataques e a incerteza de saber como o Conselho de Segurança irá responder aos mesmos de forma atempada, parece válido assumir que um Estado escolherá lidar com os ciberataques através do exercício do seu direito de legítima defesa (GRAHAM, 2010 apud FERNANDES, 2012, p. 18-19).

De fato a legislação internacional dá margem para que interpretações sejam aplicadas aos ciberataques através do instituto da legitima defesa, porém a complexidade informacional, tecnológica, econômica e política são fatores que pesam de uma maneira crucial na tomada de decisões dos membros permanentes do Conselho de Segurança. A aprovação ou o veto na utilização do recurso à guerra cibernética para se valerá da sua legitima defesa em prol da paz internacional. Os efeitos podem resvalar multilateralmente sem real certeza da extensão dos danos, diferentemente de uma guerra convencional, pois a humanidade já passou por duas guerras mundiais, fora as outras guerras pelos principais continentes do mundo (América, Europa, Ásia, África, Oceania).

Segundo Fernandes (2012) é necessário não olhar apenas para o artigo 51° da carta da ONU, mas um olhar sob o prisma do Direito Internacional Consuetudinário a respeito das interpretações que podem ser tomadas quando um Estado sofre um ataque armado e se utiliza da legítima defesa como uma resposta proporcional a esse ataque. Segundo o Direito Internacional Consuetudinário a legitima defesa apropriada consiste em dois fundamentos: a

necessidade e a proporcionalidade. A necessidade é um requisito a ser completado quando se evidencia a inexistência meios pacíficos do Estado atacado resolver o conflito. Já o requisito da proporcionalidade, demanda um limite que a legítima defesa deve ter levando em conta a proporção no quantitativo de força necessária para se repelir um ataque atual ou eminente.

Entende-se que é fundamental caracterizar os ataques cibernéticos ou sua sequência continuada de ataques como um ataque armado. Pois a legítima defesa só poderá ser recorrida se utilizando do uso da força, segundo o entendimento legal da norma. Contudo Sommer e Brown comentam que a ciberguerra deve passar por uma verificação para poder ser chamada de um ataque armado. Segundo os dois autores referidos anteriormente, se tem a seguinte afirmação:

> Carta das Nações Unidas requer uma justificação para a adoção de contra-medidas por aqueles que afirmam ter sido atacados. No essencial, a vítima deve ser capaz de produzir provas fidedignas sobre quem a atacou – algo nem sempre fácil como mostraremos em seguida – e sobre os efeitos dos ataques sobre o seu território e população. O objetivo das contra-medidas deverá ser forçar o Estado atacante a acatar as suas obrigações nos termos da Carta das Nações Unidas (SOMMER E BROWN, 2011 apud FERNANDES, 2012, p. 19).

É evidente que a caracterização de um ciberataque como um ataque armado necessita de um suporte mínimo probatório para as pretensões punitivas sejam tomadas. Contudo com o amplo suporte cibernético que os entes infratores possuem, ocultando seus crimes, fica facilitada a impunidade. Um caminho doutrinário a ser seguido seria a extensão da responsabilidade ao Estado que sediou aquele ataque, e se não sabia da existência desses crimes deveria ter tido um controle de segurança cibernética mais forte para prevenir esses tipos de incidentes.

Retornando ao termo ‘’ataque armado’’, é possuída também uma visão teórica bastante interessante do jurista suíço, Jean Pictet, sendo o principal redator técnico do texto das Convenções de Genebra em 1949. Nota-se que o uso da força de acordo com os artigos 2° das quatro Convenções de Genebra, será considerado um ataque armado quando submetido à verificação do ‘’escopo, duração e intensidade suficiente’’ (PICTET, 1958 apud FERNANDES, 2012).

A questão está na interpretação que os demais juristas especializados em Direito Internacional possuem a respeito dessa verificação. De acordo com essa questão David Graham faz o seguinte comentário:

> [...] ao longo do tempo certos instrumentos internacionais evoluíram, o que facilitou a aplicação dos critérios de Jean Pictet. O instrumento mais relevante nesse contexto é a resolução da Assembleia Geral das Nações Unidas definindo ‘agressão”. Embora a resolução não contenha uma definição definitiva de ataque armado, fornece exemplos de ações estaduais que devem ser qualificadas como tal, e estes ganharam uma extensa aceitação internacional(GRAHAM, 2010 apud FERNANDES, 2012, p. 19-20).

Por mais que ocorra uma evolução doutrinária e tenham resoluções abundantes que permeiam a temática do termo ‘’ataque armado’’, esse patamar ideológico de certa forma está baseado de maneira muito anterior ao surgimento do ciberespaço e evoluções tecnológicas. Deste jeito foram propostas três abordagens que tem o objetivo de tornar mais fácil a aplicação da verificação criada por Pictet (escopo, duração e intensidade suficiente), utilizando as formas não convencionais do uso da força, sendo abordados os ciberataques (FERNANDES, 2012).

A primeira abordagem é chamada de *instrument-based approach* ou abordagem instrumental, de acordo com esse paradigma a verificação levará em conta se o dano causado por um ciberataque teria efeitos prévios iguais e apenas a um ataque cinético. Como exemplo no caso de um ciberataque que provoque um *blackout* ou dano na parte elétrica em uma rede de computadores, sendo caracterizado como um ataque armado.(FERNANDES, 2012).

A segunda abordagem é nomeada de *effects-based approach* ou abordagem baseada nos efeitos, esse modelo leva em conta as consequências globais que um ciberataque provocaria aos Estados. Tem-se o exemplo do caso da Estônia mostrado anteriormente no trabalho (FERNANDES, 2012).

A última abordagem que é a terceira, sendo fundamentada na *strict liability* ou responsabilidade estrita. Esse modelo seria como uma responsabilidade objetiva nas devidas proporções, porque o ciberataque é visto nessa abordagem como uma prática contra qualquer infraestrutura nacional, automaticamente denominado como um ataque armado. Essa caracterização leva em conta as demais consequências por danos indeterminados suportados pelos Estados vítimas em suas infraestruturas nacionais (FERNANDES, 2012).

Mesmo existindo essas três abordagens a respeito da verificação de um ataque armado criado por Pictet, ainda existem diferentes interpretações, mas todas conforme a essência dessas abordagens convergindo na caracterização de um ciberataque como um ataque armado (SKLEROV, 2009 apud FERNANDES, 2012).

Michael N. Schmitt, elaborou no final dos anos 90, seis parâmetros avaliativos que vão medindo até que ponto um ciberataque poderá ser equiparado a um ataque armado:

> a. gravidade (*severity*): os ataques armados ameaçam danos físicos e destruição da propriedade num grau muito mais elevado que outras formas de coerção;
> b. iminência (*immediacy*): as consequências negativas de uma ação armada ou as ameaças das mesmas geralmente ocorrem com mais rapidez do que outras formas de coerção;
> c. caráter direto (*directness*): as consequências de uma coerção armada estão mais diretamente ligadas ao *actus reus* (ato de culpabilidade), do que outras formas de coerção que dependem de vários fatores para atuar;
> d. caráter invasor (*invasivness*): na coerção aramada, o ato que provoca danos normalmente traduz-se num atravessar da fronteira nacional, enquanto que os atos de guerra econômica geralmente ocorrem fora das suas fronteiras;
> e. mensuralidade ou extensão (*measurability*): enquanto que as consequências de uma ação armada são geralmente fáceis de verificar (por exemplo, certo nível de destruição), as consequências de outras formas de coerção são mais difíceis de definição;
> f. legitimidade (*presumptive legitimacy*): na maioria dos casos, o uso da força, seja sob o prisma da lei doméstica ou da lei internacional, é presumivelmente ilegal, exceto se estivermos perante uma disposição que a permita (SCHMITT, 1999 apud FERNANDES, 2012, p. 20-21).

Mira-se que esses parâmetros avaliativos são bastante específicos, dando vários focos a vários tipos de situações e efeitos que um ciberataque possa gerar. Dessa forma os Estados ao avaliarem um ataque cibernético poderão ter uma vasta interpretação dentro dos parâmetros avaliativos trazidos por Schmitt. Vale ressaltar que um ponto avaliativo desse conjunto de parâmetros por si só não traz uma resposta efetiva, mas a utilização de todos parâmetros, na avaliação, traz resultados suficientes, caracterizando um ataque armado. Portanto no futuro, talvez esses seis pontos avaliativos possam ser normatizados como uma forma padronizada de avaliação internacional pelos Estados para classificar os ataques cibernéticos. De certa forma ainda se depende da complexa política internacional com múltiplos interesses entre os Estados e os entes-não estatais, sendo incerto e provavelmente ocorrer uma classificação diferente dos ciberataques (SKLEROV, 2009 apud FERNANDES, 2012).

A respeito da identificação dos ataques cibernéticos, se parte da premissa de uma análise realizada pelo administrador responsável pelo sistema atacado, utilizando programas

de detecção. Esses programas não necessariamente irão identificar de maneira exata o ataque cibernético, mas podem auxiliar o administrador a reunir pistas para buscar o autor, ajudando a apontar de que Estado aquele ataque veio, ou identificar o ciberataque no sentido de um ataque armado ou o uso de uma força menor, porém esses programas não previnem todos os ciberataques de maneira geral (SKLEROV, 2009 apud FERNANDES, 2012).

Por conseguinte se o programa identificar previamente o ataque, o Estado poderá ganhar tempo, analisando na tentativa de responsabilizar o autor e direcionar sua legítima defesa de maneira efetiva. Contudo um dos maiores desafios é se antevir a velocidade tremenda que esses ataques possuem, sendo assim Sklerov comenta:

> [...] olhar para o imediatismo de futuros danos, para determinar em que medida um ataque deverá ser classificado como um ataque armado iminente. [Todavia] dada a velocidade extremamente rápida a que os códigos dos computadores podem ser executados, tais decisões serão muito difíceis de concretizar, uma vez que o retardar do uso de defesa ativas aumenta a probabilidade de causar danos ao Estado (SKLEROV, 2009 apud FERNANDES, 2012, p. 22).

Nota-se que a identificação e a confirmação do ataque cibernético não é fácil, já que a prévia analise dá uma grande margem para o Estado vítima receber danos e ao mesmo tempo um contra-ataque sem análise prévia poderia desencadear de fato uma guerra cibernética. Deveras o que resta é o administrador continuar analisando e aperfeiçoando cada vez mais os programas que lhe auxiliem nessa detecção.

Foi falado anteriormente também da dificuldade de identificação da autoria em um ciberataque. Por mais que um programa ajude a avisar o ataque, é arriscado ocorrer uma atribuição errada de autoria, já que os autores desses ataques possuem meios tecnológicos de ocultar sua identidade. Sendo assim, volta-se à questão então de responsabilizar o Estado que deixou de vigiar e garantir a segurança cibernética que causou o ataque, por mais que não se tenha descoberto a autoria. É presente a seguinte opinião de Sklerov:

> A responsabilidade de um Estado deve ser julgada pelos factos disponíveis, mesmo se esta resulta numa atribuição errada. Primeiro, enquanto um Estado avalia uma ataque com o melhor da sua capacidade técnica e atua com boa fé face à informação disponível, este cumpre as suas obrigações internacionais. Segundo, Estados que recusam atuar em conformidade com o seu dever internacional de prevenir que o seu território seja usado para cometer ciberataques, escolheram o risco de serem

> considerados indiretamente responsáveis, por acidente (SKLEROV, 2009 apud FERNANDES, 2012, p. 22).

Isso acaba de certa forma estimulando os Estados a começarem a punir severamente através de leis criminais os autores que realizam ciberataques se utilizando de seu território, e prevenindo um atentado a própria segurança cibernética internacional. Além de existir uma cooperação dos Estados contribuírem com um monitoramento e aperfeiçoamento comum de legislações, sistemas cibernéticos de segurança trilhando um objetivo comum que é a regulação da guerra cibernética. Todavia, o Estado que não estiver disposto a cooperar e for negligente no monitoramento do seu território, a atribuição da responsabilidade por terem indiretamente cooperado com o ataque acabam resultando uma série de punições internacionais.

4.4 Uma abordagem dos institutos que auxiliam as Nações Unidas nas atividades cibernéticas

Será percorrida agora uma análise dos institutos jurídicos que regulam ou que propõem disposições sobre os ciberataques e a própria guerra cibernética, já que não existe ainda um tratado internacional de comum acordo para uma regulação global desses fenômenos.

Começando pela Organização das Nações Unidas, que em dezembro no ano de 2011, o Conselho Econômico e Social da ONU realizou um encontro global para alertar a importância de se disseminar uma cultura de segurança cibernética mencionando os problemas que o Direito Internacional possui com a regulação do ciberespaço. Dessa forma sendo umas das principais questões que modificam o equilibro internacional, e existindo um de interesse de todos os Estados do globo em um amplo debate jurídico a respeito de uma regulação (ECOSOC, 2011 apud BARRO, 2015).

Contudo o Conselho de Segurança ainda está caminhando aos poucos na demonstração de uma opinião efetiva sobre as violações do Direito Internacional através do ciberespaço. O único pronunciamento oficial sobre guerra cibernética é a resolução 1.113 de 2011 do Conselho de Segurança, definindo o seu próprio conceito (BARROS, 2015):

> Guerra cibernética é a utilização de computadores ou meios digitais por um governo ou com conhecimento explícito de, ou aprovação do governo contra outro Estado, ou propriedade privada dentro de outro Estado incluindo:

> -Acesso intencional, intercepção de dados ou danos à infraestrutura digital ou digitalmente controlável.
> -Produção e distribuição de dispositivos que podem ser usadas para subverter a atividade doméstica. (ONU, 2011). [8]

Sendo assim mesmo existindo essa resolução, não existe ainda qualquer decisão pautada especificamente sobre casos práticos a respeito de ciberataques ou de guerra cibernética. Os direcionamentos vindos da ONU ainda são baseados largamente na doutrina clássica do Direito Internacional (MAURER, 2011 apud BARROS, 2015).

Por outro lado a Assembleia Geral da ONU estimulada sobre a regulação do ciberespaço dividiu duas linhas teóricas de análise: de um lado transações de caráter político-militares e de outro, questões econômicas, todos associados ao ciberespaço. A guerra cibernética e o cibercrime são termos optativos para essas duas linhas teóricas, já que a guerra cibernética é a violação de uma rede não autorizada pelo Estado ou outro tipo de atividade perigosa que ponha em risco essa rede e suas respectivas informações. Cibercrimes tem um objetivo mais voltado para um interesse econômico e não político (BARROS, 2015).

Existem variados órgãos da ONU trabalhando em conjunto no estudo de toda essa problemática da segurança cibernética. Na esfera político-militar foi criado o Primeiro Comitê de Assembleia Geral da ONU, sendo um órgão Intergovernamental designado para lidar com questões políticas e bélicas internacionais sobre o ciberespaço. Esse Comitê é amparado pela União Internacional de Telecominucações (UIT), pelo Instituto das Nações Unidas para a Pesquisa sobre o Desarmamento (UNIDIR) e pela Força-Tarefa de Implementação do Combate ao Terrorismo (CTITF) (MAURER, 2011 apud BARROS 2015).

Falando de maneira mais específica sobre essas agências de apoio ao Primeiro Comitê de Assembleia Geral da ONU, a UIT cuida da parte de tecnologias da informação e comunicação com a função de criar regulamentos que deem uma segurança maior aos usuários que trafegam pelo ciberespaço. Como resultado desse trabalho em normatizar a segurança cibernética, a UIT criou um compêndio chamado de Política de Segurança Global Cibernética ou *Global Cybersecurity Agenda*, voltado para uma cooperação internacional na criação de medidas que torne o ciberespaço mais seguro. Existem 5 alicerces definidos pela UIT como estruturas organizacionais, medidas técnicas, procedimentais e jurídicas,

[8] Tradução livre do original: "Cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another state including:
-Intentional access, interception of data or damage to digital and digitally controlled infrastructure.
-Production and distribution of devices which can be used to subvert domestic activity". (ONU, 2011).

cooperações internacionais e capacitações a respeito da segurança cibernética. Todas sempre com o objetivo de trazer uma nova visão séria na regulação do ciberespaço e conscientizando de como deve-se ter um correto uso dessa tecnologia informacional com mais proteções (UIT, 2007 apud BARROS 2015).

O Instituto das Nações Unidas para a Pesquisa sobre o Desarmamento (UNIDIR) tem o objetivo de propiciar estudos e pesquisas na cooperação para resoluções dos problemas que consistem nas ameaças vindas do ciberespaço. O UNIDIR é quem descobre essas ameaças cibernéticas que são nomeadas de ameaças emergentes (PAKALNIŠKIS, 2011 apud BARROS, 2015).

A Força-Tarefa de Implementação do Combate ao Terrorismo (CTITF) possui a função de unificar forças para lutar contra os ataques terroristas que venham a prejudicar o sistema internacional das Nações Unidas. Seu objetivo principal é o combate ao terrorismo, sendo assim tendo a responsabilidade de impedir que o ciberespaço se torne um meio de disseminação do terrorismo, como por exemplo, grupos terroristas do oriente médio criados virtualmente dando aulas e dicas de como se fabricar uma bomba e ensinando táticas militares de invasões (ONU, 2006 apud BARROS, 2015).

Tem-se também além do Primeiro Comitê, o Terceiro Comitê de Assembleia Geral da ONU e o Conselho Econômico e Social (ECOSOC), sendo o ponto de vista econômico como principal foco desses órgãos intergovernamentais. A esses órgãos é tido o suporte do Instituto de Investigação Inter-regional de Crime e Justiça das Nações Unidas (UNICRI) e do Escritório das Nações Unidas sobre Drogas e Crime (UNODC) (MAURER, 2011 apud BARROS, 2015). De acordo com essa estrutura o Terceiro Comitê cuida das questões socioeconômicas que permeiam o ciberespaço, sempre baseada em uma ampla analise jurídica voltada também para a segurança cibernética (BARROS, 2015).

Finalmente o Segundo Comitê de Assembleia Geral da ONU possui a atribuição de unir as atividades desempenhadas pelo Primeiro e pelo Terceiro Comitês, ou seja, a posição da política-militar somada com as questões econômicas voltadas para um desenvolvimento de uma cultura da segurança cibernética global (MAURER, 2011 apud BARROS, 2015).

No ano de 2013, inúmeros debates foram realizados entre os Comitês e os órgãos auxiliares da ONU sobre a questão da segurança cibernética, ocasionando na aprovação de comum acordo no “Relatório sobre os desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional”. Esse acordo comprova que é possível uma regulação do ciberespaço, mesmo que existam muitas outras questões mais

melindrosas, trazendo um equilibro internacional na utilização do ciberespaço. Sendo assim esse acordo segundo Barros:

> [...] reconhece a plena aplicabilidade do Direito Internacional ao comportamento do Estado no ciberespaço, ao considerar indispensável a obediência aos princípios e medidas segurança estipulados para os outros domínios de convivência, como, por exemplo, o respeito à soberania, a não-intervenção, a limitação ao uso de força, o respeito aos direitos humanos, dentre outros (ONU, 2013 apud BARROS, 2015, p. 145).

É obseervado que mesmo existindo vários conteúdos específicos que tratem dessa relação do Direito Internacional com o ciberespaço, seus princípios basilares se mantêm presentes no desenvolvimento de uma futura regulação jurídica a respeito dessa nova realidade em que vivemos no século XXI.

Será analisado agora o que a Convenção do Conselho Europeu sobre Crime Cibernético de 2001 trouxe de disposições que visem regular o ciberespaço. O conselho Europeu agrupa os chefes de governo e de Estado para discutir assuntos políticos mais importantes a respeito de desenvolvimentos que normatizem questões políticas sobre segurança cibernética na organização de cada região na Europa. Destarte a União Europeia tem levantado a bandeira em prol de uma segurança cibernética mais sólida que protejam os sistemas de informação garantindo um tráfego econômico online estabilizado, assim como, lutando contra os ataques que tenham visão em desestruturar as relações amistosas entre os Estados Soberanos (PAKALNIŠKIS, 2011 apud BARROS, 2015).

É importante ser destacado no trabalho, além da Convenção do Conselho Europeu sobre Crime Cibernético, ser apresentado o primeiro tratado internacional a versar sobre a questão da segurança cibernética, que é a Convenção de Budapeste sobre o Cibercrime. A principal finalidade dessa convenção é traçar uma proteção da sociedade contra a cibercriminalidade utilizando uma política criminal que conte com uma cooperação internacional dos Estados (CONSELHO EUROPEU, 2001 apud BARROS, 2015). Dessa forma a Convenção permite que Estados não participantes da União Europeia e consequentemente Estados não europeus ratifiquem o tratado internacional. Potências como os Estados Unidos ratificaram esse tratado e posteriormente vem fazendo pressões políticas para o Brasil também participar.

No ano de 2004 foi criada a Agência Europeia para a Segurança das Redes e da Informação (ENISA), com o objetivo de administrar a segurança das informações das entidades privadas na Europa (SCHIBBERGES, 2015 apud BARROS 2015).

A ENISA tem a função de garantir os direitos humanos dos cidadãos europeus e dos sujeitos não estatais no âmbito da segurança cibernética, impedindo as violações desse direito fundamental pela via eletrônica. Além dessa função, a ENISA cuida da vigilância nas relações cibernéticas entre o continente europeu e o resto do mundo, mapeando, analisando, prevenindo, as demais ameaças vindas do ciberespaço que possam ofender os cidadãos ou pessoas jurídicas de direito privado, funcionando como uma agência de apoio à União Europeia na defesa da segurança cibernética (SCHIBBERGES, 2015 apud BARROS 2015).

5. CONCLUSÃO

Nesta pesquisa monográfica, procurou-se atingir o objetivo geral analisando de que maneiras o Direito Internacional pode modificar seu sistema jurídico através de doutrinas e normas para regular a realidade da guerra cibernética, trazendo uma segurança jurídica mais efetiva ao ciberespaço. Diante disso o trabalho investigou, partindo desde o início, as doutrinas mais clássicas e abrangentes como a soberania e a jurisdição, até teses, explicações mais complexas e específicas dentro dessas questões abrangentes relacionadas a utilização do ciberespaço na guerra cibernética.

No desdobramento da soberania tem-se como resultado o constitucionalismo do Direito Internacional levando em conta a decadência do poder soberano dos Estados diante da interdependência nas relações internacionais, já que o instituto da soberania a cada vez mais se torna impraticável por conta de sua característica assoberbada do poder estatal. Essa constitucionalização do Direito Internacional relativiza alguns direitos inerentes a personalidade dos Estados, pois atos realizados na guerra cibernética podem levar a guerra cibernética propriamente dita e o Direito com o apoio da ONU pode desenvolver formas de dirimir esses conflitos limitando essa postura ativa e destrutiva que a soberania propõem.

Passando agora para o estudo da jurisdição, compreendeu-se que com base no conceito clássico sendo aplicado ao ciberespaço, é demasiadamente ampla a atuação desse domínio, porque este mistura elementos físicos, que são mantidos através de infraestruturas como servidores, sedes e outros elementos reais no território de determinados Estados, e elementos virtuais que é o próprio funcionamento lógico ocorrendo o fluxo de informações, que transpõem as fronteiras físicas e jurisdicionais dos mesmos. Por ser um domínio híbrido foram abordadas temáticas doutrinárias jurídicas *sui generis* tratadas pelo Direito internacional, como a questão os condomínios globais ou *global commons* que seriam áreas comuns ou espaços globais regulados pelo Direito Internacional e áreas que são submetidas à jurisdição e soberania dos Estados sendo criado de acordo com a realidade do ciberespaço e a pluralidade dos entes presentes na comunidade internacional.

Foi estudado também outra visão do Direito Internacional sendo desenvolvido pelo alemão Gunther Teubner, que é o direito transnacional ou o *global law*, constituindo-se na ideia que vai além da soberania e jurisdição dos Estados, deixando de lado a tradição jurídica do Estado ser o centro como o legislador, aplicador e ordenador das normas nas relações internacionais. Isso leva o direito transnacional a criar formas de comunicações de redes especializadas como a *lex mercatória*, formando um painel composto de vários sistemas

jurídicos inter-relacionados não estando necessariamente conectados com a postura soberana do Estado. Esse painel acaba por trazer uma repolitização do Direito internacional para uma possível formação de uma legislação para o ciberespaço e dando mais segurança jurídica ao fenômeno da guerra cibernética.

Por fim o trabalho analisou o ciberespaço tanto em sua parte específica detalhadamente passando por sua evolução até os dias de hoje, como o seu prolongamento na esfera jurídica abordando pontos vitais na legislação da ONU. Por inicio foi caracterizado o ciberespaço como um domínio operacional que se utiliza do elemento informação, sendo no século atual o principal vetor que alimenta, cria e estrutura esse sistema composto por várias tecnologias informacionais. Sendo assim o ciberespaço se tornou uma nova forma de poder global, estando ao lado do *hard power* e do *soft power* como foi estudado detalhadamente, além do *smart power* que é um poder extremamente eficaz e aliado ao ciberespaço, resultando em uma amplitude complexa no alcance de objetivos extremamente relevantes para os Estados soberanos na influência dos demais entes da comunidade internacional.

Superada as explicações acerca dos demais poderes influentes na comunidade internacional, tem-se um aprofundamento na interpretação se o uso da força através do ciberespaço pode ser utilizado na legítima defesa com a devida autorização do Conselho de Segurança da ONU. Contudo para falar-se de legítima defesa é necessário caracterizar o ataque cibernético como um ataque armado, trazendo a visão do suíço Jean Pictet baseado no escopo, duração e intensidade suficiente, tal qual as 3 abordagens que aperfeiçoaram a sua visão sendo a abordagem instrumental, a abordagem baseada nos efeitos e a responsabilidade estrita para a verificação de um ataque armado ser visto como um ciberataque.

Outro ponto interessante abordado no trabalho foram os seis critérios avaliativos elaborados por Michael N. Schmitt, dando uma ideia futura de bases normativas internacionais para classificar os ataques cibernéticos. Já no final foi estudando a possibilidade dos Estados que não monitoraram de maneira efetiva seu território, deixando passar ataques cibernéticos, serem punidos mesmo que não se saibam os reais autores do ataque, fazendo que os Estados cada vez mais monitorem e contribuam no aperfeiçoamento comum de legislações e na própria segurança do sistema cibernético.

Com base nos parágrafos relatados a cima, confirma-se de maneira parcial da hipótese do trabalho, porque o Direito Internacional possui institutos jurídicos seculares que precisam ser repensados para a nova realidade tecnológica sendo a principal marca do século XXI, em função de não estarem dando mais conta de maneira efetiva do novo fenômeno do ciberespaço e da guerra cibernética. Isso quer dizer que é possuído um grande suporte

doutrinário com várias teses que podem modernizar o Direito Internacional, contudo a assimilação do próprio sistema jurídico internacional é por demais complexa, já que fatores como a política internacional e a economia são essenciais para permitir uma normatização que traga mais segurança a guerra cibernética. Mesmo que tenham vários órgãos criados para assessorar a ONU sobre questões cibernéticas, ainda não se sabe como a comunidade internacional irá se comportar ao longo dos anos a respeito da regulação da guerra cibernética. Isso se faz concluir que o presente trabalho monográfico contempla um horizonte de novos estudos neste assunto tão abrangente e relevante para as futuras relações que pautam o Direito Internacional, necessitando ser continuado não só no estudo do próprio Direito mas também no estudo na área das Relações Internacionais e até mesmo na área da economia.

6. REFERÊNCIAS

ACCIOLY, Hildebrando; CASELLA, Paulo Borba. **Manual de Direito Internacional Público**. 20. ed. São Paulo: Saraiva, 2012.

BARROS, Renata Furtado de. **Guerra cibernética e os novos desafios do direito internacional**. 2015. 169 f. Tese (Doutorado) – Programa de Pós-Graduação em Direito, Pontifícia Universidade Católica de Minas Gerais, Minas Gerais, 2015.

BARBOSA, Luiza Noqueira; Moschen, Valesca Raizer Borges. **O direito transnacional (''global law'') e a crise de paradigma do estado-centrismo**: É possível conceber uma ordem jurídica transnacional? Revista de Direito Internacional, v.13, nº3, dez. 2016.

BBC BRASIL. **Estônia acusa Rússia de 'ataque cibernético' ao país.** 2007. Disponível em:<http://www.bbc.com/portuguese/reporterbbc/story/2007/05/070517_estoniaataquesinternetrw.shtml>. Acesso em: 24 de mai. 2018.

COLOMBO, Silvana. O princípio da soberania dos Estados face ao direito internacional do ambiente. **UNOPAR Científica** - Ciências Jurídicas e Empresariais, Londrina, v.9, n.1, p.5-12, mar. 2008.

COUNCIL OF EUROPE. **Convention on Cybercrime (2001)**. Disponível em:<https://rm.coe.int/1680081561>. Acesso em: 7 de nov. 2018.

CEIRI NEWSPAPER. **O vale do Silício da China e a regulação do ciberespaço**. 2017. Disponível em:< https://jornal.ceiri.com.br/o-vale-do-silicio-da-china-e-regulacao-do-ciberespaco>. Acesso em: 22 de nov. 2018.

FERNANDES, José Pedro Texeira. O direito internacional humanitário e a emergência da ciberguerra. Revista de Direito Internacional, Brasília, v.9, n°2, jul-dez. 2012.

FERRAJOLI, Luigi. **A soberania no mundo moderno**. São Paulo: Martins Fontes, 2002.

GARDINI, Mayara Gabrielli**. Terrorismo no ciberespaço**: o poder cibernético como ferramenta de atuação de organizações terroristas. Fronteira. Belo Horizonte, v. 13, n. 25 e 26, p. 7 - 33, 2014.

LIMA, Gabriela Eulalio de. **Ciberataques:** Uma reflexão sobre a responsabilidade internacional dos Estados. Caderno de Relações Internacionais, v.8, nº15, jul-dez. 2017.

MAZZUOLI, Valerio De Oliveira. **Curso de direito internacional público**. 5. ed. São Paulo: Revista dos Tribunais, 2001.

MINIONU. **Svalbard**: O arquipélago internacionalizado. 2018. Disponível em: <https://minionupucmg.wordpress.com/2017/06/16/svalbard-o-arquipelago-internacionalizado>. Acesso em: 22 de nov. 2018.

NYE, Joseph S. **O futuro do poder**. Tradução de Magda Lopes. 1. ed. São Paulo: Benvirá, 2012.

MARTINS, Thiago. A Relativização do Princípio da Soberania no Direito Internacional. **Virtuajus.** Revista Eletrônica da Faculdade Mineira de Direito, v. 8, p. 1-13, 2009.

MAURER, Tim. Cyber Norm Emergence at the United Nations – An Analysis of Activities at the UN Regarding Cyber-Security. **Explorations in Cyber International Relations Discussion Paper Series**, Belfer Center for Science and International Affairs, Harvard Kennedy School, set. 2011. Disponível em: <http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf>. Acesso em: 7 de nov. 2018.

ONU BR. Nações Unidas do Brasil. **Carta das Nações Unidas.** Disponível em: <https://nacoesunidas.org/carta/>. Acesso em: 26 de mai. 2018.

REVISTA MUNDORAMA**. Ciberespaço e Internet**: Implicações Conceituais para os Estudos de Segurança, por Diego Rafael Canabarro e Thiago Borne. 2013. Disponível em:< https://www.mundorama.net/?p=11226>. Acesso em: 8 de set. 2018.

ÚLTIMO SEGUNGO IG. **Pentágono acusa Exército chinês de ciberataques contra os EUA; China nega**. 2013. Disponível em:<https://ultimosegundo.ig.com.br/mundo/2013-05-07/pentagono-acusa-exercito-chines-de-ciberataques-contra-os-eua-china-nega.html>. Acesso em: 19 de nov. 2018

UN DOCUMENTS. **Gathering a Body of Global Agreements.** Disponível em: <http://www.un-documents.net/a25r2625.htm>. Acesso em: 20 de nov. 2018.

VAZ, Vânia. **Comitê do Conselho de Segurança das Nações Unidas**: A primeira guerra mundial da web e a urgência na criação de uma resolução cibernética nacional. Curso de Direito do Centro Universitário do Rio Grande do Norte, Natal, 2016.