PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Programa de Pós-Graduação em Direito

Renata Furtado de Barros

GUERRA CIBERNÉTICA E OS NOVOS DESAFIOS DO DIREITO INTERNACIONAL

Belo Horizonte
2015

Renata Furtado de Barros

GUERRA CIBERNÉTICA E OS NOVOS DESAFIOS DO DIREITO INTERNACIONAL

Tese apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica de Minas Gerais, Área de Concentração: Direito Público, Linha de Pesquisa: Direitos Humanos, Processo de Integração e Constitucionalização do Direito Internacional, como requisito para obtenção do título de Doutor.

Orientador: Prof. Dr. Mário Lúcio Quintão Soares.

Belo Horizonte
2015

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

Barros, Renata Furtado de
B277g Guerra cibernética e os novos desafios do direito internacional / Renata Furtado de Barros. Belo Horizonte, 2015
169 f.: il.

Orientador: Mário Lúcio Quintão Soares
Tese (Doutorado) - Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito.

1. Direito internacional público. 2. Cibernética. 3. Ciberespaço. 4. Guerra (Direito internacional público). 5. Direitos humanos e globalização. 6. Sociedade da informação. I. Soares, Mário Lúcio Quintão. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito. III. Título.

CDU: 341.36

Renata Furtado de Barros

GUERRA CIBERNÉTICA E OS NOVOS DESAFIOS DO DIREITO INTERNACIONAL

Tese apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica de Minas Gerais, Área de Concentração: Direito Público, Linha de Pesquisa: Direitos Humanos, Processo de Integração e Constitucionalização do Direito Internacional, como requisito para obtenção do título de Doutor.

_____
Mário Lúcio Quintão Soares (Orientador) – PUC Minas

_____
José Luiz Quadros de Magalhães – PUC Minas

_____
Lusia Ribeiro Pereira – PUC Minas

_____
Alexandre Melo Franco Bahia – UFOP

_____
Juliana Maria Matos Ferreira – Estácio

_____
Maria Emília Naves Nunes – PUC Minas (suplente)

_____
Angela Maria Siman – PUCMINAS (suplente)

Belo Horizonte, 03 de julho de 2015.

Dedico esse trabalho acadêmico aos meus pais, pelo apoio, encorajamento, amor e pelos ensinamentos que formam os alicerces da minha vida.

Ao meu pai, Professor Raul de Barros Neto, interlocutor nessa tese que com paciência ouviu, leu e criticou esse trabalho.

À minha mãe, Vânia Maria Fonseca Furtado, pilar afetivo, que nos momentos mais difíceis foi o colo que me deu forças para continuar.

AGRADECIMENTOS

À Deus, presença constante em minha vida, causa primeira de todas as coisas;

Ao meu orientador, Professor Dr. Mário Lúcio Quintão Soares, meu grande apoio acadêmico, filho da utopia, incentivador da construção de um Direito Internacional revolucionário e democrático;

Aos meus amados pais minha eterna gratidão pela contribuição afetiva e intelectual, determinantes para a minha formação moral;

Aos meus queridos irmãos Felipe e Lucas, professores dedicados no sonho utópico da vida docente, obrigada pelo carinho e apoio;

À Laila, minha querida amiga de toda uma vida e ao Chico pelas alegrias malucas;

Aos Professores José Luiz Quadros de Magalhães; Lusia Ribeiro Pereira, Leonardo Nemer Caldeira Brant, Carlos Augusto Canêdo Gonçalves da Silva e Bruno Wanderley Jr.;

Aos colegas e funcionários do Programa de Pós-Graduação em Direito da PUC-Minas, pelo apoio e companheirismo;

Aos colegas e amigos do Centro Universitário da Faculdade Estácio de Sá de Belo Horizonte, em especial à Profa. Dra. Juliana Maria Matos Ferreira e à Profa. Maria Ângela Brescia Gazire Duch, meus agradecimentos pelo reconhecimento profissional e pela amizade;

Ao Prof. Wesley Roberto de Paula pelo apoio nas lutas acadêmicas diárias no Centro Universitário da Faculdade Estácio de Sá de Belo Horizonte;

Aos colegas e amigos da PUC Minas, unidade São Gabriel, em especial à Profa. Dra. Maria Emília Naves Nunes, obrigada pelas oportunidades profissionais;

Às professoras Alana Carlech Correia, Luciana Maria Reis Moreira e Sara Costa Benevides pela amizade e apoio em toda essa jornada;

Aos meus alunos, razão constante de estudos e reflexões, que me desafiam buscar o aperfeiçoamento pessoal e crescimento acadêmico e profissional.

À beira do caos é o lugar onde a vida tem estabilidade suficiente para se sustentar e criatividade suficiente para merecer o nome de vida. (WALDROP, 1992, p. 12).

RESUMO

O ciberespaço, novo domínio relacional no qual ocorrem conexões interativas, no âmbito nacional e internacional, requer um olhar apurado do direito para os perigos que representa. O presente trabalho tem com objeto de estudo o ciberespaço como um domínio de guerra e os desafios que essa análise apresenta para o Direito Internacional. O domínio do ciberespaço é definido como o quinto domínio da guerra, após a terra, o mar, a água e o espaço. Elege-se autores que adotam uma análise sistêmica da humanidade, e sustenta-se, consequentemente, uma análise holística do sistema mundial, com a quebra dos paradigmas lineares adotados pela ótica cartesiana positivista. O desenvolvimento da temática central da guerra cibernética ocorre, em um primeiro momento, por meio da ideia de complexidade de Edgar Morin aplicada à sociedade internacional e ao Direito Internacional, para se compreender efetivamente as relações de caos e o surgimento da cibernética, nas relações interativas da sociedade internacional. Analisa-se, também, o atual estado de guerra cibernético, a aplicação da atual legislação internacional em vigor para esse domínio e as possíveis soluções encontradas por alguns organismos internacionais. Os pontos principais abordados tratam da preservação da soberania dos Estados, no âmbito do ciberespaço, e da necessidade de se atentar para a defesa do Direito Internacional e dos direitos humanos nesse novo domínio. O trabalho não busca uma única solução para o problema da guerra cibernética e não se entende que criar um único pacto internacional, regulador das relações no ciberespaço, seria a solução. Trata-se de uma análise da nova realidade das relações cibernéticas internacionais e da necessidade de se interpretar o Direito Internacional existente de acordo com as constantes interações, em rede, e os variáveis pontos de tensão existentes na complexa sociedade internacional. Vislumbra-se interpretar o ciberespaço como um condomínio global a ser utilizado e regulado por toda humanidade com responsabilidade.

Palavras-chave: Guerra cibernética. Sociedade internacional complexa. Direito Internacional complexo. Ciberespaço. Condomínio global.

ABSTRACT

Cyberspace, new relational domain in which interactive connections occur, nationally and internationally, requires a sharp look of the duty for the dangers it represents. The present work has with object of study cyberspace as a domain of war and the challenges that this analysis presents to International Law. The domain of cyberspace is defined as the fifth domain of warfare, after land, sea, space and water. Elect-if authors who adopt a systemic analysis of humanity, and is sustained, consequently, a holistic analysis of the world system, with the breaking of paradigms adopted by Cartesian positivist optical linear. The development of the central theme of the cyber war occurs, in a first moment, through the idea of complexity of Edgar Morin applied to international society and International Law, to effectively understand the relationships of chaos and the emergence of Cybernetics, interactive relations of international society. Also analyzes the current state of cyber war, the implementation of the current International Law in force for that domain and the possible solutions for some international organizations. The main points addressed deal with the preservation of the sovereignty of States, within the framework of cyberspace, and the need to pay attention to the defense of International Law and human rights in this new domain. The paper researches not a single solution to the problem of cyber war and don't understand that create a unique international treaty, regulator of relations in cyberspace, would be the solution. This is an analysis of the new cyber international relations reality and the need to interpret the existing International Law according to the constant interactions, networked, and the points of tension exist in variables complex international society. Can interpret the cyberspace as a global commons to be used and regulated by all mankind with responsibility.

Keywords: Cyber war. Complex international society. Complex International Law. Cyberspace. Global commons.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

IP – ‘*Internet Protocol’* ou Protocolo de Internet

IPv4 – Sistema de IP versão 4

IPv6 – Sistema de IP versão 6

N°. – número

LISTA DE SIGLAS

ABIN – Agência Brasileira de Inteligência

CEPESC - Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações

CDN – Conselho de Defesa Nacional

CREDEN – Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo

CIT – Corte Internacional de Justiça

DPF – Departamento de Polícia Federal

DSIC – Departamento de Segurança da Informação e Comunicações

ECOSOC – Conselho Econômico e Social da ONU

ENISA – Agência Europeia para a Segurança das Redes e da Informação

EUA – Estados Unidos da América

GOP - Guardiões da Paz

GSI – Gabinete de Segurança Institucional

ICANN – Corporação da Internet para Atribuição de Nomes e Números

MD – Ministério da Defesa

MERCOSUL – Mercado Comum do Sul

MIT – Instituto de Tecnologia de Massachusetts

MJ – Ministério da Justiça

OCX – Organização de Cooperação de Xangai

OEA – Organização dos Estados Americanos

OMS – Organização Mundial da Saúde

ONG – Organização não governamental

ONU – Organização das Nações Unidas

OTAN - Organização do Tratado do Atlântico Norte

RGI – Rede Global de Informação

RSI – Regulamento Sanitário Internacional

SAE – Secretaria de Assuntos Estratégicos

UE - União Europeia

UIT – União Internacional das Telecomunicações

UNIDIR – Instituto das Nações Unidas para Pesquisas sobre Desarmamento.

SUMÁRIO

1 INTRODUÇÃO

A era da informação e a introdução generalizada dos elementos digitais e da Internet, na vida humana, transformou a realidade social interna dos Estados e as relações internacionais. Na contemporaneidade, as relações humanas, em sua maioria, se dão em rede e são interativas. Essas relações englobam uma interatividade governamental, econômica, militar e até mesmo pessoal, dentre os entes civis e políticos da sociedade. O aumento da importância e do uso da tecnologia da informação e das interações, no ciberespaço, faz com que essas redes digitais sejam pontos de ameaça para a soberania dos Estados.

A marcha constante do progresso tecnológico trouxe inúmeros benefícios para a humanidade e possibilitou que gerações recentes pudessem salvar e preservar inúmeras vidas, pelas influências que esses avanços fizeram nas técnicas de saúde. Entretanto, a mesma tecnologia que salva vidas, também fomentou novas capacidades militares, nos campos de batalha. Além dos domínios convencionais da terra, mar, ar e espaço, a tecnologia possibilitou com que um novo domínio relacional humano fosse criado, o ciberespaço. A realidade da disputa de poder das relações internacionais, viabiliza com que o ciberespaço possa ser encarado como mais que um domínio de interação nacional e internacional, mas também como um campo de batalha para a guerra cibernética.

Os desafios encontrados nesse trabalho estão nas imprecisões para lidar com o novo domínio virtual, que foge das regras estabelecidas pela limitação física da natureza, existente nos demais domínios de guerra. A cibernética de segunda ordem trabalha com o ideal revolucionário da complexidade e da noção do pensamento sistêmico, pois entende o organismo ou sistema social com uma interação complexa aberta, sem predeterminações. Adota-se como marco teórico desse trabalho a cibernética de segunda ordem.

O ciberespaço pode ser definido como o domínio criado pelo uso da eletrônica. O poder cibernético é medido pela habilidade de usar esse domínio para alcançar um resultado específico e estratégico. O potencial desse novo campo de batalha está apenas começando a ser identificado, pelo Direito Internacional, e as vulnerabilidades de segurança nacional são inúmeras. Além disso, há um grande desafio a ser enfrentado, pelo Direito Internacional, que é o aumento de atores participantes das relações interativas, uma vez que soluções baseadas no

interestatismo não funcionam, nesse domínio virtual. O ciberespaço depende de uma cooperação entre os setores públicos e privados e entre os diferentes atores internacionais.

A complexidade da guerra cibernética está presente, em especial, pela nova realidade da assimetria. Esta refere-se à ideia de que, através de um ataque cibernético, atores com recursos limitados podem alcançar grandes resultados com seus ataques. Além disso, ao contrário dos domínios da terra, mar, ar e espaço, os ataques cibernéticos não vêm com os uniformes de um exército de ocupação, nem bandeiras estampadas, na verdade, a grande vantagem é a facilidade com que o rastro do ataque digital pode desaparecer em questão de segundos, gerando a impunidade. Não só é difícil determinar quem poderia ter sido responsável por um ataque, mas definir o que são atos de guerra, terrorismo, espionagem, crime, protesto, vandalismo, são desafios necessários de serem solucionados pelo Direito Internacional. Outro desafio complexo é definir o conceito de uso de força no âmbito do ciberespaço e quando esta força ensejaria o direito de exercer contramedidas de legítima defesa.

A sociedade internacional clama por respostas efetivas, do Direito Internacional, para a regulação de suas relações no ciberespaço, a fim de que o desenvolvimento tecnológico traga benefícios à humanidade. Analisa-se, nesse trabalho, conceitos tradicionais do Direito Internacional como a soberania e a jurisdição real, com o objetivo de interpretá-los na lógica sistêmica do ciberespaço.

Trabalha-se a hipótese da tentativa de regulação efetiva do domínio do ciberespaço, pelo Direito Internacional, objetivando uma maior estabilidade da nova realidade sistêmica tecnológica. Entretanto, todos os desafios apresentados pelo ciberespaço, devem ser analisados, em prol da construção de um sistema jurídico internacional que compreenda a nova realidade complexa das relações tecnológicas interativas.

Na cultura tradicional do legalismo jurídico há uma grande dificuldade de lidar com a incapacidade humana de obter certezas sobre as relações sociais. Esse trabalho tem o objetivo de abordar o novo paradigma da complexidade das relações humanas, levando em consideração a realidade complexa da sociedade internacional e a necessidade de reconhecimento pelo Direito Internacional dessa realidade. A partir do entendimento da existência de relações interativas, em rede, na sociedade internacional, objetiva-se estudar a cibernética e as consequências do

desenvolvimento tecnológico, do domínio do ciberespaço, para as relações de guerra no âmbito internacional.

Adota-se, também, a hipótese de revisitar o conceito de ‘global commons’, no texto traduzido como ‘condomínios globais’, que são áreas de recursos definidos como sendo aplicáveis a qualquer Estado soberano, ao domínio do ciberespaço. Os condomínios globais são socialmente construídos como, por exemplo, o alto mar, o fundo do mar, a Antártida, o espaço e a atmosfera global. Vislumbra-se a hipótese que o ciberespaço possa se enquadrar nesse regime jurídico. Por fim, analisa-se os princípios existentes, no sistema atual do Direito Internacional, e sua aplicabilidade nos casos de guerra cibernética.

Os capítulos foram organizados a fim de enfatizar a análise sistêmica e complexa do Direito Internacional, na Era Cibernética, e os desafios a serem enfrentados pela sociedade internacional. No segundo capítulo, realiza-se uma análise sobre a quebra de paradigmas cartesianos lineares e a introdução do pensamento complexo, base teórico-filosófica para a cibernética. Desenvolve-se o pensamento de que a troca interativa de informações, no ciberespaço, aumenta a complexidade das relações na sociedade internacional, fato que não pode ser ignorado pelo Direito Internacional.

A complexidade da sociedade internacional é discutida no terceiro capítulo, tendo como base jurídica a concepção sistêmica de Estado, que por sua característica interativa, apresenta-se como mais adequada para a pesquisa das relações travadas no ciberespaço. As interações constantes, no âmbito tecnológico, aumentam as tensões e interações dos diferentes atores internacionais, o que leva à reflexão dos impactos dessa nova perspectiva no Direito Internacional. Discute-se o aumento dos atores e das fontes jurídicas, que compõe o Direito Internacional, no ciberespaço de forma interativa. O propósito do terceiro capítulo é tratar do paradigma da complexidade do Direito Internacional, nas relações tecnológicas travadas no ciberespaço.

A análise do ciberespaço como um novo domínio da guerra é feita no quarto capítulo. As disputas constantes de poder, travadas nos cenários internacionais, previamente conhecidos, são também realizadas no ciberespaço. Discute-se a tendência atual de desenvolvimento do chamado poder cibernético (‘cyber power’), como estratégia para a disputa de poder entre os Estados, na política internacional. O domínio cibernético desafia as regras do Direito Internacional, até então limitadas

pelo espaço físico, com um ambiente mais hostil e complexo para a instauração da guerra.

O quinto capítulo trava uma discussão sobre o Direito Internacional e o estado de guerra cibernética. A guerra cibernética aumenta a possibilidade de atores não estatais participarem dessa disputa, uma vez que o ciberespaço facilita a interação, sem barreiras territoriais. A dominação ideológica, que se apresenta como uma manipulação tecnológica, é uma poderosa arma na guerra cibernética, travada entre os diferentes atores internacionais. Além disso, o respeito à soberania dos Estados é fruto de reflexões, no ciberespaço, e levanta-se a hipótese de necessidade de preservação do respeito à esse princípio para se evitar a guerra. Questiona-se os conceitos clássicos de soberania, analisando-a na perspectiva das relações sistêmicas e interativas estatais. A hipótese é de abandono do conceito de soberania absoluta, para se adotar o princípio da soberania no paradigma sistêmico. Nessa visão, só há soberania quando as sociedades sistêmicas possuem a liberdade de construírem suas identidades e diferenças. Vislumbra-se que a permissão da interação, no ciberespaço, e o respeito da construção das identidades estatais, permitem o verdadeiro exercício da soberania, na Era Cibernética.

A lei da guerra e sua possível aplicação, nos casos de guerra cibernética, são os objetos do sexto capítulo. Questiona-se a possibilidade de aproveitamento da legislação internacional de guerra, em vigor, para os conflitos travados no ciberespaço. Analisa-se a ideia de ‘controle de armas’ ou ‘restrição de armas’, utilizada para armas de destruição em massa e armas biológicas, ser aplicada por analogia no ciberespaço. Levanta-se a possibilidade de entender o ciberespaço como um domínio de jurisdição real. Apesar do ambiente do ciberespaço não poder ser delineado como território de um Estado, limites jurídicos podem ser impostos sobre os meios pelos quais as comunicações sem fio e transmissões de mídia são propagadas. Vislumbra-se, ainda, que entender o ciberespaço como um ‘condomínio global’ (‘global commons’) é uma possibilidade para a busca da regulação internacional das relações interativas, nesse novo ambiente. Discute-se, também, a possibilidade de aplicação das fontes tradicionais do direito internacional no ciberespaço.

No sétimo e último capítulo, estuda-se o atual quadro jurídico das relações internacionais, na Era da Cibernética. Analisa-se o princípio de legítima defesa, e a possibilidade de agir com contramedidas, na perspectiva de ataques de guerra

virtuais. Analisa-se os principais tratados internacionais, em vigor, e as ações preventivas e repressivas realizadas pela Organização das Nações Unidas (ONU), Conselho Europeu, Organização dos Estados Americanos (OEA), Organização de Cooperação de Xangai (OCX), Organização do Tratado do Atlântico Norte (OTAN) e pelo Brasil.

A partir da observância da existência do problema das relações interativas internacionais, no ciberespaço, e de uma possível guerra cibernética entre os atores internacionais, escolhe-se pesquisar o tema, através do método analítico dedutivo, tendo como embasamento a revisão bibliográfica e adota-se a hipótese de que o Direito Internacional, por meio do paradigma da complexidade, possa estabelecer um regramento nas relações sistêmicas do novo domínio.

O presente trabalho busca, portanto, fazer uma análise jurídico-social da problemática, a partir da perspectiva do paradigma da complexidade e das consequências, que as relações interativas, trazem para conceitos tradicionais do Direito Internacional Público.

2 O PARADIGMA DA COMPLEXIDADE DO PENSAMENTO CIENTÍFICO E A CIBERNÉTICA

O primeiro conceito importante de ser esclarecido nesse trabalho é o sentido da palavra ‘paradigma’ e como deve ser utilizado, de forma adequada, no mundo acadêmico. Utiliza-se a definição científica de ‘paradigma’, traçada por Thomas Kuhn (1922-1996), em seu livro ‘A Estrutura das Revoluções Científicas’ de 1962. O termo ‘paradigma’ tem sido utilizado de forma equivocada, sem o devido cuidado técnico como uma simbologia de qualquer mudança que possa ocorrer na sociedade contemporânea. No pensamento de Thomas Kuhn a ciência e a vida humana são movimentadas pela quebra de paradigmas, pela busca de novas respostas apesar de já se ter respostas prontas que se tornarão paradigmas ultrapassados. Desta forma, a vida contemporânea e a expressão mais contundente dela, que é a ciência, só se constrói e se elabora com a ruptura de conceitos, perspectivas, expectativas e modelos, dentro da grande possibilidade dos tempos atuais: a inovação.

Paradigmas, na concepção de Thomas Kuhn são “as realizações científicas universalmente reconhecidas que, durante algum tempo, fornecem problemas e soluções modelares para uma comunidade de praticantes de uma ciência”. (KUHN, 1970, p.13). Assim, a inovação se elabora com um novo construto paradigmático que certamente irá nortear a ruptura estabelecendo novas conexões, novas possibilidades de criar na perspectiva da pesquisa.

Qualquer estudioso, independente de sua área, estuda os paradigmas de sua época para se preparar, visando sua atuação profissional na sociedade, inserindo a pesquisa e a extensão, em seu campo de estudos. (KUHN, 1970, p.30). “Para ser aceita como paradigma, uma teoria deve parecer melhor que suas competidoras, mas não precisa (e de fato isso nunca acontece) explicar todos os fatos com os quais pode ser confrontada”. (KUHN, 1970, p.38). O paradigma obedece, então, a um conceito de circularidade, que permite abertura para novos conhecimentos e fatos científicos.

Entretanto, quando surge um novo paradigma, a comunidade científica se sente abalada diante da mudança das estruturas e da forma de pensamento na atuação em diferentes campos científicos. O novo paradigma, se for suficientemente forte para se sustentar, poderá fazer com que os antigos paradigmas desapareçam

de forma gradual; é assim que a ciência se transforma; com a quebra de paradigmas. (KUHN, 1970, p.39).

> Para que se compreenda como isso é possível, devemos reconhecer que um paradigma pode ser muito limitado, tanto no âmbito como na precisão, quando de sua primeira aparição. Os paradigmas adquirem seu status porque são mais bem sucedidos que seus competidores na Resolução de alguns problemas que o grupo de cientistas reconhece como graves. Contudo, ser bem sucedido não significa nem ser totalmente bem sucedido com um único problema, nem notavelmente bem sucedido com um grande número. De início, o sucesso de um paradigma — seja a análise aristotélica do movimento, os cálculos ptolomaicos das posições planetárias, o emprego da balança por Lavoisier ou a matematização do campo eletromagnético por Maxwell — é, em grande parte, uma promessa de sucesso que pode ser descoberta em exemplos selecionados e ainda incompletos. A ciência normal consiste na atualização dessa promessa, atualização que se obtém ampliando-se o conhecimento daqueles fatos que o paradigma apresenta como particularmente relevantes, aumentando-se a correlação entre esses fatos e as predições do paradigma e articulando-se ainda mais o próprio paradigma. (KUHN, 1970, p.44).

O grande fascínio da ciência, sob o olhar de Thomas Kuhn, é a possibilidade constante de se pesquisar, buscar, estudar e tentar compreender o mundo por meio da coragem de quebrar paradigmas na construção de novos paradigmas. O que se questiona, nesse trabalho, é exatamente a quebra do paradigma da ciência linear cartesiana, para a adoção do novo pensamento complexo, base para o entendimento da vivência em redes, da cibernética.

Diante disso, demonstra-se inquestionável que um dos grandes paradigmas aceitos pela ciência é a conceituação do que faz parte da própria ciência, pois o pensamento cartesiano, paradigma científico até muito pouco tempo não contestado, afirma que só é ciência aquilo que pode ser provado experimentalmente e seja imbuído somente de racionalidade e pode ser repetido quantas vezes se fizer necessário para se estabelecer como verdade científica, inserida em um *modus operandi* paradigmático.

A ciência tradicional, os dogmas religiosos e os sistemas organizacionais de governo, com um pensamento cartesiano, tem aprisionado o desenvolvimento humano, reproduzindo diferentes versões da caverna de Platão. Estudar a Teoria da Complexidade e a Cibernética é buscar entender as diferentes formas complexas que conectam os universos humanos, de forma não linear, na perspectiva desse novo paradigma vigente do mundo complexo, onde variáveis múltiplas se interconectam. O universo é uma grande caverna e o ser humano deve encarar a

realidade pautada nas incertezas da ciência não cartesiana, lembrando que essa caverna está conectada em rede com outras cavernas.

No século XV, a ciência baseava-se na conhecida regra da ‘navalha de Ockham’ que definia que “a pluralidade não deve ser postulada sem necessidade”, ou seja, buscava-se a objetividade na observação científica e escolhia-se sempre a resposta mais simples, levando-se em consideração somente os fenômenos essenciais para a explicação dos questionamentos humanos sobre o universo. (SPADE, 1999, p. 100).

A objetividade do pensamento científico é reproduzida por inúmeros outros cientistas, dentre eles Blaise Pascal (1623–1662), ao afirmar que o conhecimento era uma esfera e quanto mais essa esfera de conhecimento cresce maior é o seu contato com o desconhecido. Tudo que não podia ser explicado era atribuído aos deuses gregos, em uma noção não científica da realidade. (SPADE, 1999, p. 108).

A dinâmica da objetividade científica, pautada na materialidade da natureza atinge o seu ápice com o desenvolvimento da terceira lei de Newton que afirma que “toda ação provoca uma reação de igual ou maior intensidade, mesma direção e em sentido contrário". Nessa perspectiva, a ciência passa a acreditar em uma lógica de que sempre se obterá o mesmo resultado proporcional na experimentação científica. A certeza passa então a habitar o imaginário dos cientistas que afirmam que tudo que é subjetivo não pode receber a qualificação de científico. (PRIGOGINE, 1996, p.113).

O primeiro a questionar essa lógica objetiva da ciência foi Epicuro, em 307 a.C, ao desenvolver seu conhecido ‘dilema de Epicuro’, ou seja, muito antes do desenvolvimento da lei da ação e da reação. Em sua teoria da declinação dos átomos, Epicuro questiona a sua concepção de universo, que em tese seria constituído por átomos em movimento no vazio. Epicuro imaginava que os átomos cairiam todos em trajetórias paralelas e na mesma velocidade, entretanto, o choque dos átomos o levava a pensar no motivo dessas colisões, pois não lhe cabia uma explicação objetivamente científica para esse fato. Ele começa então a perceber a faceta ética ainda não explorada, em sua teoria. No sistema atômico tudo se explicava por uma única razão: a necessidade. Entretanto, o fatalismo e a dificuldade de explicar o comportamento das partículas atômicas o leva à incerteza da liberdade humana e inclusive sobre a vivência de uma vida moral, como concebia. (PRIGOGINE, 1996, p. 19).

O primeiro filósofo que começa a estudar o mundo sob a perspectiva da complexidade é Gaston Bachelard, (1884–1962), em seu livro “A Formação do Espírito Científico”. (BACHELARD, 1996). Este autor tece uma crítica ao espírito científico baseado em certezas e fatos e em uma “ética geométrica de representação”, ao afirmar que os acontecimentos científicos são colocados em uma ordem exata de episódios que nem sempre contam somente com um elemento objetivo para determiná-los. A tarefa científica de unir conhecimentos exatos e fatos por meio da experiência é, para ele, uma tentativa dos cientistas, que adotam o pensamento cartesiano, de criarem um meio do caminho entre o concreto e o abstrato, em busca do exato. (BACHELARD, 1996, p. 7).

Bachelard chama o pensamento linear científico de um “realismo ingênuo das propriedades espaciais”, uma vez que a análise científica não deve levar em consideração somente aquilo que o olho métrico cartesiano é capaz de ver, pois a real busca do espírito científico deve ser pautada em uma verossímil tentativa de conhecer o mundo e não apenas de mensurá-lo e ignorar aquilo que não pode ser medido, nomeando como ‘não científico’. O pensamento científico linear busca apenas a construção do espaço real científico, olvidando-se do abstrato e metafórico que, em uma análise social, interferem no resultado científico. “O matematismo já não é descritivo e sim formador. A ciência da realidade não se contenta com o como fenomenológico; ela procura o porquê matemático.” (BACHELARD, 1996, p. 7-8).

A necessidade humana de representar, geometricamente, e de explicar racionalmente, os fenômenos leva à ordenação linear que coloca a “teoria da ordem pura” como fundamental para o espírito científico cartesiano. O estudioso, com suas aspirações de racionalizar, criar e explicar de forma linear os fenômenos científico-sociais acaba, portanto, comprometendo os resultados da observação, pois a incerteza é temerosa para o cientista e para a humanidade. (BACHELARD, 1996, p. 8).

O primeiro grande obstáculo para o desenvolvimento do espírito científico complexo, segundo Bachelard, é a “experiência primeira”, ou seja, a colocação da concretude da experiência acima de qualquer crítica. A experiência, sem a intervenção da crítica, é uma base inconsistente para o desenvolvimento do raciocínio científico. (BACHELARD, 1996, p. 29).

O segundo obstáculo é o chamado de “conhecimento geral”. “Nada prejudicou tanto o progresso do conhecimento científico quanto a falsa doutrina do geral, que

dominou de Aristóteles a Bacon e que continua sendo, para muitos, uma doutrina fundamental do saber". (BACHELARD, 1996, p. 69).

A palavra e a verbalização da ciência são um obstáculo, segundo Bachelard. De fato, a expressão por meio das letras vê-se limitada diante da complexidade dos elementos estudados. A utilização de metáforas e analogias, antes da análise do que está sendo estudado, pode dificultar e até mesmo transformar aquilo que está sendo pesquisado. Assim, como a palavra pode estimular o pensamento, mal empregada também pode limitá-lo ao concreto. (BACHELARD, 1996, p. 91).

O sociólogo francês Pierre Bourdieu (1930-2002) analisa a força do "poder simbólico" diante da sociedade e, demonstra nitidamente a capacidade humana de transformar o real, por meio de representações da realidade, ou seja, da utilização da cognição e da subjetividade humanas na construção de uma realidade que muitas vezes é utilizada como arma de dominação. (BOURDIEU, 1989, p.13).

> O poder simbólico, poder subordinado, é uma forma transformada, quer dizer, irreconhecível, transfigurada e legitimada, das outras formas de poder: só se pode passar para além da alternativa dos modelos energéticos que descrevem as relações sociais como relações de força e dos modelos cibernéticos que fazem delas relações de comunicação, na condição de se descreverem as leis de transformação que regem a transmutação das diferentes espécies de capital em capital simbólico e, em especial o trabalho de dissimulação e transfiguração (numa palavra de eufemização) que garante uma verdadeira transubstanciação das relações de força fazendo ignorar-reconhecer a violência que elas encerram objetivamente e transformando-as assim em poder simbólico, capaz de produzir efeitos reais sem dispêndio aparente de energia. (BOURDIEU, 1989, p.15).

O mundo da linguagem, escrita ou falada, só é possível através do simbólico, não verbal, não explícito e constituído de subjetividade, inerente ao humano. Nesse particular, a ciência e a compreensão do mundo só são possíveis quando se concebe esse mundo de forma qualitativa, associado em rede com os aspectos quantitativos.

O conhecimento unitário e pragmático é apontado por Bachelard, dessa forma, como um outro obstáculo ao conhecimento verdadeiramente científico. Há uma necessidade de quebra de paradigmas, de modificação de utilização do pensamento empírico, priorizador da experimentação, e aplicação do pensamento filosófico, dotado não somente de elementos objetivos e lineares, mas também dos elementos não explícitos, intangíveis que constituem a argamassa do conhecimento científico. (BACHELARD, 1996, p. 103).

O cientista, ao delinear seu pensamento, tem outra tendência, a de atribuir qualidades materiais para descrever o fenômeno científico, esse fato Bachelard chama de substancialismo. A necessidade de materializar a ciência é um obstáculo para o estudo científico. (BACHELARD, 1996, p. 121).

A adoção do pensamento voltado para a observação do chamado de “real” limita também o desenvolvimento do pensamento científico. Inicialmente o realista, ao observar o mundo, reproduz em seu pensamento aquilo que enxerga como real, enquanto os ingênuos partiriam de teorias não baseadas no concreto. Entretanto, Bachelard afirma que “a certeza do realista provém de uma alegria avarenta”. (BACHELARD, 1996, p.164).

Portanto, o indivíduo que pretende saber pela reprodução do que vê como real tem como obstáculo perceber a subjetividade intrínseca na natureza e nas relações naturais e sociais, de forma míope e às vezes incompleta. A percepção de mundo voltada somente para o realismo coloca a substância material como determinante para a observação do olhar científico sobre a realidade. O culto ao realismo e à materialização científica gera um obstáculo epistemológico entre observador e observado, uma vez que toda subjetividade é desconsiderada. (BACHELARD, 1996, p.165). Essa ciência, sem dúvida, é ‘manca’, ‘claudicante’, uma vez que desconsidera a essência do cientista – a sua visão, como observador da observação.

Para Humberto Maturana (1928 –) toda objetividade é ‘entre parêntesis’, ou seja, toda observação é realizada de forma subjetiva, dependendo da visão do observador em relação ao observado. Não há fato científico sem o conteúdo subjetivo do cientista por mais racional e objetivo que ele queira ser. A ação humana pela própria estrutura cerebral-mental engloba emoção e razão e toda a ponta do processo de desenvolvimento da ciência e do mundo contemporâneo não pode desprezar o contexto emocional como ponto de partida de toda a racionalidade. Em outra linguagem, quer dizer que as emoções no contexto da subjetividade são elementos de iniciação de toda resposta cognitiva-racional, não sendo, portanto, dispensável como muitas vezes se veicula na abordagem científica cartesiana tradicional. (MATURANA,1998, p.34).

> Na tradição cultural do ocidente, na qual a ciência moderna e a tecnologia surgiram, nós falamos, na vida diária, de realidade e do real, como um

> domínio de entidades que existem independentemente do que façamos como observadores. (MATURANA, 1997, p. 39, tradução nossa)[1].

Além do realismo, Bachelard aponta a utilização do animismo para a descrição do pensamento científico como um obstáculo. A utilização da vida como pressuposto para a descrição do pensamento científico coloca-a como um 'dado científico', esquecendo-se que ela também é imbuída de subjetividade. (BACHELARD, 1996, p.209).

Além disso, Bachelard critica o culto ao pensamento quantitativo e afirma que qualquer conhecimento objetivo e imediato é falseado pela subjetividade do observador. As certezas quantitativas são prematuras e precisam ser analisadas com o pensamento crítico. (BACHELARD, 1996, p.259).

A partir das reflexões de Bachelard sobre o pensamento científico desvinculado da linearidade cartesiana, o filósofo contemporâneo francês Edgar Morin (1921–) desenvolve a ideia de complexidade, base para o pensamento sistêmico e da Teoria da Informação, vinculada à cibernética.

A noção de que não há certezas na ciência se torna mais evidente com o desenvolvimento do pensamento de Edgar Morin que introduz ao estudo do pensamento e da sociedade humana a noção de 'complexidade', transformadora dos paradigmas de certeza da ciência.

Em sua análise social, Morin afirma que o ser humano tem trabalhado o pensamento científico voltado para uma ética de certezas que formam a ciência; delimitando-se a natureza das relações humanas entre o que é uma certeza científica e o que não seria pautado de certezas e, portanto, não poderia ser tratado como científico. (MORIN; ALMEIDA; CARVALHO, 2002, p. 13).

O problema da complexidade é esquecido e até mesmo ignorado pelo paradigma da ciência linear cartesiana, que não admite a possibilidade de se viver em um mundo de incertezas e articulado em múltiplas redes de comunicação, interesses e, sobretudo valores. Morin, entretanto, demonstra que a realidade da ciência e da vida social é mais complexa que a dinâmica cartesiana do pensamento da 'causa e efeito'. A ciência não se constrói com continuidade, mas com rupturas e construto de novos saberes. (MORIN; ALMEIDA; CARVALHO, 2002, p.14).

---

[1] "En la tradición cultural occidental en la cual la ciencia moderna y la tecnología han surgido, nosotros hablamos, en vida diaria, de la realidad y de lo real, como un dominio de entidades que existen independientemente de que hagamos como observadores". (MATURANA, 1997, p. 39).

A partir do conceito de paradigma pode-se depreender que a primeira grande quebra de paradigma se deu com Galileu Galilei (1564-1642) e Copérnico (1473-1543) com a teoria heliocêntrica, mudando totalmente a visão de mundo e de universo do homem. A segunda quebra veio com a teoria evolucionista de Charles Darwin (1809-1882) que retira o homem do centro da criação e o coloca como resultado de um processo de evolução e adaptação que teve um grande percurso na história da vida. Esse conceito de Darwin rompe com todos os valores até então constituídos de ordem, inclusive espiritual-religiosa. A terceira quebra de paradigmas se dá com Sigmund Freud (1856-1939) ao apresentar ao mundo novidades psíquicas que desbancam a inocência das crianças (sexualidade infantil), a pulsão de morte que arrasta o sujeito para as suas dificuldades intrapsíquicas mais complexas e o inconsciente que consiste no substrato real da personalidade humana.

Warren Weawer (1894-1978) questiona o paradigma da linearidade científica. Weawer desenvolve o pensamento de que a complexidade não pode ser estudada de forma desorganizada, mas que organizar o pensamento não é buscar uma linearidade para a ciência. (WEAWER, 1948, p.537).

A complexidade em Morin não é sinônimo de complicação, de bagunça. A ideia de complexidade está ligada à profundidade e dificuldade do exercício do pensar. O desenvolvimento de um pensamento científico deve ser crítico às regras, palavras e lógicas pré-fabricadas; deve lutar contra a vontade do ser humano de simplificar o real e valorizar somente o material; além de não ignorar a subjetividade existente no mundo. (MORIN; ALMEIDA; CARVALHO, 2002, p. 14).

A teoria da complexidade, na realidade, não é uma teoria, mas um complexo de teorias. A palavra “complexo” deve ser analisada etimologicamente, pois vem da palavra em latim ‘plexus’ que significa ‘tecido’, ‘rede’, e a partícula ‘com’ significa ‘junto’, ou seja, a ideia de complexidade demonstra que a realidade não é linear, mas cheia de interações; tudo está ligado a tudo. Nessa nova perspectiva, quebra-se o paradigma da linearidade e percebe-se que uma pequena causa pode gerar um grande efeito e uma grande causa pode gerar um pequeno efeito. Não há proporcionalidade nas relações complexas, é o que se chama de metáfora da borboleta[2], princípio primeiro da teoria do caos. (PRIGOGINE, 1996, p.93).

[2] Na teoria do caos, o efeito borboleta se expressa pela dependência sensível que uma pequena mudança em um lugar ou em um sistema não linear pode causar com grandes consequências no

A partir desse aspecto, o ser humano deve enfrentar a realidade de que vive uma nova perspectiva, de que as certezas não existem e vivemos na incerteza, onde nada é linear e tudo está em constante ligação, em um complexo interativo inconstante. (PRIGOGINE, 2002, p.11).

> O termo científico 'caos' se refere a uma interconectividade subjacente que existe em eventos aparentemente aleatórios. Equações simples têm a capacidade de gerar movimento, de modo complexo, de modo sensível à medição, que parece ser por acaso. Isso demonstra que sistemas simples, obedecendo leis precisas, pode, no entanto, agir de forma aparentemente "aleatória" - o imprevisível levando ao novo. Loops de feedback existem em toda parte. (HAYLES,1991, p. 3, tradução nossa).[3]

Morin traz o questionamento de que a ideia do caos faz uma verdadeira revolução na percepção de mundo atual, uma vez que o mundo é visto pela ciência linear como uma máquina exata, principalmente a partir das leis de Newton, pelo desenvolvimento da Revolução Industrial e do positivismo científico de Augusto Comte, cheio de certezas e ordens. A vida, para Morin, é movimento, interação, complexidade e, consequentemente, incertezas desproporcionais. A relação no mundo virtual da internet é o exemplo mais clássico da complexidade, pode-se perceber com facilidade, nesse meio, a realidade complexa das relações humanas. Não se parte para o pensamento de que ou alguém é 'A' ou 'B'; mas muitas vezes ele é 'A' e 'B' ao mesmo tempo, assim como as suas relações interativas. O raciocínio complexo é aditivo, não é alternativo; includente, não excludente; ele proporciona a soma das variáveis que se compõe em redes de percepções e ações. (MORIN; ALMEIDA; CARVALHO, 2002, p. 17).

Os seres vivos e suas relações não são dotados de uma lógica linear, existem inúmeras variáveis que estão interconectadas. A terceira lei de Newton da ação e reação é questionada pelo pensamento complexo que além de afirmar que as reações não são proporcionais, diz ainda que elas não são imediatas. A natureza é mais complexa do que a limitação do pensamento linear, exemplo disso está na análise química do grafite e do diamante: objetivamente não há diferença entre eles,

---

futuro. O nome do efeito foi dado por Edward Lorenz e deriva de seu exemplo de teórico de que uma pequena borboleta que bateu asas semanas antes no Brasil pode acabar causando um grande tornado no Texas. (LORENZ, 1972, p.1).

[3] "The scientific term chaos refers to an underlying interconnectedness that exists in apparently random events. Simple equations have the ability to generate motion so complex, so sensitive to measurement, that it appears to be by chance. It has shown that simple systems, obeying precise laws, can nevertheless act in a seemingly 'random' manner – the unpredictable leading to the new. Feedback loops exist everywhere". (HAYLES,1991, p. 3).

a diferença está na complexidade de interações entre os átomos de carbono. (MORIN; ALMEIDA; CARVALHO, 2002, p. 20).

Karl Popper (1902–1994) observava a impossibilidade de se afirmar em ciência, pois o ser humano precisa compreender a sua incapacidade de saber. O conhecimento é mutável, o mundo observado se modifica, assim como o observador. O máximo que o homem pode fazer é conjecturar. (POPPER, 1972, p. 62).

> É comum dizer-se “indutiva” uma inferência, caso ela conduza de enunciados singulares (...), tais como descrições dos resultados de observações ou experimentos, para enunciados universais, tais como hipóteses ou teorias. Ora, está longe de ser óbvio de um ponto de vista lógico, haver justificativa no inferir enunciados universais de enunciados singulares, independentemente de quão numerosos sejam estes; com efeito, qualquer conclusão colhida desse modo sempre pode revelar-se falsa; independentemente de quantos cisnes brancos possamos observar, isso não justifica a conclusão de que todos os cisnes são brancos. (POPPER, 1972, p. 41).

A complexidade como base no pensamento sistêmico é terreno fértil para o matemático estadunidense Norbert Wiener (1894-1964) desenvolver o pensamento da complexidade através da criação do conceito de ‘cibernética’, tratando as organizações, grupos e pessoas como sistemas complexos, sistemas abertos que estão em constante interação com o meio ambiente, sendo vulneráveis às forças internas e externas. (WIENER, 1970, p. 25). Wiener ficou conhecido como fundador da cibernética que hoje viabiliza a existência da tecnologia em rede, em todo o mundo.

No mundo atual, não há que se questionar que o mundo é complexo e não linear. Primeiro foi a física quântica e depois a cibernética que aumentaram a capacidade humana de conhecer o desconhecido e expandir as dimensões e limites para o pensamento humano.

A cibernética deu ao homem uma nova compreensão de seus dons naturais e capacidades, além de ajudar a sedimentar a ideia de que informação é poder. O mundo é complexo, dinâmico e sistêmico, sendo assim, é necessário questionar como a religião e as organizações governamentais ainda estão tentando governar o mundo usando a lógica linear da ‘causa e efeito’. A análise mundial desenvolvida pelos pensadores das relações internacionais e do Direito Internacional ainda tem contemplado o mundo sob uma perspectiva reducionista, por meio de metáforas como a das bolas de bilhar ou de um relógio mecanizado. A visão mecânica do universo tem sérias limitações, quando há de se explicar a complexidade encontrada

em todos os meios, inclusive nas relações internacionais. Cabe aqui lembrar que a concepção mecanicista cartesiana de universo e das relações possui também grandes possibilidade.

Não se deseja, nesse texto, excluir o paradigma cartesiano, mas incluí-lo no novo e contemporâneo paradigma da complexidade.

A necessária nova visão e interpretação das relações humanas e internacionais se desenvolve desde 1948, com o nascimento da 'cibernética', de responsabilidade de Norbert Wiener e, mais recentemente, com a aplicação da Teoria do Caos de James Gleick. Trata-se de uma nova forma de fazer ciência e analisar as relações sociais que viabiliza respostas que o pensamento científico clássico não consegue explicar. Esse novo paradigma científico gerou a tecnologia que permite a descoberta de um universo que não é estático, mas em expansão. (MORIN; ALMEIDA; CARVALHO, 2002, p. 22).

Após o fim da Segunda Guerra Mundial, reuniu-se em Nova York, nos dia 8 e 9 de março de 1946, um grupo de vinte e um dos cientistas para discutir algo que intrigava a todos: sistemas que tinham propósitos e o conceito de 'feedback de informações', de grande potencial científico. Esse foi o primeiro de dez encontros realizados, hoje chamados de 'o big bang da era da informação'. Os principais cientistas envolvidos eram Dr. Arturo Rosenblueth do México, Dr. Norbert Wiener e Dr. Warren McCulloch do Instituto de Tecnologia de Massachusetts, nos Estados Unidos. (VASCONCELLOS, 2002, p.210).

Diante do estudo das teorias das mensagens Norbert Wiener, percebe-se a existência de novo campo científico que vai além do estudo da linguagem, com estudo mais aprofundado das relações da informação como meio de dirigir as máquinas e a própria sociedade, através de uma análise do sistema nervoso humano e suas relações com a utilização das máquinas por meio do envio de mensagens. (WIENER, 1954, p. 15).

Norbert Wiener decide, portanto, nomear esse novo paradigma do pensamento científico que une a relação humana com a informação e com as máquinas de 'cibernética'. O termo 'cibernética' foi escolhido por causa da palavra grega 'kubernetes' que significa 'controle'. A cibernética é, portanto, a ciência da comunicação e do controle do elemento animal (homem) e da tecnologia, por meio das máquinas. A comunicação do ser humano com a máquina integra os sistemas. (WIENER, 1954, p. 15-16).

Segundo Bertalanffy “a cibernética é uma teoria dos sistemas de controle baseada na comunicação (transferência de informação) entre o sistema e o meio e dentro do sistema, e do controle (retroação) da função dos sistemas com respeito ao ambiente”. (BERTALANFFY, 2010, p. 37).

Wiener demonstrou pela primeira vez que existia uma ligação entre dois mundos até então vistos como completamente dissociados: o mundo das máquinas e dos animas (homem). Ele comprovou que tanto os animais, quanto as máquinas apresentam um comportamento direcionado a um objetivo teleológico e usam um processo de ‘feedback’ ou seja, de retorno, na busca de suas finalidades.

Segundo Wiener “a sociedade só pode ser compreendida através de um estudo das mensagens e facilidades de comunicação de que disponha”. (WIENER, 1954, p. 25).

Em 1956, Ross Ashby publicou o seu livro “Introdução à Cibernética” e construiu uma base mais sólida para que a cibernética se tornasse um novo paradigma do pensamento científico, questionador da visão do papel das máquinas na sociedade, da sua complexidade e da interpretação da atuação do cérebro humano nas relações sociais. (ASHBY, 1956, p.5).[4]

> Durante os últimos anos, tornou-se evidente que o conceito de "máquina" deve ser extensamente prolongado, se for para incluir os desenvolvimentos mais modernos. Especialmente isso é verdade, se estamos estudando o cérebro e tentando identificar o tipo de mecanismo que é responsável por poderes pendentes do cérebro de pensamento e ação. Tornou-se evidente que, quando ousamos duvidar se o cérebro pode ser uma máquina, as nossas dúvidas foram devidas principalmente ao fato de que por “máquina” entendemos algum mecanismo do tipo muito simples. Familiarizado com a bicicleta e a máquina de escrever, que estavam em grande perigo de tomá-los como o tipo de todas as máquinas. A última década, no entanto, corrigiu este erro. Ela nos ensinou como restrita nossa perspectiva costumava ser; por isso desenvolveu-se mecanismos que ultrapassavam em muito o máximo que se pensava possível, e nos ensinou que “mecanismo” ainda estava longe de ser esgotado em suas possibilidades. Hoje sabemos apenas que as possibilidades vão além de nossa visão mais distante. (ASHBY, 1951, p. 1, tradução nossa).[5]

---

[4] Outros pensadores que contribuíram para a cibernética foram: West Churchman, Russel Ackoff, Heinz Von Foerster, Stafford Beer e o Instituto de Santa Fé, a partir de 1984.

[5] “During the last few years it has become apparent that the concept of "machine" must be very greatly extended if it is to include the most modern developments. Especially is this true if we are studying the brain and attempting to identify the type of mechanism that is responsible for the brain’s outstanding powers of thought and action. It has become apparent that when we used to doubt whether the brain could be a machine, our doubts were due chiefly to the fact that by ‘‘machine’’ we understood some mechanism of very simple type. Familiar with the bicycle and the typewriter, we were in great danger of taking them as the type of all machines. The last decade, however, has corrected this error. It has taught us how restricted our outlook used to be; for it developed mechanisms that far transcended the utmost that had been thought possible, and taught us that

A Cibernética evoluiu e hoje divide-se em duas fases: de primeira e segunda ordens. A cibernética de primeira ordem, datada de 1940 a 1975, é demarcada pela caracterização do campo de estudos como um campo passivo, ainda voltado para o determinismo linear do cientificismo clássico. Norbert Wiener não conseguiu alcançar a junção do pensamento complexo com a cibernética, pois ainda afirmava em fé às leis da natureza. A cibernética de segunda ordem trabalha com o ideal revolucionário da complexidade e da noção do pensamento sistêmico, pois entende o organismo ou sistema social com uma interação complexa aberta, sem predeterminações. (VASCONCELLOS, 2002, p. 218). Adota-se como marco teórico desse trabalho a cibernética de segunda ordem.

O paradigma da cibernética passou a interpretar o mundo de acordo com novas regras complexas. Os estudiosos de Direito, Economia e Política têm utilizado a linguagem da cibernética de segunda ordem, pois um mundo complexo não pode ser governado e predeterminado por normas lineares.

A grande expansão da cibernética, no campo das comunicações, produz um mundo caracterizado por ricas relações interativas, diferenciadas por uma explosão de complexidade. A complexidade se torna então o novo paradigma temático que a ciência passa a explorar, em especial por meio da Teoria do Caos, como já observado.

O mundo das informações é um mundo paralelo, tão rápido como o mundo físico que cria e destrói novas realidades e relações a todo o momento. Nessa nova perspectiva, o ser humano precisa se atentar para a realidade de que os sistemas mecânicos são máquinas previsíveis e sistemas complexos tem um número tão grande de componentes ou relações que são impossíveis de serem descritos em detalhes, e, por essa razão, tenta-se criar modelos que muitas vezes não conseguem expressar a complexidade da realidade. O que se percebe é que os sistemas que encontram viabilidade no mundo complexo são aqueles que possuem uma capacidade plástica de adaptação, se reconstruindo de acordo com as novas necessidades dos sistemas. (PRIGOGINE, 1996, p.17).

O exemplo mais contundente de compreensão das redes adaptáveis é o conceito de plasticidade cerebral, vinculado ao funcionamento do sistema nervoso. O sistema nervoso, formado por cerca de cem a cento e quarenta bilhões de

---

‘‘mechanism’’ was still far from exhausted in its possibilities. Today we know only that the possibilities extend beyond our farthest vision”. (ASHBY, 1951, p.1).

elementos funcionais, caracteriza-se por neurônios que se interconectam de maneiras diferentes, de tal forma que todo neurônio é direta ou indiretamente ligado a todos os outros. (BUONOMANO & MERZENICH, 1998, p.150). Essa complexidade semelhante a um caos de conexões que confere a capacidade de organização desse sistema a partir dos estímulos, que recebemos de toda ordem (sensorial, motor e cognitivo) que possibilita, então, a partir do caos uma organização sistêmica altamente elaborada, complexa e eficiente.

Enquanto a física está interessada na energia e troca de massas, a cibernética preocupa-se com a informação que controla a energia. Como uma pequena quantidade de energia é capaz de controlar uma grande quantidade de energia? O conceito importante aqui é a amplificação, ou seja, fornecer uma quantidade e produzir outra quantidade. A informação é essa pequena quantidade de energia capaz de amplificá-la; a partir dessa reflexão a cibernética começa a provar a importância da informação no mundo complexo.

A cibernética construída por muitos fatores/determinantes ao mesmo tempo, é especialista em controle e comunicação, ao computar e alcançar resultados. Conhecedora de transformação, caos e auto-organização. Perita em complexidade e mudanças: em sistemas complexos adaptáveis. É a ciência capaz de explicar o aparente equívoco da noção de desproporção que faz com que pequenas mudanças possam causar grandes diferenças. Segundo Stafford Beer, é a ciência da efetiva organização. (BEER, 1975, p.2).

No pensamento complexo da cibernética percebe-se que toda a realidade da vida humana existe à beira do caos. Tudo que é vivo, parte do simples ao mais complexo, e os sistemas são abertos e auto-organizáveis, com governo e identidade próprios. Conceito importante, quando se menciona a auto-organização dos sistemas, é o conceito de *autopoiesis* desenvolvido pelos biólogos chilenos Humberto Maturana (1928–) e Francisco Varela (1946-2001).

A *autopoiesis* é o processo pelo qual uma organização ou um sistema organiza, produz e movimenta a si mesmo. Um sistema autopoiético consiste em uma unidade autônoma e de automanutenção, que contém os processos de produção dos componentes necessários para tanto. Os componentes, por meio de uma interação em rede complexa, geram de forma recursiva a mesma rede de processos que os produziu. (MATURANA; VARELA, 1980, p.82).

Inicialmente, imaginava-se que um sistema autopoiético seria operacionalmente fechado e estruturalmente determinado, sem entradas e saídas aparentes, mas no atual paradigma da complexidade percebe-se que as relações humanas são redes complexas e abertas entre diversos sistemas autopoiéticos que interagem a todo o momento, criam e recriam sua manutenção, com influências do sistema interno e do mundo externo. A célula de um organismo, uma corporação e até mesmo um Estado Nacional, são exemplos de sistemas autopoéticos complexos interativos.

Uma interessante analogia para se compreender o pensamento sistêmico da cibernética, está na comparação da vida humana com um vórtice, que nada mais é que um frequente fluxo turbulento de movimentos girando em espiral, parecido com um ciclone. Cada entidade constituinte da sociedade poderia ser representada por um ciclone em constante movimentação. O ciclone, representador da vida, tem características específicas: trata-se de entidade singular, individualizada, apesar de ser dependente do sistema onde vive.

Além disso, a vida humana é um fluxo, cada ser humano está interconectado a um sistema de natureza, sociedade e pensamento que o rodeia e que flui entre os seres humanos. Portanto, vive-se momentos que constantemente afetam os outros e criam um imprevisível caos em diferentes níveis, apesar de nesse caos se criar a ordem que hoje é conhecida.

A terceira característica é a de que o corpo humano é constantemente renovado e transformado regularmente. Somos, ao mesmo tempo, a mesma pessoa que éramos dez anos atrás e também, substancialmente, uma nova pessoa. Além do mais, pode-se dizer que as fronteiras entre o mundo interior e o exterior não são tão claras, até mesmo as fronteiras entre Estados também não o são e muitas vezes existem brechas utilizadas por imigrantes ilegais para violar a entrada nos territórios. Há um delicado equilíbrio entre forças opostas e informação de feedback gerando uma ordem espontânea. Os sistemas humanos são dominados por essas respostas dadas pelo universo e movimentam o universo com as reações que produzem, em um constante movimento. Uma pequena mudança pode produzir um grande resultado no ciclone humano.

"À beira do caos é o lugar onde a vida tem estabilidade suficiente para se sustentar e criatividade suficiente para merecer o nome de vida". (WALDROP, 1991, p.12, tradução nossa).[6]

Na teoria da cibernética, ligada à noção do caos, percebe-se que a vida depende de uma troca de informações, baseada na habilidade de processar informação, guardar informação e mapear informações sensoriais. A vida faz uma complexa transformação de informações para produzir mudanças e ações no mundo. "Na fronteira do caos e da ordem, encontramos sistemas que são suficientemente estáveis para armazenar informações e suficientemente difusos para transmiti-las". (WALDROP, 1991, p. 29, tradução nossa).[7]

Esse raciocínio leva a uma reflexão das relações humanas nas relações complexas. O estudo da ideia de complexidade é basilar para o desenvolvimento do presente trabalho, pois a partir da quebra do pensamento linear, busca-se estudar as relações internacionais no âmbito da cibernética, sem cair na armadilha de simplificação dessas complexas relações interativas em um novo domínio não físico, que inclusive é utilizado como domínio de guerra.

A cibernética é fundamental para a compreensão do poder que a informação e a manipulação dessa informação em prol da movimentação de homens e máquinas podem causar no atual cenário internacional. Como vem se demonstrando, a partir do pensamento complexo e da aplicação da teoria da cibernética, uma pequena ação pode causar uma grande reação, nas relações interconectadas pelo mundo virtual da sociedade contemporânea internacional.

[6] "The edge of chaos is where life has enough stability to sustain itself and enough creativity to deserve the name of life". (WALDROP, 1992, p.12).

[7] "At the border of chaos and order we find systems which are sufficiently stable as to store information and sufficiently diffuse as to transmit it". (WALDROP, 1992, p.29).

3 A COMPLEXIDADE DA SOCIEDADE INTERNACIONAL EM TEMPO DE GLOBALIZAÇÃO

O homem gasta bilhões de dólares tentando entender, cientificamente, a origem do universo, mas ainda não sabe explicar as condições de existência de uma sociedade estável, uma economia bem sucedida ou até mesmo como se alcançar a paz entre diferentes povos. (CHO, 2009, p.406). O paradigma linear científico tem viabilizado a visão de mundo muito mais voltada para o pragmatismo dos eventos entendidos como concretos do mundo natural; sendo que se tem uma facilidade muito maior de atingir uma compreensão daquilo que é visível na natureza do que das próprias interações humanas. Uma solução da contemporaneidade, que começa a ser explorada pela ciência da complexidade, é tentar compreender as interações humanas como relações estabelecidas de forma circular e não linear, viabilizadoras de trocas interativas em um sistema aberto de redes que está em constante modificação.

A física tem o objetivo de descrever a realidade de mundo, que é vivenciada no dia a dia; de uma forma simplista e linear, entende-se que ela explora um fato da realidade e busca compreendê-lo e traduzí-lo para a matemática, por meio de equações que viabilizem a possibilidade de se prever e testar o futuro. Apesar de seu sucesso, a física tem seus limites, pois não consegue entender efetivamente a complexidade que se relaciona com o ser humano, sendo que esse paradoxo é a grande discussão da complexidade de sistemas sociais humanos. (VITALI; GLATTFELDER; BATTISTON, 2011, p.17).

Os sistemas são compostos de inúmeras partes que estão interconectadas, sendo que se pode perceber a complexidade e a existências de sistemas complexos em diversos campos como o ecossistema, o cérebro humano, o mercado financeiro e até mesmo nas relações internacionais. Sistemas complexos são muito difíceis de serem expressos em equações matemáticas, pois a visão linear e pré-determinista da realidade não funciona na análise desses sistemas. (BERTALANFFY, 2010, p.82).

O que pode parecer como um comportamento complexo é, na realidade, o simples resultado de inúmeras interações entre os sujeitos que fazem parte desse sistema. A complexidade é, portanto, o resultado de interações. Não há mais a

possibilidade de se buscar entender o mundo por meio de equações ou teorias pré-deterministas sobre o comportamento das relações humanas.

É necessário compreender o sistema, ao se analisar as interações feitas por seus componentes. Além disso, a maioria dos sistemas complexos tem uma propriedade chamada de ‘emergência’, que determina que não é possível entender o comportamento das relações sistemáticas analisando somente os componentes do sistema, assim sendo o todo é na realidade mais que a soma das partes componentes dos sistemas. (VITALI; GLATTFELDER; BATTISTON, 2011, p.20). Deve-se esquecer da análise individual de partes do sistema e manter o foco nas regras e consequências das interações em rede. Como resultado disso, as relações em rede são a representação ideal dos sistemas complexos, sendo que as mensagens e a rede são os componentes do sistema e as conexões são feitas por meio da interação. Deste modo, percebe-se que a importância que as equações têm para a física, as redes complexas tem para o estudo do mundo complexo e, nesse caso, das relações internacionais por meio do paradigma da complexidade de sistemas.

Um alto grau de interconectividade pode ser ruim para se ter um sistema estável, pois qualquer nível de desequilíbrio pode se alastrar pelo sistema como uma epidemia. Cientistas têm criticado teóricos das ciências sociais que tem afirmado que ideias e conceitos são mais importantes do que dados coletados por meio de pesquisas quantitativas.

Há o jargão “deixe os dados falarem por si”, mas em um sistema complexo existe uma necessidade de se perceber que os critérios objetivos, observáveis a olho nu, não são o único paradigma de análise, assim como uma única teoria não consegue explicar todas as possíveis circunstâncias que podem ocorrer em um sistema social complexo.

A organização de um sistema complexo é resultado de uma auto-organização, remetendo ao conceito de *autopoiesis* previamente mencionado, essa é uma propriedade da complexidade que emerge das regras de interações no sistema. Existe, ainda, uma questão dificultadora da análise da sociedade como um sistema complexo que é a influência das ideologias pessoais do observador na produção de uma explicação a respeito da observação; como não há objetividade na natureza humana a análise da complexidade é ainda mais árdua de ser realizada. Na visão da complexidade, percepções ideológicas diferentes, divergências

culturais, religiosas, étnicas, dentre outras, somam à análise complexa, sendo que nesse paradigma toda a diversidade é importante ser considerada para se entender a interação dos sistemas. No ponto de vista da sociedade internacional, a realidade é tão complexa que todos os dogmas, teorias, elementos econômicos e culturais devem ser interconectados na busca da compreensão desse sistema.

A visão complexa é bem sucedida, ao ser aplicada na física, biologia, ciência da computação e até mesmo na psicologia, mas como entender e aplicar o paradigma da complexidade no Direito e nas relações internacionais?

No âmbito jurídico estatal, o sociólogo alemão Niklas Luhmann (1927–1998), aplicou a teoria dos sistemas à Teoria do Estado e entendeu o Estado como um sistema autopoiético.

Segundo Luhmann, o objetivo principal da lei é a função reguladora e/ou constitutiva das relações sociais. Diante da holística ordem complexa social, o objetivo dos sistemas jurídicos é de tentar trazer certa ‘estabilidade’ ao elemento de incerteza das relações entre os diferentes atores sociais. O sistema jurídico, em vez de reforçar a incerteza, oferece, pelo menos, um grau de probabilidade de consequências das ações na sociedade. Entretanto, essa regulação jurídica, só funcionará se levar em consideração a realidade sistêmica da sociedade, que exige uma constante dialética entre o direito e as demandas sociais, que são mutáveis. (LUHMANN, 2004, p.83). Para Mário Lúcio Quintão Soares (1952–), em seu livro Teoria do Estado, “a função das instituições políticas, na concepção sistêmica, é converter as demandas provenientes do ambiente social em respostas, que são dadas sob a forma de decisões políticas vinculatórias para toda a sociedade”. (QUINTÃO SOARES, 2008, p.45).

Assim, como na análise da complexidade estatal, percebe-se que com uma crescente e grande regularidade o ser humano está tendo que lidar sempre com surpresas sobre a dinâmica complexa da sociedade internacional, pois eventos que não eram antecipados acabam por ocorrer cada vez mais. Muitos pensadores das relações internacionais criam teorias que tentam explicar a sociedade internacional levando em consideração o poder econômico, o militarismo, a cultura, a religião e até mesmo a história dos povos, mas, essas teorias, por mais que consigam aclarar uma faceta das relações internacionais são teorias reducionistas que constantemente são surpreendidas por eventos que de forma inesperada as colocam em cheque. Isso ocorre, pois não há teoria linear, utilizadora de uma

linguagem analógica e limitada, que possa expressar e esclarecer toda a complexidade das relações interativas em rede da real sociedade internacional. Deve-se compreender que essas teorias não perdem o seu valor, mas podem ser observadas de forma aditiva à análise das relações internacionais complexas.

Há uma grande volatilidade em diferentes indicadores sociais que fazem com que compreendamos cada vez mais a limitação das interpretações atuais de mundo, no estudo da sociedade internacional. Não se deve espantar com surpresas nesse novo mundo complexo, pois a mudança e a constante movimentação fazem parte do sistema. De acordo com o sociólogo canadense Thomas Homer-Dixon (1956–), Diretor do Instituto de Waterloo para a complexidade e Inovação, existem três principais razões para termos mais mudanças e surpresas nas relações complexas das sociedade internacional: a interação de estresses múltiplos e simultâneos entre os atores internacionais; um aumento na exploração humana dos recursos e sistemas naturais e uma maior complexidade dos sistemas sociais, tecnológicos e humano-ecológicos. (HOMER-DIXON, 2006, p.31). Evidentemente esses três fatores são relacionados entre si e se influenciam de forma interativa.

Ao analisar especificamente, no âmbito das relações internacionais, percebe-se que o sistema internacional viabiliza de forma intensa a interação dos estresses múltiplos dos atores internacionais e faz com que haja uma movimentação imprecisa das conexões. Obviamente, tendo como base a teoria da complexidade, não se faz uma análise linear de que os estresses individuais somados seriam a representação do todo.

Thomas Homer-Dixon, ao analisar graficamente os estresses individuais e a complexidade dessa interação, utiliza-se do sinal de multiplicação para explicar a realidade e não do sinal de adição que seria utilizado por um pensador cartesiano. Os fatores multiplicadores do estresse são inúmeros, mas o primeiro grande fator seria o crescimento da velocidade de aumento da conectividade global das atividades, tecnologias e sociedades. Além disso, há o crescente poder de pequenos grupos destruírem coisas e pessoas, como ocorreu nos ataques de 11 de setembro de 2001. (HOMER-DIXON, 2006, p.38-40).

Além dos dois fatores citados por Thomas Homer-Dixon a sociedade internacional sofre a influência de todos os campos sociais que evidenciam a diversidade dos atores que a ela pertencem e nela atuam, seja por questões de

nacionalidade, religião, poderio econômico, força militar, diferenças étnicas, desenvolvimento tecnológico, dentre outros.

> A fragmentação da sociedade em pequenos grupos de identidades, em pequenas nomeações pode gerar novos tipos de problemas. A sociedade cosmopolita de Los Angeles, Nova York, São Paulo, Londres ou Paris não está além das nomeações ou dos predicados radicais. Ela está multifragmentada em diversos predicados radicais.
>
> Negros, asiáticos, coreanos, chineses, árabes, turcos, persas, nordestinos, brancos, góticos, cabeças raspadas, nacionalistas, racistas, mexicanos, hispânicos, caucasianos e mais um monte de nomeações convivem no espaço "democrático" da cidade. São obrigados pela lei a se suportarem embora os que aplicam a lei pertençam a um grupo e vejam o mundo limitado pela compreensão do seu grupo. (MAGALHÃES, 2014).

Apesar de se falar em uma fragmentação da sociedade por meio da criação de diferentes identidades, percebe-se a intensificação de relações interativas entre atores distintos que fazem parte da sociedade e esse é um ponto que acaba por estabelecer uma dinâmica de grande tensão e exclusão a partir do momento em que se tem a efetivação da divisão de um mundo interativo e em rede entre os nomeados como ‘nós’ e os excluídos chamados de ‘eles’. (DUSSEL, 1994, p.8).

A teoria da complexidade ainda leva a uma reflexão mais curiosa: a de que nem sempre os mesmos grupos, constituídos pelos mesmos atores, serão nomeados como ‘nós’ e nem sempre o conceito de exclusão ‘deles’ será atribuído aos mesmos sujeitos. Paulo Freire (1921–1997) analisa bem a questão complexa da mudança de visão de mundo em relação a diferentes grupos sociais quando afirma que a dinâmica entre opressor-oprimido está em constante movimentação. “A violência dos opressores, que os faz também desumanizados, não instaura uma outra vocação – a do ser menos. Como distorção do ser mais o ser menos leva os oprimidos, cedo ou tarde, a lutar contra quem os fez menos”. (FREIRE, 2013, p.41).

> A humanidade tem cruzando o globo por milênios, e estamos negociando grandes quantidades de matérias-primas e produtos manufaturados em todo o mundo por muitos séculos. Mas só nos últimos cem anos ou mais, enquanto a nossa população quadruplicou, criamos sistemas fortemente interligados no âmbito econômico, tecnológico e sociais – da agricultura industrial aos mercados financeiros – que penetram virtualmente em todos os cantos do planeta. Os kiwis no seu prato pequeno-almoço vem da Nova Zelândia, a própria placa vem da Malásia, enquanto o metal de tântalo no celular ao lado de seu prato vem das selvas do leste do Congo. (HOMER-DIXON, 2006, p.40, tradução nossa).[8]

[8] “Humankind has been crisscrossing the globe for millennia, and we’ve been trading large quantities of raw materials and manufactured goods around the world for many centuries. But only in the past hundred years or so, while our population has quadrupled, have we created tightly interlinked economic, technological, and social systems—from industrial agriculture to financial markets—that

As relações entre os sujeitos de Direito Internacional estão sustentadas por uma política constantemente interativa e competitiva, voltada para a disputa de poder entre os atores internacionais, cada vez mais estimulada pela busca do lucro, característica fundamental do ideal capitalista.

A caracterização humana, traçada por Thomas Hobbes, ao defender a necessidade da existência de um Estado-Leviatã persiste no cenário internacional que, por ter uma estrutura sistêmica em rede de conexões interativas extremamente interligadas, viabiliza a exaltação das diversidades e uma maior manifestação da natureza competitiva humana.[9]

Na perspectiva do Realismo Ofensivo, relata-se que os atores internacionais, em especial os Estados, vivem em constante insegurança em relação aos outros atores, o que os incentiva a competir constantemente pelo poder econômico e militar e a impor o seu modo de pensar e a sua cultura aos outros grupos sociais. (MEARSHEIMER, 2007, p.20).[10] Contudo, ao mesmo tempo em que há competição e embates ideológicos, os atores internacionais dependem uns dos outros para o seu desenvolvimento econômico-social e acabam estabelecendo inúmeras interações complexas.

Apesar de não se questionar a postura dos realistas que afirmam que o objetivo de cada ator internacional é o de defender seus próprios interesses, não se pode olvidar do fato de que a cooperação interativa também faz parte do interesse

---

penetrate virtually every corner of the planet. The kiwifruit on your breakfast plate comes from New Zealand, the plate itself comes from Malaysia, while the tantalum metal in the cell phone beside your plate comes from the jungles of eastern Congo". (HOMER-DIXON, 2006, p.40).

[9] "E dado que a condição do homem é uma condição de guerra de todos contra todos, sendo neste caso cada um governado por sua própria razão, e não havendo nada, de que possa lançar mão, que não possa servir-lhe de ajuda para a preservação de sua vida contra seus inimigos, segue-se daqui que numa tal condição todo homem tem direito a todas as coisas, incluindo os corpos dos outros. Portanto, enquanto perdurar este direito de cada homem a todas as coisas, não poderá haver para nenhum homem (por mais forte e sábio que seja) a segurança de viver todo o tempo que geralmente a natureza permite aos homens viver. Consequentemente é um preceito ou regra geral da razão, que todo homem deve esforçar-se pela paz, na medida em que tenha esperança de consegui-la, e caso não a consiga pode procurar e usar todas as ajudas e vantagens da guerra. A primeira parte desta guerra encerra a lei primeira e fundamental de natureza, isto é, procurar a paz, e segui-la. A segunda encerra a suma do direito de natureza, isto é, por todos os meios que pudermos, defendermo-nos a nós mesmos". (HOBBES, 1988, p.48).

[10] "As grandes potências raramente estão satisfeitas com a distribuição de poder; pelo contrário, enfrentam um incentivo permanente para a alterarem ao seu favor. Têm quase sempre intenções revisionistas e usarão da força para alterar o equilíbrio de 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 demasiado elevados, forçando as grandes potências a aguardarem circunstâncias mais favoráveis". (MEARSHEIMER, 2007, p.20).

desses atores, em muitas circunstâncias. Nem sempre a relação complexa interativa no cenário internacional vai gerar o resultado do embate entre os atores internacionais, pois pela complexidade e pluralidade do sistema não é possível prever efetivamente as reações e consequências da interação nesse cenário.

A realidade conflituosa das relações internacionais levará, segundo Immanuel Wallerstein, a uma necessidade de dominação ideológica dos grupos que manifestarem o seu pensamento de forma diferente da criada e vivenciada pelos detentores de poder. (WALLERSTEIN, 2007, p. 22).

As relações internacionais, sob a perspectiva do que os atores internacionais chamam de 'universalismo', giram em torno do que é de interesse das grandes potências de ser difundido para todos. A intenção inicial é de que somente aquilo que os grupos dominantes acharem necessário de ser 'universalizado', em nome de ideais como a paz, a segurança internacional e os direitos humanos, será implantado com a ajuda do Direito Internacional. Percebe-se que as políticas internacionais dos países pan-europeus baseiam-se em um agir moralista, no qual é atribuída a eles a responsabilidade de dizer o que é melhor para a sociedade. As suas condições de avanço econômico e militar os permitem se colocar como moralmente superiores a todos os outros Estados, uma vez que são os defensores dos valores e verdades determinados por eles como universais. O universalismo é uma afronta à realidade complexa do sistema internacional.

> A retórica dos líderes do mundo pan-europeu – sobretudo, mas não só, dos Estados Unidos e da Grã-Bretanha –, da grande mídia e dos intelectuais do establishment está cheia de apelos ao universalismo como justificativa básica para as suas políticas. Isso acontece principalmente quando falam das políticas relativas aos "outros" (os países do mundo não-europeu, a população dos países mais pobres e "menos desenvolvidos"). O tom costuma ser moralista, intimidador e arrogante, mas a política é sempre apresentada como se refletisse valores e verdades universais. (WALLERSTEIN, 2007, p. 26).

Wallerstein chama de 'universalismo europeu' a tentativa de imposição do pensamento da cultura social dominante sobre as demais culturas e, de 'universalismo universal', o ideal genuíno de buscar alcançar, nas relações internacionais, uma real universalidade e defesa de interesses de todos os grupos sociais, sem a imposição de um pensamento dominante. (WALLERSTEIN, 2007, p.27).

> No fundo, o debate sempre girou em torno do que queremos dizer como universalismo. Tentarei demonstrar que o universalismo dos poderosos sempre foi parcial e distorcido, um universalismo que chamo de "universalismo europeu" por ter sido promovido por líderes e intelectuais

> pan-europeus na tentativa de defender os interesses do estrato dominante do sistema-mundo moderno. (WALLERSTEIN, 2007, p. 27).

A realidade do sistema mundo moderno é a de tentativa de imposição da vontade dos mais fortes, mas, nas palavras de Wallerstein, “não há nada tão etnocêntrico, tão particularista, quanto a pretensão ao universalismo”. (WALLERSTEIN, 2007, p. 73).

Aqueles que adotam a doutrina da universalização não conseguem compreender o emprego da teoria da complexidade na sociedade internacional, uma vez que aplicam, de forma linear, aquilo que acreditam ser a vontade das grandes potências, sem perceber a necessidade destas interagirem, de forma constante com a sociedade. Não há nada mais linear e cartesiano quanto acreditar em um universalismo aplicado a uma sociedade complexa e sistêmica.

Wallerstein questiona se existe realmente, no sistema mundo atual, a possibilidade do homem identificar quais seriam os valores realmente universais e em quais condições seria possível, ao ser humano, encontrá-los. Ele chega à conclusão de que todas as formas de universalismo europeu, até mesmo o universalismo científico cartesiano, são passíveis de questionamento. (WALLERSTEIN, 2007, p. 107).

A preocupação excessiva, reforçada pelo pensamento moderno, em tratar da intelectualidade somente com a base do racionalismo científico, sem qualquer preocupação com os valores, a moral e a ética, após a análise crítica do sistema universalista europeu, cai por terra. No século XXI, há uma necessária mudança na postura intelectual de análise do sistema mundo.

A análise intelectual[11] do mundo será de papel fundamental para a quebra dos paradigmas[12] modernos, uma vez que ela não estará preocupada em agradar ou legitimar os que estão no poder, com o intuito de alimentar o universalismo

[11] “Então há algo de especial no papel do intelectual? Há, sim. Chamo de intelectuais as pessoas que dedicam seu tempo e energia à compreensão analítica da realidade e, presumivelmente, têm algum treinamento especial para fazer isso da melhor maneira possível. Não é pouca exigência. E nem todos querem tornar-se especialistas nesse conhecimento mais geral, ao contrário do conhecimento concreto específico de que todos precisamos para cumprir com competência qualquer tarefa. Assim, os intelectuais são generalistas, ainda que o alcance de sua competência seja de fato limitado a um domínio específico do vasto mundo de todo o conhecimento”. (WALLERSTEIN, 2007, p. 121).

[12] Como previamente mencionado, Thomas Kuhn, na obra “A Estrutura das Revoluções Científicas” afirma que a ciência só progride através do mecanismo de rupturas. O cientista percebe o mundo através do que Kuhn chama de paradigmas. A evolução da ciência se dá através do questionamento do paradigma anteriormente aceito e da criação de um novo paradigma (KUHN, 1970, p. 32).

europeu. Além disso, o compromisso da análise intelectual será o de descrever o sistema como ele realmente é, para evitar qualquer distorção de dominação ideológica e tecnológica. Essas análises terão o compromisso com a intelectualidade complexa, mesmo que desagradem os que se opõem aos que estão no poder ou, até mesmo, as inúmeras classes trabalhadoras. (WALLERSTEIN, 2007, p. 121). Essa postura reafirma a preocupação em não haver uma substituição do universalismo europeu por um outro tipo de universalismo arbitrário, que desconsidere o sistema complexo e que leve em consideração apenas o interesse de um grupo social específico.

A solução talvez esteja nas palavras de Léopold-Sédar Senghor que sugeriu, como solução para se alcançar relações humanas mais igualitárias “o encontro do dar e do receber”, ou seja, o estabelecimento de interações sistêmicas. (WALLERSTEIN, 2007, p. 119).

A solução final, trazida por Wallerstein, está na possível alternativa de aceitação de uma “multiplicidades de universalismos, que lembraria uma rede de universalismos universais”. (WALLERSTEIN, 2007, p. 124). Dessa forma, chegar-se-ia, a partir da análise intelectual do mundo, a uma aceitação do diferente e da sua possibilidade de criar seu próprio sistema de visão e ordenação do mundo, de acordo com suas próprias vontades e necessidades.

Diante dessa realidade interativa e da existência de variados pontos de estresse que se multiplicam ocorrem impactos cumulativos que levam ao fenômeno chamado pelas ciências sociais de ‘sobrecarga’, no qual as instituições e as capacidades de cooperação em uma sociedade não conseguem lidar com os estresses que são experienciados. Segundo Thomas Homer-Dixon “uma sociedade sobrecarregada com tensões, quebra. Se uma sociedade está sobrecarregada depende não só da natureza das tensões que se depara, mas também se pode controlar ou adaptar-se a elas. As sociedades variam muito em sua capacidade de lidar com o estresse”. (HOMER-DIXON, 2006, p.40, tradução nossa).[13]

Os principais fatores de estresse e tensão da sociedade internacional, na atualidade, são, segundo Thomas Homer-Dixon o crescimento da população, a falta de energia, os danos ambientais, a mudança de clima e a desigualdade econômica.

[13] “A society overloaded with stresses breaks down. Whether a society is overloaded depends not only on the nature of the stresses it encounters but also on whether it can manage or adapt to them. Societies vary a lot in their ability to cope with stresses”. (HOMER-DIXON, 2006, p.82).

(HOMER-DIXON, 2006, p.41). O relatório intitulado "Riscos Globais 2014", elaborado no Fórum Econômico Mundial, assinala que os pontos de tensão internacional são ainda maiores e conforme se constata do gráfico, apresentado no próprio relatório, há uma rede interativa de pontos de estresse que determinam uma sociedade internacional cada vez mais complexa e cibernética. (FÓRUM ECONÔMICO MUNDIAL, 2014, p.21).

ILUSTRAÇÃO 1 - Gráfico: Relatório de riscos globais 2014

Fonte: Fórum Econômico Mundial, 2014, tradução nossa.

Um relógio, por ser uma máquina, pode ser desmontando e montado novamente, pois facilmente se visualiza suas peças individualizadas, suas funções e como cada parte do relógio encaixa uma com a outra, sendo possível colocá-las novamente juntas para que o relógio funcione. A analogia mecanicista do relógio não funciona para as relações internacionais, pois não se pode ter um pensamento reducionista das relações humanas.

Comumente, os cientistas fazem distinções entre máquinas simples, tais como o relógio, e máquinas complexas como o sistema internacional, mas essa analogia também é equivocada, pois não há como descrever sistemas complexos como se máquinas previsíveis fossem. As máquinas possuem uma proporcionalidade de causa e efeito, pequenas causas geram pequenos efeitos e grandes causas, grandes efeitos, é essa a premissa do pensamento linear. Há um comportamento normal e linear nas máquinas e, por isso, estas podem ser controladas, pois são previsíveis. Tudo é compreensível, inteligível e administrável. Os sistemas complexos destroem essa visão de mundo, pois são mais do que a soma de suas partes, não possuem uma proporcionalidade entre causa e efeito, ou seja, possuem um comportamento não linear, não são previsíveis e, portanto não podem ser facilmente controlados, administrados e interpretados. Esse é o grande desafio das relações internacionais na análise da sociedade internacional.

É necessário deixar de delinear as relações internacionais como compostas por máquinas lineares, no caso, Estados nacionais esboçados e explicados de forma simplista, para perceber que a sociedade internacional é formada de sistemas complexos que vivem uma dinâmica de rede interativa e com inúmeros fatores que aumentam as tensões entre os atores internacionais. Além disso, não é possível esquecer que esse sistema internacional é aberto e circular, sendo que novos fatores de tensão e novas interações surgem a cada momento, ao mesmo tempo e sem qualquer linearidade. A ordem dessas relações internacionais acaba ocorrendo através de uma organização autopoiética vinculada a todos os fatores que possam de forma objetiva e subjetiva mudar os rumos das conexões. Há, na realidade, uma profunda mudança ontológica, pois se deve perceber o mundo e sua realidade básica de uma forma completamente diferente do até estão estudado.

Na sociedade internacional complexa há uma combinação de interações, feedbacks e efeitos multiplicadores de tensões que viabilizam uma total desproporção e imprevisibilidade para as relações internacionais. O equilíbrio desse sistema passa a ser, portanto, múltiplos equilíbrios, assim como se percebe nas relações internacionais que possuem pontos de estresse, mas também pontos de equilíbrio que viabilizam as interações.

Uma das grandes causas que tem levado ao aumento da complexidade das relações internacionais é o avanço na tecnologia da informação, pois o desenvolvimento tecnológico e a melhora de desempenho na comunicação entre as

unidades do sistema, organizações, povos e tecnologias, aumentam o número de interações e, consequentemente, a complexidade da sociedade internacional. Além disso, a velocidade dessas conexões é cada vez maior, pois há uma expansão dos atores partícipes das relações internacionais e as conexões em rede são cada vez mais densas, com uma grande movimentação de energia, matéria e informações entre eles.

O grande desafio é compreender como os estudos da sociedade internacional e do Direito Internacional podem se beneficiar efetivamente da teoria da complexidade. Em 1971, os cientistas políticos Robert O. Keohane (1941–) da Universidade de Duke, e Joseph S. Nye Jr (1937–) da Universidade de Harvard, publicaram o livro "Organização Internacional"[14]. Nessa obra questionam o conhecimento linear tradicional das relações internacionais e, em especial, o papel de sujeitos não estatais na política mundial, as ações não militares e a instabilidade econômica internacional. Após identificarem uma série de limitações do pensamento analítico centrado apenas nas relações interestatais, os autores passaram a buscar uma alternativa passível de aplicação. Em 1977, Keohane e Joseph Nye escreveram, então, o livro "Poder e Interdependência"[15] no qual abordam quais são as características principais de um mundo em que a interdependência é tão extensiva. (KEOHANE; NYE JR., 1977, p.3).

Na obra "Poder e Interdependência" o primeiro questionamento feito é sobre "quais são as características da política mundial em condições de extensa interdependência". Essa questão é respondida por meio de uma comparação da visão de mundo do Realismo Político com o paradigma da interdependência estatal. A interdependência refere-se a situações em que os Estados ou atores são determinados por eventos externos em uma relação de reciprocidade com outros Estados ou atores, ao limitar em conjunto a sua autonomia e predeterminação. Esse novo paradigma é criado por meio da expansão das operações internacionais, que ganham uma dinâmica complexa. (KEOHANE; NYE JR., 1977, p.3).

A visão tradicional de poder, definida pela visão realista muitas vezes como poder militar, é muito limitada nesse contexto. O poder pode ser coerção militar ou

[14] Nome original do livro editado em inglês e traduzido para o português pela autora: "International Organization" de 1971.

[15] Nome original do livro editado em inglês e traduzido para o português pela autora: "Power and Interdependence" de 1977.

pode ser a capacidade para controlar os resultados - o que está relacionado com a interdependência assimétrica, em que os atores menos dependentes em uma relação de interdependência podem usar sua posição para influenciar os outros. (KEOHANE; NYE JR., 1977, p.13-14). Na perspectiva sistêmica o poder passa a ser a capacidade de estabelecer interações complexas no sistema internacional.

Outro ponto importante explorado é o das dimensões do papel do poder na interdependência. Os autores fazem uma distinção entre a sensibilidade e a vulnerabilidade do poder, sendo que a sensibilidade refere-se às mudanças sensíveis em um Estado que terão a capacidade de produzir impactos em outros Estados. Basicamente, a velocidade e a magnitude com que uma mudança ocorre em um Estado se faz sentir na sociedade internacional, dentro de um quadro político. "Interdependência sensível é criada pelas interações dentro de um quadro de políticas". (KEOHANE; NYE JR., 1977, p.13-14, tradução nossa).[16]

A vulnerabilidade trata da capacidades dos entes políticos adaptarem-se a mudanças que possam ocorrer no cenário internacional. A interdependência vulnerável, que permite a adaptação a mudanças, é mais importante no fornecimento de recursos de poder para os atores internacionais, pois com essa capacidade adaptativa os atores sofrem menos com os efeitos de sensibilidade interativa. A vulnerabilidade pode assumir uma estratégica dimensão, pois Estados menos vulneráveis e mais adaptados podem explorar a sensibilidade dos outros atores internacionais, em uma busca de mais poder.

> A vulnerabilidade pode ser definida como a capacidade de um ator de sofrer os custos impostos por eventos externos, mesmo depois de as políticas serem alteradas. (...) A vulnerável dependência pode ser medida apenas pela opulência de fazer ajustes eficazes para um ambiente alterado ao longo de um período de tempo. (KEOHANE; NYE JR., 1977, p.15-16, tradução nossa).[17]

O segundo questionamento feito por Keohane e Nye foi o de como e por que os regimes internacionais são modificados. Relações interdependentes, por vezes, ocorrem dentro de redes de regras, normas e procedimentos para regular o comportamento e controlar os efeitos de mudanças de regimes. Embora a lei e as

[16] “Sensitivity interdependence is created by interactions within a framework of policies”. (KEOHANE; NYE JR., 1977, p.13).

[17] “Vulnerability can be defined as an actor's liability to suffer costs imposed by external events even after policies have been altered.(...)Vulnerability dependence can be measured only by the costliness of making effective adjustments to a changed environment over a period of time”. (KEOHANE; NYE JR., 1977, p.13).

organizações internacionais possuam uma constante desaprovação de sua força e efetividade no cenário internacional, em áreas específicas, as regulações (formais ou informais) tem produzido grande influência. A organização da sociedade internacional, por meio da normatividade do direito, estabelece fatores regulatórios imediatos entre a estrutura de poder do sistema internacional e à negociação político-econômica, dentro do sistema. (KEOHANE; NYE JR., 1977, p.36). Entretanto, não se pode esquecer que a regulação e o próprio Direito Internacional é também produto do sistema complexo. Diante dessa interferência do sistema na produção normativa, pelo sistema ser aberto, mudanças graduais ou bruscas de regimes ocorrem constantemente.

> Regimes internacionais são fatores intermediários entre a estrutura de poder de um sistema internacional e a negociação política e econômica que ocorre dentro dele. A estrutura do sistema (...) afeta profundamente a natureza do regime. O regime, por sua vez, afeta e, em certa medida governa a barganha política e a tomada de decisão diária que ocorre dentro do sistema. (KEOHANE;. NYE JR ., 1977, p.36, tradução nossa).[18]

Outra tentativa de caracterizar o sistema internacional, em termos complexos, foi esboçada pelo cientista político James N. Rosenau (1924-2011), no livro "Turbulência na Política Mundial: uma teoria da mudança e continuidade"[19] de 1990, que inicialmente se utiliza do conceito de complexidade, demonstrando a necessidade de uma diversidade teórica e metodológica para compreender o sistema da sociedade internacional. (ROSENAU, 1990, p. 10).

Rosenau elabora uma visão geral das questões normativas confrontando-as com o ponto de vista do final do século XX sobre as relações político-sociais. Afirma a história dos séculos XIX e XX como relato de interações em torno de cada vez mais abrangentes entidades políticas, a fim de preservar os valores individuais no contexto das necessidades coletivas. (ROSENAU, 1990, p. 10). No livro "Ao Longo da Fronteira Doméstica: explorando governança em um mundo turbulento"[20], de 1997, James Rosenau aprofunda sua reflexão, ao afirmar que a complexa

---

[18] "International regimes are intermediate factors between the power structure of an international system and the political and economic bargaining that takes place within it. The structure of the system...profoundly affects the nature of the regime. The regime, in turn, affects and to some extent governs the political bargaining and daily decision-making that occurs within the system". (KEOHANE; NYE JR., 1977, p.36).

[19] Nome original do livro editado em inglês e traduzido para o português pela autora: "Turbulence in World Politics: a theory of change and continuity" de 1990.

[20] Nome original do livro editado em inglês e traduzido para o português pela autora: "Along the Domestic-Foreign Frontier: exploring governance in a turbulent world" de 1997.

fragmentação da sociedade internacional faz com que partes singulares, de pessoas e povos que 'optam' por um subgrupo individual fechado, 'adaptaptando-se' a valores e exigências específicos, viabiliza crescente ineficácia do sistema como mantenedor de equilíbrio. Pode-se inclusive causar um colapso, ou seja, um rompimento dos sistemas nacionais e internacionais existentes. (ROSENAU, 1997, p. 19). O grande equívoco de Rosenau foi não ter mencionado os conceitos de 'feedback', 'não linearidade' e de 'emergência'; fundamentais para a discussão do paradigma da complexidade.

Robert Jervis (1940–), em seu livro 'Efeitos do sistema: complexidade na vida política e social'[21], publicado em 1997, na Universidade de Princeton, Estados Unidos, conclui que os próprios fundamentos das teorias das ciências sociais não correspondem a real expressão da realidade complexa. A partir de fundamentos da teoria da complexidade, afirma que a sociedade internacional organiza-se por meio de uma estrutura sistêmica de redes, onde tudo está interligado e onde as consequências das atividades dos atores internacionais são inevitáveis e imprevisíveis, pois o efeito total de comportamento não é igual à soma das ações individuais dos interlocutores. Ele destaca a interconexão do mundo político e como uma série de ações em rede podem levar à guerra, tendo como exemplo a Guerra Fria. (JERVIS, 1997, p.33).

Segundo Jervis, as ramificações da criação de uma compreensão rigorosa da política são catastróficas, em especial quando se utilizam de limitados critérios, tidos como científicos, para a análise internacional. Jervis passa a examinar o feedback na sociedade internacional, a negociação em diferentes tipos de relacionamentos, e os efeitos de polarização de alinhamentos para começar a construir uma base complexa para sua análise do cenário internacional. (JERVIS, 1997, p.36).

Immanuel Wallerstein também adota em seu livro "Análise Sistemas-Mundo: uma Introdução"[22], publicado em 2007, a noção sistêmica para a análise da sociedade internacional. O autor afirma que a análise de mundo, baseada apenas em fenômenos isolados tende a fazer com que os teóricos cheguem a conclusões que se sustentam somente por um pequeno período de tempo, pois falham em

[21] Nome original do livro editado em inglês e traduzido para o português pela autora: "System Effects: Complexity in Political and Social Life", de 1997.

[22] Nome original do livro editado em inglês e traduzido para o português pela autora: "World-Systems Analysis: an introduction", de 2007.

buscar uma percepção de mundo que possa expressar todo o cenário sistêmico internacional. (WALLERSTEIN, 2007, p. 10).

Assim, o homem, constantemente, vê-se surpreendido com a sua incapacidade de estabelecer previsões para o futuro de suas relações sociais. Parte do problema situa-se na tendência humana de fragmentar e especializar o conhecimento em 'caixas' fechadas que separam e nomeiam diferentes ramos como a política, a economia, a cultura, o direito. Falta perceber que essa divisão, sem conexões, consiste numa construção da própria imaginação humana, não condizente com a realidade que é holística. (WALLERSTEIN, 2007, p. 11).

A fragmentação do conhecimento, que as universidades concretizam por meio da criação de diferentes disciplinas ('caixas') não é uma ferramenta didática de facilitação da cognição, mas um obstáculo para a compreensão da realidade sistêmica. Além disso, não se pode ignorar que o sistema mundo constitui-se por inúmeras instituições que não necessariamente são somente as previstas pelo Direito Internacional e pelas relações internacionais. (WALLERSTEIN, 2007, p. 11).

> Evidentemente, a análise de sistemas-mundo é realmente uma grande narrativa. Analistas do sistemas-mundo argumentam que todas as formas de atividade de conhecimento, necessariamente, envolvem grande narrativa, grande propósito narrativo que algumas refletem melhor a realidade do que outras. Na sua insistência na história absoluta e unidisciplinar, os analistas de sistemas-mundo se recusam a substituir a chamada base cultural para uma base económica. Pelo contrário, como foi dito, eles procuram abolir as fronteiras entre econômico, político e sociocultural modos de análise. Acima de tudo, os analistas de sistemas-mundo não tem a intenção de jogar o bebé fora com a água do banho. Ser contra o cientificismo não é ser contra a ciência. Ser contra o conceito de estruturas atemporais não significa que as estruturas (tempo-limite) não existem. Acreditar que a atual organização das disciplinas é um obstáculo a ser superado não significa que há não existe a possibilidade de coletivamente reunir conhecimento (apesar de provisório ou heurístico). Ser contra o particularismo disfarçado de universalismo não significa que todos os pontos de vista são igualmente válidos e que a busca por um universalismo pluralista é fútil. (WALLERSTEIN, 2007, p. 21, tradução nossa).[23]

[23] "Of course, world-systems analysis is indeed a grand narrative. World-systems analysts argue that all forms of knowledge activity necessarily involve grand narratives, but that some grand narratives reflect reality more closely than others. In their insistence on total history and unidisciplinarity, world-systems analysts refuse to substitute a so-called cultural base for an economic base. Rather, as we have said, they seek to abolish the lines between economic, political, and sociocultural modes of analysis. Above all, world-systems analysts do not wish to throw the baby out with the bath. To be against scientism is not to be against science. To be against the concept of timeless structures does not mean that (time-bound) structures do not exist. To feel that the current organization of the disciplines is an obstacle to overcome does not mean that there does not exist collectively arrived-at knowledge (however provisional or heuristic). To be against particularism disguised as universalism does not mean that all views are equally valid and that the search for a pluralistic universalism is futile". (WALLERSTEIN, 2007, p. 21).

O pensamento liberal, adotado no âmbito das relações internacionais, tem sido a grande agenda de política externa do Ocidente desde a Guerra Fria, e no Ocidente, há muito tempo ocupou o degrau mais alto de um sistema teórico hierárquico. Hilton Root (1951–), especialista em economia política internacional e desenvolvimento da Escola de Políticas Públicas da Universidade George Mason, no livro “Dinâmica entre as nações: a evolução de legitimidade e desenvolvimento em estados modernos”[24] argumenta que as relações internacionais, assim como outros ecossistemas complexos, existem em uma paisagem em constante mudança. As estruturas hierárquicas fechadas abrem espaço para uma análise de mundo por meio do paradigma holístico, composto por sistemas de interdependência em rede. Assim, os formuladores de políticas precisam de uma nova forma de compreender o processo de mudança. Root sugere que a ciência dos sistemas complexos oferece um quadro analítico para explicar as imprevistas falhas de desenvolvimento, as tendências de governança e mudanças na economia política global de hoje. (ROOT, 2013, p. 16).

> O sistema de relações internacionais, como a maioria dos ecossistemas complexos, tais como o sistema nervoso ou uma floresta tropical, estão se rendendo às suas regras de complexidade. Em sistemas complexos, um administrador central raramente orienta os comportamentos coletivos que caracterizam os processos de desenvolvimento. O sistema tem um comportamento coletivo por si mesmo onde o todo depende das partes. Ao invés de uma convergência para um modelo dominante, ou "ótimo global", são as dinâmicas interativas são coevolutivas; suas interações resultam em intercâmbio recíproco e mudança evolutiva. (ROOT, 2013, p.5, tradução nossa).[25]

A rede sistemas de raízes, que compõem os Estados modernos e maiores, constituem-se em paisagens interdependentes que partilham. Usando análise de sistemas sobre o ‘todo’, a mudança institucional e desenvolvimento econômico são entendidos como complexidades de auto-organização, visão alternativa de superação linear do cenário internacional. A partir dessa perspectiva, a

[24] Nome original do livro editado em inglês e traduzido para o português pela autora: “Dynamics among Nations: The Evolution of Legitimacy and Development in Modern States”, de 2013.

[25] “The system of international relations, like most complex ecosystems, such as the nervous system or a rain forest, is yielding to its rules of complexity. In complex systems, a central administrator rarely guides the collective behaviors that characterize development processes. The system itself has a collective behavior that depends on all its parts. Rather than convergence toward a dominant model, or “global optimum,” the interactive dynamics are coevolutionary; their interactions result in reciprocal and evolving change”. (ROOT, 2013, p. 5).

complexidade argumenta a impossibilidade de processos de mudança histórica com precisão algorítmica cartesiana. (ROOT, 2013, p.21).

> Quando as interações de um Estado deixarem de ser de base local regional ou nacional com base, seus comportamentos mudam através da rede e do sistema maior. Assim uma teoria geral do sistema não pode ser deduzida a partir das propriedades de suas partes constituinte, assim como o universo não pode ser reconstruído a partir das leis fundamentais da física. (ROOT, 2013, p. 31, tradução nossa).[26]

Mas quais são as vantagens de se aceitar a incerteza nas relações da sociedade internacional? Na realidade, há vantagens na adoção da visão de mundo complexo, pois ela viabiliza a explicação das relações entre os atores internacionais em uma visão não linear, como há muito tem se observado. As teorias cartesianas são importantes para a análise de certos aspectos dessa sociedade, mas falham na explicação da imprevisibilidade do cenário internacional. Ao mesmo tempo, a teoria da complexidade é uma fonte de inovação, por meio da viabilidade de novas combinações interativas que não eram possíveis antes do estabelecimento das relações de rede. A complexidade é também viabilizadora do desenvolvimento de uma maior capacidade de adaptação dos atores internacionais a novas condições do cenário internacional; percebe-se, portanto, que os sistemas mais bem adaptados tendem a ser os mais complexos sistemas, pois possuem diversidade e distribuição de obrigações na solução de problemas.

Não obstante, a adoção do pensamento complexo na análise da sociedade internacional também pode ser uma opção perigosa e até mesmo negativa. Aceitar que a sociedade internacional forma-se de sistemas complexos é também admitir a impossibilidade das relações internacionais e do próprio Direito Internacional de possuírem a capacidade de obter paradigmas lineares de certeza. É aceitar que, nas relações internacionais, não há como se obter uma explicação plausível para todos os acontecimentos, entregando-se à teoria do caos, à certeza da incerteza. A complexidade também pode causar eventos extremos e revertérios nos sistemas, chegando inclusive a uma sobrecarga, especialmente quando se tem inúmeros pontos de tensão entre os sistemas. O último e grande problema da complexidade é que esta pode causar também a proliferação de efeitos brutais, ou seja, quanto

[26] “When a state’s interactions shift from being locally based to being regionally or nationally based, its behaviors change across the network and the greater system. Thus a general theory of the system cannot be deduced from the properties of its constituent parts, just as the universe cannot be reconstructed from the fundamental laws of physics”. (ROOT, 2013, p.31).

maior o número de interações, maior a possibilidade de um fator negativo se proliferar nas redes.

Muda-se a perspectiva e passa-se a enxergar o cenário internacional não como um cenário de riscos, mas como um cenário de incertezas. Em um mundo de riscos é possível analisar as potenciais causas e efeitos das ações dos atores internacionais para se tomar decisões, mas no mundo complexo não há previsibilidade, pois não há informação o suficiente que possa estimar os caminhos e consequências das relações interativas. Esse novo paradigma de mundo é diferente e desafiador na análise das relações internacionais e do Direito Internacional. Muitos acadêmicos inclusive não vão aceitar cogitar a possibilidade de não serem os detentores do saber, pois o poder muitas vezes emana da possibilidade de poucos se nomearem como detentores do conhecimento para auxiliar na tomada de decisões e até na imposição de determinadas ideologias à sociedade complexa.

3.1 A complexidade do Direito Internacional

Em 1625, Hugo Grotius, no livro “O Direito da Guerra e da Paz” professava a importância do direito para a sociedade internacional ao afirmar: “Nenhuma associação de homens pode ser mantida sem lei (...) Certamente também que a associação que une a raça humana, ou une muitas nações, tem a necessidade da lei”. (GROTIUS, 2004, p.107). Inicialmente saber da necessidade da existência de uma ordem normativa não quer dizer que seja simples estabelecer um sistema de leis, em especial no âmbito internacional, para atender às necessidades da sociedade internacional complexa. O grande desafio no Direito Internacional é compreender a sociedade que regula e entender que esse direito não parte da linearidade, uniformidade e verticalidade que estão presentes no direito interno, ainda muito mergulhado no pensamento cartesiano linear.

A sociedade internacional, muitas vezes comparada a outras formas de organizações sociais e o próprio Direito Internacional, também confronta com outros ramos do direito e inclusive se confunde com o positivismo das leis dos Estados nacionais, o que é um equívoco. Em uma primeira análise, o Direito Internacional parece não ter uma real efetividade legislativa para a organização das relações na

sociedade internacional, além de sofrer com a não existência de um mecanismo centralizador de poder que possa impor normas e viabilizar a sua aplicabilidade por meio da coercibilidade, em função do respeito necessário à liberdade soberana dos Estados. Apesar das diversas ambiguidades teóricas, que já apontam para uma relação de uma sociedade internacional complexa e em rede, o Direito Internacional uniformizador, assim como o pensamento do universalismo das leis estatais, muitas vezes não leva em consideração o respeito à vontade daquele que se demonstra mais fraco diante dos outros. (JANIS; NOYES, 2001, p.3).

É uma tendência humana pensar que todos os sistemas legais devem ter como modelo o Estado para se preestabelecerem, entretanto, se o sistema é distinto não há sentido em manter o mesmo padrão de organização para uma sociedade que não se organiza da mesma forma que os Estados. O padrão de produção normativa e organização, apresentado pelo Direito Internacional é completamente sofisticado, pois não se pode contar com instituições centralizadas responsáveis pela produção legislativa, uma vez que essa universalização não é possível em uma sociedade internacional complexa. (CASSESE, 2005, p.3).

A definição de Direito Internacional, mais aceita pelos pensadores contemporâneos, tem sido voltada para o objeto dessa disciplina, ou seja, para a organização e regulação das relações da sociedade internacional, composta pelos chamados sujeitos de Direito Internacional. (DINH; DAILLIER; PELLET, 2003, p.37). Como qualquer ramo do direito, o Direito Internacional é um produto de seu ambiente social e reflete as características da sociedade na qual opera que nesse caso é extremamente complexa. A partir desse pensamento as relações internacionais e o próprio Direito Internacional trabalham para compreender o funcionamento da sociedade internacional, seus padrões de comportamento e as mudanças de regulações, ao longo da história a fim de se estabelecer normas reguladoras dessa sociedade que está em constante movimentação. (SHAW, 2010, p.36).

O Direito Internacional ainda é trabalhado, por muitos doutrinadores, em dimensão imaginária, sonhada, do ‘dever ser’ que por meio do pensamento positivista linear científico tende a regular as relações olvidando-se da real complexidade da sociedade regulada. O Direito Internacional é, ainda hoje, um direito que objetiva a regulação das relações entre Estados, não indivíduos, pois eles são os principais atores das relações internacionais. (CASSESE, 2005, p.4).

Além disso, não há uma autoridade centralizadora, pois com o objetivo de se viabilizar uma relação entre os Estados sem se desrespeitar a soberania que lhes é peculiar o poder é fragmentado e disperso, sendo o sistema legal horizontal e não vertical. Isso significa que a produção normativa é realizada e aplicada pelos próprios sujeitos que se submeterão a ela, pelo princípio do *pacta sunt servanda*. (CASSESE, 2005, p.5).

> Por outro lado, na comunidade internacional, nenhum Estado ou grupo de Estados tem conseguido manter o poder duradouro de impor sua vontade sobre toda a comunidade mundial. O poder é fragmentado e disperso. Na verdade, alianças políticas e militares têm sido ocasionalmente articuladas com uma forte convergência de interesses entre dois ou mais membros da comunidade. No entanto, estes não tem se endurecido em uma estrutura de poder permanente. As relações entre os Estados que compõem a comunidade internacional permanecem em grande parte horizontais. Nenhuma estrutura vertical tem se cristalizou ainda, como é, em regra, no âmbito dos sistemas nacionais dos Estados. (CASSESE, 2005, p.5, tradução nossa).[27]

Antonio Casesse (1937–2011) afirma, ainda, que existe uma responsabilidade coletiva da sociedade internacional quando há a violação do Direito Internacional. Assim, como o sistema internacional estabelece que o grupo desenvolve um papel maior que o indivíduo, a responsabilidade por violações de Direito Internacional realizadas por um indivíduo é respondida também por seu Estado. Além disso, no âmbito comunitário, se os Estados resolveram se representar em conjunto, todos respondem pela violação realizada pelo representante do grupo. Essa regra, muito distinta do direito interno, depende de se analisar o real comprometimento do Estado de participar de um grupo de forma efetiva. (CASSESE, 2005, p.7). Exemplo está no artigo 2º do Tratado de Lisboa que afirma a responsabilidade coletiva de todos os Estados membros da União Europeia ao determinar sua competência para gerir a segurança internacional dos Estados.

> Art. 2º A fim de alcançar os objetivos referidos no artigo 1º, os Estados-Membros que participem na cooperação estruturada permanente comprometem-se a:
> a) Cooperar, desde a entrada em vigor do Tratado de Lisboa, no sentido de

[27] By contrast, in the international community no State or group of States has managed to hold the lasting power required to impose its will on the whole world community. Power is fragmented and dispersed. True, political and military alliances have occasionally been set up or a strong convergence of interests between two or more members of the community has evolved. However, these have not hardened into a permanent power structure. The relations between the States comprising the international community remain largely horizontal. No vertical structure has a yet crystallized, as is instead the rule within the domestic systems of States. (CASSESE, 2005, p.5).

> alcançar objetivos acordados relativamente ao nível das despesas de investimento em matéria de equipamentos de defesa, e a rever regularmente esses objetivos, em função do ambiente de segurança e das responsabilidades internacionais da União. (UNIÃO EUROPEIA, 2007).

Outra característica do Direito Internacional vem da adoção do dualismo legislativo. A maioria dos Estados, para efetivamente aplicar os tratados que se comprometeram seguir no âmbito internacional, precisam recepcioná-los no âmbito doméstico, como é o caso do Brasil. A soberania dos Estados permite determinar até qual extensão as normas internacionais serão aplicadas, com que hierarquia serão recepcionadas, mesmo que o tratado tenha sido ratificado no âmbito internacional. (CASSESE, 2005, p.8).

O grande desafio de se estabelecer um Direito Internacional efetivamente viabilizador de uma ordenação universal é a própria heterogeneidade e, consequentemente complexidade, da sociedade internacional. Além disso, há a dificuldade de se encontrar entre os sujeitos de Direito Internacional, em especial entre os Estados nacionais, uma possibilidade de união baseada em uma identidade de povos em prol de um ordenamento internacional comum, que possa beneficiar e viabilizar a segurança jurídica de uma convivência pacífica entre eles.

A sociedade internacional, por estabelecer uma constante interação entre sujeitos tão distintos, seja do ponto de vista cultural, étnico, religioso, linguístico e até mesmo jurídico, se estabelece pautada na necessidade desses sujeitos de conviverem para viabilizarem intercâmbios que lhes sejam favoráveis, sempre de acordo com uma dinâmica de poder vinculada ao interesse e não à afinidade ou até mesmo à identidade entre diferentes povos. É por esse motivo que muitos doutrinadores do Direito Internacional inclusive criticam a utilização da expressão ‘comunidade internacional’, pois uma comunidade é baseada em elementos subjetivos que fazem com que seus componentes encontrem o que há de ‘comum’ entre eles e construam uma identidade grupal. (DINH; DAILLIER; PELLET, 2003, p.40-41).

A complexidade das relações internacionais e a heterogeneidade dos sujeitos de Direito Internacional impedem a efetiva construção de uma identidade, uma vez que o interesse passa a ser o grande combustível que viabiliza a determinação de quem são os Estados aliados ou não nesse contexto competitivo. O que se percebe é que grande parte das chamadas identidades entre diferentes povos, na realidade, não partem dessa vinculação de encontro de fatores comuns entre eles, mas de

uma atuação de um grupo, que se utilizando da força, acaba por impor a sua cultura a outro povo e acaba chamando essa violência de identidade.

O grande desafio do Direito Internacional e da própria análise da sociedade internacional tem sido trabalhar as relações internacionais como complexas e impossíveis de serem regulamentadas e controladas por normas jurídicas lineares e universais, que em grande parte acabam por reforçar as diferenças entre os atores internacionais. Ao analisar a história percebe-se que a tendência de se universalizar muitas vezes viabiliza a criação e aplicação de normas que levarão à manutenção daquelas que são vistas equivocadamente como civilizações superiores no controle do pensamento, da aplicação das normas e até mesmo do poder no âmbito internacional.

O sistema internacional é um sistema exemplar de complexidade, pois em regra objetiva a regulação das relações de interatividade entre os sujeitos de Direito Internacional, ou seja, entre os Estados, organizações internacionais, coletividades não estatais (insurgentes, beligerantes) e o ser humano, como destinatário de direitos, em especial de direitos humanos. (SHAW, 2010, p.147). Além disso, a complexidade das relações se agrava pela grande diversidade cultural, econômica, linguística, histórica, étnica e religiosa existente entre esses sujeitos.

Outro problema não muito discutido pelos teóricos do Direito Internacional é o da própria diversidade presente no âmbito nacional dos Estados. A diversidade no Direito Internacional, expressa-se pela possibilidade de todos participarem do cenário internacional, mediante o alargamento do conceito de ator internacional passível de agir e possuir direitos, tendência admitida em algumas correntes voltadas para a proteção dos direitos humanos, no próprio Direito Internacional.

Além do aumento de atores internacionais, há uma aceitação de se discutir uma gama maior de assuntos sensíveis à sociedade e de se estabelecer interações com instrumentos variados, não somente com os previstos pelo Direito Internacional clássico. Diversidade no Direito Internacional, portanto, primeiro consiste em aceitar a diversidade de atores internacionais e, em consequência, viabilizar a discussão de um número maior de assuntos, através de instrumentos diversos, pois não só o Estado nacional deve ser ouvido como sujeito legitimado a se manifestar. (NOCOLAÏDIS; TONG, 2014, p.1352).

Não há sistema mais uniformizador do que o sistema do Estado Moderno, estabelecedor de normas gerais uniformes a todos os indivíduos que nomeia de

povo. Há uma grande diversidade dentro dos Estados Nacionais, muitas vezes ignorada pela noção de Estado Moderno uniforme e linear, instituída pelo direito. Na realidade, há uma diversidade de relações que se estabelecem no cenário internacional por meio de interações dos atores internacionais em rede e, concomitantemente, ocorrem um turbilhão de outras interações complexas dentro de cada sujeito, no âmbito nacional. Essas interações e conflitos internos de ideologias, identidades, interesses, etnias, culturas, religiões e línguas também trazem grande repercussão e complexidade para as relações internacionais.

ILUSTRAÇÃO 2 - Complexidade das Relações dos sujeitos de Direito Internacional

Fonte: Elaborado pela autora.

O fenômeno da complexidade do Direito Internacional acompanha a complexidade e as relações em rede da própria sociedade internacional, que regula. A noção de complexidade do Direito Internacional tem obtido cada vez mais adeptos devido à dificuldade de um direito hierárquico, linear e piramidal, proposto por Kelsen, conseguir regular as relações complexas, interativas e em rede dos atores internacionais. Assim, a criação de um direito uniforme e linear, no âmbito interno dos Estados, não tem atendido aos interesses dos povos, formados por uma

diversidade grande de indivíduos, o Direito Internacional também não consegue atingir seu objetivo ignorando essa diversidade.

O relato de existência de relações complexas em rede, dentre os atores das relações internacionais, se agrava pelos fenômenos do aumento de atores não estatais influenciadores dessas relações, pela internacionalização do direito, pelo aumento de fontes de Direito Internacional, pela diversidade político-econômica entre os atores internacionais e pelo esvanecimento do tempo e do espaço com as novas tecnologias.

3.1.1 A atuação de atores não estatais e a complexidade do Direito Internacional

O Direito Internacional objetiva regular as inúmeras interações complexas e adaptáveis que ocorrem em vários níveis na sociedade internacional e esse tem se demonstrado ser seu maior desafio. Não há nada de simples e linear na tentativa de organizar um emaranhado de relações interativas, em rede, que estabelecem conexões complexas. A complexidade começa a ser diagnosticada inicialmente pelo complexo de interações nacionais dos membros que compõe os Estados e posteriormente se chega a um nível de representação de interesses nacionais.

Sucessivamente, há um alto grau de relações interativas entre Estados nacionais, sempre imaginando que esses sujeitos são compostos por pessoas com interesses distintos e muitas vezes opostos.

Além das relações interestatais, busca-se regular também as relações travadas entre organizações internacionais, blocos econômicos e coletividades não estatais em prol de uma organização da sociedade internacional. Há uma interação constante, em rede, entre os sujeitos de Direito Internacional tradicionais (Estados, organizações Internacionais e coletividades não estatais) e entre os atores não estatais que passam a influenciar esse cenário, como as empresas transnacionais, as organizações não governamentais (ONG's) e os indivíduos com poder de negociação econômica internacional.

As relações internacionais ocorrem por meio de um sistema auto-organizável, adaptável e complexo que interconecta os tradicionais sujeitos de Direito Internacional com atores não estatais influenciadores dessas relações.

A definição de atores não estatais das relações internacionais ainda hoje demonstra-se bastante obscura, uma vez que não se chegou efetivamente a uma definição sobre quem seriam esses atores não estatais. A noção mais ampla sustenta que os atores não estatais são todos aqueles que não se caracterizam como um Estado nacional. Apesar das divergências doutrinárias, há uma grande dificuldade em definir o que vem a ser um ator não estatal das relações internacionais, pois os atores são muito diferentes entre si, mais uma vez, com uma marcante heterogeneidade. (VUKAS, 2010, p.11). Na atualidade, é muito ingênuo buscar estudar o Direito Internacional sem levar em consideração a influência que esses atores representam na sociedade internacional, entretanto, com o intuito de facilitar a compreensão, muitos doutrinadores tendem a especializar o Direito Internacional em um estudo apenas legalista de alguns atores internacionais que nomeia como sujeitos de Direito Internacional, não levando em consideração a sociedade complexa que regula.

Por outro lado, alguns doutrinadores buscam examinar a atuação de todos os atores não estatais na sociedade internacional, apesar de ser difícil definir com precisão quais são todos eles, diante da sua diversidade e constante surgimento de novos atores. Em regra, os especialistas de Direito Internacional limitam-se a estudar somente alguns sujeitos não estatais, levando em consideração os seus objetivos de representação de grupos no âmbito internacional, tais como os insurgentes e beligerantes, por exemplo. Entretanto, diante da rede de interações estabelecidas, os atores não estatais se mostram cada vez mais relevantes para o Direito Internacional na medida em que eles impactam cada vez mais nos valores e regras da sociedade internacional. O impacto desses atores pode ser positivo ou negativo, e isso se justifica pela capacidade crescente que entes não estatais têm de influenciar nesse cenário, seja por autorização legal chancelada pelo Direito Internacional, seja pela força da tecnologia que permite que qualquer indivíduo tenha o poder de ser ouvido e de fazer interações no âmbito internacional, independente de apoio do seu Estado.

Exemplo dessa questão está na Resolução nº.31 de 1996 do Conselho Econômico e Social (ECOSOC) da Organização das Nações Unidas (ONU) que regula o artigo 71[28] da Carta da ONU que autoriza a consulta a ONG's, atores não

[28] Artigo 71. O Conselho Econômico e Social poderá entrar nos entendimentos convenientes para a consulta com organizações não governamentais, encarregadas de questões que estiverem dentro

estatais, quando o assunto for de sua competência. (ONU, 1945). Esse é um caso em que a sociedade civil, independente da representação estatal, pode participar das interações no Direito Internacional. (CLAPHAM, 2009, p.212).

Além disso, não se pode ignorar que a ação estatal é essencial em alguns setores da sociedade internacional quando o ator não estatal é o próprio violador do Direito Internacional, como por exemplo, quando há a violação dos direitos humanos realizada por um ente não estatal. Não se pode ignorar a possibilidade dos atores não estatais terem direitos, mas também deveres de obedecer aos ditames estabelecidos pelo Direito Internacional, em especial quando se trata da proteção de direitos humanos. A não atribuição da legitimação de atuação desses atores, no cenário internacional, além de dificultar a possibilidade de se ouvir e legitimar a participação de todos os entes interativos da rede complexa internacional, leva à impunidade daqueles que atuam fora dos ditames traçados pelo Direito Internacional.

A complexidade das relações de Direito Internacional tem sido reconhecida por meio de uma maior relevância adquirida por atores não estatais, acentuando a pluralidade de interações estabelecidas na sociedade internacional. Os atores não estatais adquiriram uma importância mais significativa e têm impactado não só as relações internacionais, mas também o Direito Internacional, o que demonstra um equívoco na adoção de uma abordagem exclusivista estatal na análise complexa dessa sociedade.

A contemporaneidade caracteriza-se por profundas modificações nas relações internacionais promovidas pelo impacto do avanço tecnológico e da evolução da capacidade de análise da sociedade civil. Desde a Segunda Guerra Mundial, o mundo foi gradualmente introduzido na era pós-industrial, manifesta em uma grande turbulência política e de complexidade relacional, na qual padrões simultâneos de mudança e continuidade estão em funcionamento. Como o modelo tradicional, traçado pelos realistas, não possui mais a capacidade de expressar a complexidade da contemporaneidade, deve-se sair do pensamento de base estatal para se pensar em um Direito Internacional que aceita a interação também de atores não estatais nas relações em rede. (ROSENAU, 1990, p.244).

---

da sua própria competência. Tais entendimentos poderão ser feitos com organizações internacionais e, quando for o caso, com organizações nacionais, depois de efetuadas consultas com o Membro das Nações Unidas no caso. (ONU, 1945).

Uma maior interdependência do sistema internacional e um aumento na capacidade interativa dos atores faz com que a visão de mundo centrada nos Estados possa conviver e interagir com uma política multi-autônoma global, composta atores não soberanos. Esse mundo multicêntrico passa a ser cada vez mais uma certeza, pois os atores não estatais ganham mais capacidade de iniciar e sustentar suas ações no cenário internacional. Apesar de estarem até então juridicamente restritos à jurisdição dos Estados, os atores não estatais do mundo multicêntrico ganham capacidade para agir independente das restrições dos Estados e perseguir seus próprios objetivos. (ROSENAU, 1990, p.249).

Enquanto os dois mundos podem ser separados com uma maior clareza para a análise do que são relações nacionais e internacionais, percebe-se que na interatividade das relações não há uma distinção estanque entre eles. A sobreposição entre os dois mundos dos sujeitos estatais e dos atores não soberanos é inerente à estrutura do sistema como um todo, devido à crescente interdependência das políticas pós-industriais, e, mais particularmente, o aumento nas atividades transnacionais. O mundo centrado no Estado, por vezes, caracteriza-se por relações simplificadas, lineares, entre a combinação de vontades expressas por chefes de Estado. O mundo multicêntrico relata a relação complexa, em redes, sem a delimitação exata de sujeitos capazes de interagir e sem a possibilidade de se prever o futuro dessas relações. (ROSENAU, 1990, p 271-72.). Apesar de ser possível fazer a distinção entre atores soberanos e não soberanos eles coexistem interativamente na sociedade internacional e as relações entre eles se sobrepõem, não obstante manterem um grau de independência.

Os autores pluralistas têm dificuldade em traçar quais seriam os atores não soberanos participantes da sociedade internacional, em especial pelo fato de se modificarem a cada período de evolução das relações no sistema complexo aberto, que é o cenário internacional. Os principais atores não estatais vistos hoje como determinantes para as relações internacionais são as coletividades não estatais, tais como os beligerantes e os insurgentes, as ONG’s, representantes da sociedade civil, as grandes empresas transnacionais, grupos terroristas e indivíduos, dentre outros, que, de alguma forma, consigam causar impacto positivo ou negativo no cenário internacional.

3.1.2 A internacionalização do direito e o aumento da complexidade do Direito Internacional

Mireille Delmas-Marty (1941–), professora da Universidade de Paris, afirma em seu livro “Três Desafios para um Direito Mundial” que a internacionalização do Direito Internacional consiste em fenômeno que comprova a complexidade das relações jurídicas e a tendência do próprio direito e seus diferentes ramos é de relacionarem-se entre si, de forma interativa. O estudo do direito, sob a perspectiva da complexidade, deve ser visto de forma não compartimentada, ao viabilizar relação de pluralismo global interativo. O mais importante nesse novo paradigma das relações complexas é perceber como os diferentes ramos do direito interagem na regulação das relações sociais, independente da divisão entre direito nacional e internacional. (DELMAS-MARTY, 2003, p. 72).

O termo “internacionalização do direito” é usado para descrever um processo dinâmico interativo, que abre os sistemas jurídicos e ‘borra’ as fronteiras anteriormente delimitadas pela criação do conceito de Estado Moderno fechado somente em seu próprio território. Delmas-Marty afirma que a resposta para compreender a internacionalização do direito está em três palavras: diversidade, perplexidade e complexidade. (DELMAS-MARTY, 2014).

A diversidade está em toda parte, mas duas formas de diversidade são fundamentais para compreender a complexidade das relações: ‘a diversidade dos sistemas legais’ e a ‘diversidade dos atores globais’. A diversidade legal vê-se presente em diferentes níveis de organização, diferentes campos legais (nacional, regional e global) e diferentes velocidades de evolução. As relações entre todos esses fatores de organização legal não lineares, são complexos, interativos, sem continuidade e com lacunas. (DELMAS-MARTY, 2014).

O segundo aspecto da diversidade das relações internacionais envolve atores globais que atuam na sociedade. Nessa relação há atores estatais e não estatais (corporações transnacionais, atores civis como as organizações não governamentais e os peritos científicos). (DELMAS-MARTY, 2014).

A diversidade da organização legal global pode levar à fragmentação, além da pluralidade de atores internacionais poder criar um descontrole das políticas de divisão linear de poder.

Em face de tanta diversidade, o ser humano se vê sem saída com uma série cada vez maior de normas jurídicas, que criam novos desafios para a organização linear das relações globais. Para Delmas-Marty chega-se a um ponto de perplexidade e completa insegurança diante da pluralidade normativa. A não uniformidade normativa leva inicialmente a uma desordem, à arbitrariedade, tendo em vista a possibilidade de se aplicar mais de uma solução para o mesmo caso concreto. (DELMAS-MARTY, 2014).

Demonstra-se impossível perceber a solução do problema da diversidade e da perplexidade sem compreender o paradigma da complexidade. A solução para quebrar a insegurança, diante de tanta movimentação e questionamentos, exige a adoção da nova metodologia na análise das relações jurídicas, em especial do Direito Internacional.

É o que Delmas-Marty chama de buscar ‘organizar a pluralidade’, partindo-se da premissa de que a complexidade é um fato das relações humanas. A autora propõe a necessidade de uma revolução cultural, que introduza a complexidade para o mundo jurídico. A única forma de conseguir mudar essa metodologia seria imaginar novas técnicas para integrar os diferentes ordenamentos jurídicos, viabilizando suas interações, além disso, é necessário buscar novas diretrizes para o compartilhamento de regulamentação e responsabilidade legal. Deve-se buscar a interação ao invés da hierarquização das normas e se manter o foco mais no processo legislativo do que nas formas legais. (DELMAS-MARTY, 2014). Ou seja, uma possível solução de se viabilizar essa interação legislativa é por meio da internacionalização do direito.

3.1.3 Aumento das fontes de Direito Internacional na complexidade

A noção de complexidade vem da diversidade de atores que se relacionam em uma rede interativa e do aumento intensivo dessas relações, sem uma ordem linear. As tradicionais fontes de Direito Internacional (tratados, costumes, princípios gerais de direito, decisões judiciais e doutrina)[29], diante da nova realidade, devem

[29] Artigo 38. 1. A Corte, cuja função é decidir de acordo com o Direito Internacional as controvérsias que lhe forem submetidas, aplicará:

a) as convenções internacionais, quer gerais, quer especiais, que estabeleçam regras expressamente reconhecidas pelos Estados litigantes;

interagir com as novas fontes de Direito Internacional a fim de regular a complexa estrutura internacional.

A internacionalização do direito tem feito com que normas que até então eram nacionais sejam também objeto do Direito Internacional, além da existência de normas nacionais que na atualidade possuem efeito internacional. A integração econômica é um fator que faz com que haja uma dificuldade crescente em distinguir as normas de efeitos domésticos de normas internacionais, pois essas relações são cada vez mais internacionalizadas, com o objetivo de se romper barreiras entre Estados membros dos blocos econômicos.

O processo de multiplicação das fontes de Direito Internacional ocorre por motivos variados, podendo-se identificar quatro principais motivos para o aumento das normas internacionais. O primeiro motivo é a influência das leis não nacionais, uma vez que se percebe que os Estados tendem a adotar posturas similares em diversos assuntos, no âmbito doméstico, devido a uma influência não coercitiva exercida pelas ideologias defendidas no cenário internacional. Esse fenômeno é chamado, por Marcelo Dias Varella (1974–), de ‘intercruzamento normativo’, pois não há somente um enquadramento de condutas no âmbito nacional, mas uma criação de novas normas de Direito Internacional com base nesses fatores comuns. (VARELLA, 2013, p.96).

O principal motivo de existência desse ‘intercruzamento normativo’ situa-se na constante discussão de dificuldades comuns vividas pelos sujeitos de Direito Internacional, em especial nas reuniões promovidas por organizações internacionais. Existe um processo cada vez maior de uma retroalimentação normativa que incentiva os atores a pensarem de forma conjunta soluções para problemas semelhantes. Passa-se, então, a adotar políticas públicas nacionais que em muito se assemelham ao discutido e ratificado no âmbito internacional. Uma situação semelhante ocorre quando um Estado reproduz uma solução utilizada nacionalmente em outro Estado. Entretanto deve-se perceber que essa influenciação nem sempre reproduz uma real cooperação, mas sim uma prática de

---

b) o costume internacional, como prova de uma prática geral aceita como sendo o direito;

c) os princípios gerais de direito, reconhecidos pelas nações civilizadas;

d) sob ressalva da disposição do Artigo 59, as decisões judiciárias e a doutrina dos juristas mais qualificados das diferentes nações, como meio auxiliar para a determinação das regras de direito.

2. A presente disposição não prejudicará a faculdade da Corte de decidir uma questão *ex aequo et bono*, se as partes com isto concordarem. (ONU, 1945).

‘universalismo europeu’, como previamente discutido. Percebe-se que essa influência é assimétrica, uma vez que Europa e Estados Unidos influenciam muitos mais Estados do que são influenciados. (VARELLA, 2013, p.96).

O segundo motivo para o aumento de fontes de Direito Internacional se encontra nas políticas de integração entre Estados. Os processos de integração, que são sempre heterogêneos e dependem das interações realizadas entre os atores internacionais, podem ser realizados buscando uma união regional ou global. No âmbito regional, os sistemas jurídicos regionais, muitas vezes representados pelos sistemas estatais, estabelecem interações para a viabilização de coordenação de uma atuação conjunta e como consequência produzem novas fontes normativas, oriundas dos sistemas regionais complexos, como por exemplo, o MERCOSUL. Nas organizações internacionais gerais, que não restringem a participação regional de Estados, essas interações são realizadas em âmbito global, produzindo-se normas que atendam essas demandas. Exemplo de organização global é a própria ONU. (VARELLA, 2013, p.98).

O reconhecimento da existência de normas imperativas de Direito Internacional, que se aplicam a todos os Estados, é o terceiro motivo para se perceber um aumento de fontes de Direito Internacional na atual complexidade, pois não somente por meio da manifestação dos Estados surgem as normas. Essas normas imperativas a todos vão contra o sistema baseado no *pacta sunt servanda* internacional e ganharam o nome de *jus cogens*.[30]

O quarto e último fator para o aumento da quantidade de fontes normativas é político, pois trata da possibilidade de Estados, com poderio econômico e militar, influenciar outros Estados na adoção de normas que lhes sejam favoráveis. Essa imposição, geralmente, ocorre quando há uma relação de dependência ou pressão política para a adoção dessas normas. Exemplo, dado por Marcelo Dias Varella, está na edição de normas nacionais que possam atingir e punir fatos ocorridos fora do território tais como, por exemplo, no caso de Estados Unidos, França e Reino

[30] No Direito Internacional, o termo *jus cogens* (literalmente, "lei convincente" ou “lei impositiva”) refere-se às normas que comandam autoridade peremptória, substituindo conflitantes tratados e costumes. Normas de *jus cogens* são consideradas obrigatórias, não admitem rogação, e só podem ser modificadas por normas internacionais de autoridade equivalente. O surgimento das normas de *jus cogens* trouxe mudanças para o Direito Internacional, ao transformar a doutrina baseada no voluntarismo e na máxima do respeito indubitável à soberania dos Estados. Ao estabelecer limites legais sobre a atuação dos Estados, as normas de *jus cogens* desafiam a ortodoxia linear positivista que vê o Estado soberano como a única origem das obrigações legais internacionais. (CRIDDLE; FOX-DECENT, 2009, p.331-332).

Unido. Estes Estados possuem regras diferentes, com efeitos extraterritoriais, para combater corrupção e regular determinados processos de produção industrial. Essas normas tem o objetivo de punir, no âmbito doméstico, empresas nacionais ou estrangeiras que tenham cometido crimes fora do território estatal. (VARELLA, 2013, p.102).

De uma forma ou de outra, percebe-se que, independente da fundamentação, seja pela aceitação da diversidade ou pela imposição de normas de uns Estados sobre outros, há no sistema complexo do Direito Internacional um aumento, gradativo, de fontes normativas que interagem entre si, também no formato não linear de redes.

4 O CIBERESPAÇO COMO UM NOVO DOMÍNIO DA GUERRA

A evolução do conhecimento humano e a busca do desenvolvimento científico e tecnológico induzem o homem a alcançar fronteiras nunca antes imaginadas, em especial, no ramo da tecnologia. A aspiração humana de experimentação constante, em prol da sua evolução, leva a um reconhecimento, cada vez mais evidente, da influência que o desenvolvimento da tecnologia exerce nas vidas humanas, e, consequentemente, nas relações complexas da sociedade internacional.

A evolução da tecnologia e viabilização de um crescente número de interações, no cenário internacional, dos mais diversos atores coloca em xeque o futuro do Direito Internacional clássico, quase que somente interestatal e delimitado por uma normatividade ainda muito linear.

O mundo, em constante modificação, sofre influências do fenômeno da globalização e, com o advento da Internet, o poder[31], exercido pelos Estados, investe cada vez mais em novos recursos tecnológicos, que podem e são utilizados nas relações internacionais, sobretudo na relação complexa de interações, cooperações e competições, características da sociedade internacional.

A grande dificuldade de se entender as novas formas de exercício do poder e, buscar viabilizar a solução pacífica dos problemas que podem surgir, a partir do uso de novas tecnologias, está na própria estrutura complexa do cenário internacional, ainda não compreendida pelo Direito Internacional. Não se defende uma relativização da soberania dos Estados, nem uma uniformização linear do direito, mas objetiva-se analisar o Direito Internacional e as relações de poder sob a perspectiva da complexidade.

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

[31] Poder do Estado: “poder de associação que há de cuidar dos seus fins comuns e que ordenará e dirigirá a execução de suas ordens por toda a unidade, cujos destinatários são os homens”. (QUINTÃO SOARES, 2008, p. 89).

grandes potências a aguardar circunstâncias mais favoráveis, ou tentar aumentar a sua influência sem o uso do poder militar. (MEARSHEIMER, 2007, p.20). Entretanto, não se pode esquecer que não só de interações entre e com grandes potências vive a sociedade internacional e que de uma forma ou de outra, todos os atores internacionais acabam por estabelecer conexões interativas. Nessas conexões complexas, cada ator internacional utiliza-se das ferramentas de persuasão que possui para buscar seus objetivos.

Na definição do cientista político Joseph S. Nye Jr (1937–) ter poder nas relações internacionais significa a habilidade de afetar os outros atores internacionais, para obter o que se deseja. É possível realizar essa tarefa de convencimento de três formas: por meio da coerção, por meio do suborno ou por meio da persuasão. A utilização da força militar ou econômica o autor chama de ‘hard power’, e a utilização de estratagemas de persuasão ideológica de ‘soft power’ (diplomacia, cultura, história). Todos esses são meios de, ao se relacionar no âmbito internacional, conseguir com que os outros façam o que se deseja. (NYE JR, 2010, p. 12).

O termo ‘soft power’ ou “poder brando” é definido como a utilização de ferramentas de poder mais brandas, para a imposição da vontade do Estado, aos outros Estados, nas relações internacionais. O ‘soft power’ é exercido através da diplomacia, assistência econômica e comunicação pacífica, sendo de imprescindível importância, uma vez que o poder militar (‘hard power’), sozinho, não consegue defender os interesses estatais, no âmbito internacional. (NYE JR, 2010, p. 14).

Entretanto, especialistas do Direito Internacional adotam o ideal do ‘dever ser’ da doutrina e afirmam que a única forma legal de se obter um convencimento e se chegar à paz, no âmbito internacional, deve ser por meio do ‘soft power’, em especial, da diplomacia. Contudo, essa não é a realidade complexa na qual há uma vasta utilização, pelos plurais atores internacionais, de todos os poderes (‘hard power’ e ‘soft power’) ao mesmo tempo.

A compreensão do mundo como bipolar ou multipolar é usual, mas não há uma dimensão singular para a definição da sociedade internacional na atualidade. No fim do século XIX ou até mesmo início do século XX, o poder militar dominava as relações interestatais e não se percebia uma grande importância de se estudar outras formas de poder. Entretanto, na realidade atual, há diversas formas de

distribuição de poder no cenário internacional, seja no âmbito militar, econômico, transnacional, entre outros.

Joseph Nye Jr. faz uma analogia da distribuição de poder atual como um jogo de xadrez tridimensional. Em uma primeira dimensão, há um tabuleiro que trabalha as relações baseadas no poder militar, sendo que os Estados Unidos da América são, na atualidade, o único Estado com alcance militar global. Entretanto, em uma segunda dimensão, está o poder econômico, hoje multipolar com influências da União Europeia, China, Índia e até do Brasil. Na terceira dimensão transnacional está tudo aquilo que transborda do controle dos Estados, como a mudança do clima, terrorismo, dentre outros. Os poderes são distribuídos, de forma caótica e complexa, portanto não há mais sentido em discutir sobre a polarização das relações internacionais. Um Estado pode ter mais recursos de poder que os outros, mas se o Estado não consegue converter de forma eficaz esses recursos, em resultados, de nada adianta ter 'hard power' e 'soft power' sem saber conjugá-los de forma correta em cada situação. (NYE JR, 2010, p. 157-158).

A política estadunidense é um bom exemplo, ao aplicar tanto "hard power" quanto 'soft power', na persecução de seus interesses. A 67ª secretária de Estado dos Estados Unidos, Hillary Clinton, afirma que aplica nas relações internacionais o que Joseph Nye Jr. classifica como 'smart power', ou seja, 'poder inteligente'. Essa ação visa à utilização de todas as armas e meios disponíveis, brandos ou mais agressivos, na prática da política internacional do Estado. A relação de poder, travada no âmbito internacional, não se define somente pela observação da capacidade militar de cada Estado, uma vez que, além do armamento militar, os meios conhecidos como 'soft power' ou "poder brando"[32] são essenciais para a defesa dos interesses estatais, no âmbito internacional. (NYE JR, 2010, p. 13).

O "poder inteligente é a combinação do 'hard power' de coerção e do 'soft power' da persuasão e atração". (NYE JR., 2010, p.137, tradução nossa).[33] Entretanto, o Direito Internacional não legaliza a utilização do 'hard power', pois condena a utilização da guerra[34], como um meio legal para a solução de conflitos

[32] 'Soft Power' ou 'poder brando': é o poder de atrair os outros sujeitos de Direito Internacional a acreditarem que possuem a mesma vontade do Estado dominante, através do uso do poder de convencimento, sem recorrer à ameaça da força e da coerção. (NYE JR., 2004, p. 6).

[33] "Smart power is the combination of the hard power of coercion and the soft power of persuasion and attraction." (NYE JR., 2010, p. 137).

[34] "Nós, os povos das Nações Unidas, decididos:

internacionais. A tendência do legalismo internacional é a de incentivar o uso somente do ‘soft power’, como meio de solução de controvérsias, uma vez que “a promoção da democracia, direitos humanos, e desenvolvimento da sociedade civil não é melhor administrada com o cano de uma arma”. (NYE JR., 2010, p. 143, tradução nossa).[35]

O poder, bem administrado, cria metas e define quais são os debates e interações mais importantes de serem realizados entre atores internacionais. Finalmente, o poder ainda tem a capacidade de definir quais interações serão feitas de forma positiva e cooperativa, entre os identificados como aliados, ou de forma negativa e competitiva, entre inimigos. É importante, ainda, não simplificar essas relações e entendê-las de forma linear, pois elas não são estáticas. As relações de cooperação ou competição podem ser travadas a qualquer momento entre qualquer ator internacional, pois o identificado como inimigo hoje pode ser o aliado de amanhã e vice-e-versa.

Diante da realidade complexa e de luta pelo poder, vivida pelos atores internacionais, qualquer novo recurso que surja, para auxiliar os Estados nas

---

a preservar as gerações vindouras do flagelo da guerra que por duas vezes, no espaço de uma vida humana, trouxe sofrimentos indizíveis à humanidade;

a reafirmar a nossa fé nos direitos fundamentais do homem, na dignidade e no valor da pessoa humana, na igualdade de direitos dos homens e das mulheres, assim como das nações, grandes e pequenas;

a estabelecer as condições necessárias à manutenção da justiça e do respeito das obrigações decorrentes de tratados e de outras fontes do Direito Internacional;

a promover o progresso social e melhores condições de vida dentro de um conceito mais amplo de liberdade;

e para tais fins:

a praticar a tolerância e a viver em paz, uns com os outros, como bons vizinhos;

a unir as nossas forças para manter a paz e a segurança internacionais;

a garantir, pela aceitação de princípios e a instituição de métodos, que a força armada não será usada, a não ser no interesse comum;

a empregar mecanismos internacionais para promover o progresso econômico e social de todos os povos;

Resolvemos conjugar os nossos esforços para a consecução desses objetivos.

Em vista disso, os nossos respectivos governos, por intermédio dos seus representantes reunidos na cidade de São Francisco, depois de exibirem os seus plenos poderes, que foram achados em boa e devida forma, adoptaram a presente Carta das Nações Unidas e estabelecem, por meio dela, uma organização internacional que será conhecida pelo nome de Nações Unidas.” (ONU, 1945).

[35] “Promoting democracy, human rights, and development of civil society are not best handled with the barrel of a gun”. (NYE JR., 2010, p. 143)

disputas internacionais, deve ser estudado com cautela, uma vez que permitir a exploração impensada, da nova tecnologia, pode levar a consequências reais de infração ao Direito Internacional e aos direitos humanos. (ROTHKOPF, 2011).

Ao longo da história, não é novidade que a informação tem sido utilizada como fonte de poder para o estabelecimento de quais seriam os Estados e atores mais influentes, no âmbito internacional. A informação é uma das fontes de poder do Estado que, quando bem administrada, pode ser decisiva em uma situação de necessidade. “Conhecimento é poder, e mais pessoas tem mais informações do que em qualquer momento prévio na história humana.” (NYE JR, 2008, p. 47, tradução nossa).[36]

O que se discute não é o acesso à informação colocada no meio eletrônico, mas a exploração da tecnologia e da cibernética, como um conhecimento da exploração da informação e da tecnologia organizada em rede, no âmbito internacional e a utilização desses recursos como fonte de poder, e, possivelmente como arma de guerra. Identifica-se a necessidade de estudar a temática da ‘guerra cibernética’ e as consequências que essa nova realidade pode trazer para o Direito Internacional ainda voltado para uma organização do cenário de forma linear.

O Direito Internacional, ao tentar controlar as ações dos atores, no meio eletrônico, deve ter o cuidado adequado de tentar não reproduzir os erros cometidos em outros domínios políticos, uma vez que, até hoje, as relações internacionais sofrem grande influência da vontade dos Estados que possuem mais poder, em especial “hard power”.

Na dinâmica da complexidade e da certeza das incertezas, seria ingênuo acreditar em uma organização da sociedade internacional de forma linear, ou até mesmo que isso será realmente possível. Pretende-se compreender como ocorrem as interações internacionais no ciberespaço e as novas dinâmicas de poder que surgem diante desse novo espaço relacional em redes. Segundo José Luiz Quadros de Magalhães, é questionável acreditar que ainda tenhamos “segurança neste mundo de comunicações instantâneas e de mudanças constantes e fora de controle”. (MAGALHÃES, 2008, p. 27).

‘Ciberespaço’, na definição de Joseph Nye Jr., é um campo operacional delineado pelo uso de meios eletrônicos para explorar a informação por meio de

[36] “Knowledge is power, and more people have more information than at any prior time in human history.” (NYE JR, 2008, p. 47).

sistemas interconectados. (NYE JR., 2010, p. 122). O ciberespaço consiste em um novo domínio relacional no qual ocorrem conexões interativas, em rede complexa, dentre os mais diversos atores internacionais e essa novidade traz inúmeros questionamentos sobre o futuro do Direito Internacional.

O ciberespaço constitui-se, pois, por várias redes de atividades, em um sistema híbrido de relações físicas e virtuais. Na sociedade internacional, percebe-se a propriedade física do ciberespaço pala manutenção das regras econômicas, custos crescentes e normas de controle e respeito à jurisdição e soberania dos Estados. A novidade está na propriedade virtual do ciberespaço, que domina a informação, tem características de relações econômicas em rede e a prática de políticas difíceis de serem controladas pela lei, seja ela nacional ou internacional. (NYE JR., 2010, p. 123).

Ao tratar da nova realidade das relações no âmbito do ciberespaço, Joseph S. Nye Jr. utiliza-se da expressão 'cyber power' ('poder cibernético'), para se referir à habilidade dos Estados de obter, nas relações internacionais, resultados almejados, através do uso de recursos eletrônicos, por meio da informação interconectada, no domínio cibernético. (NYE JR., 2010, p. 123). As consequências do uso desse novo poder, pelos atores internacionais, não são somente virtuais, mas reais e importantes de serem examinadas pelo Direito Internacional.

> Poder cibernético pode ser definido em termos de um conjunto de recursos que se relacionam com a criação, controle e comunicação de informações-infraestrutura eletrônica e baseado em computador, redes, software, habilidades humanas. Isso inclui não apenas a Internet de computadores ligados em rede, mas também Intranets, tecnologias de celulares e comunicações espaciais. Definido de forma comportamental, poder cibernético é a capacidade de obter resultados preferidos através do uso dos recursos de informação interconectados eletronicamente do domínio cibernético. Poder cibernético pode ser usado para produzir resultados preferidos dentro do ciberespaço, ou ele pode usar instrumentos virtuais para produzir resultados preferenciais em outros domínios fora do ciberespaço. (NYE JR., 2010, p. 123, tradução nossa).[37]

No século XXI, o avanço da cibernética leva os sujeitos de Direito Internacional a buscar, através do uso da tecnologia de redes, a solução de

[37] "Cyberpower can be defined in terms of a set of resources that relate to the creation, control, and communication of electronic and computer-based information—infrastructure, networks, software, human skills. This includes not only the Internet of networked computers, but also Intranets, cellular technologies, and space-based communications. Defined behaviorally, cyberpower is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain. Cyberpower can be used to produce preferred outcomes within cyberspace, or it can use cyberinstruments to produce preferred outcomes in other domains outside cyberspace".

conflitos internacionais e a imposição de suas vontades aos outros Estados, por meio do uso inteligente da tecnologia (poder cibernético).

Os Estados estão cientes, uns mais do que outros, de que o poder cibernético pode lhes ajudar na atuação, no âmbito das relações internacionais, pela busca da dominação da informação, no espaço cibernético e, também, em outros domínios, que se encontram fora do mundo cibernético. O ideal para aquele Estado que almeja mais poder no cenário internacional é utilizar de um conceito de 'smart power' reformulado, sendo hoje constituído de 'hard power', 'soft power' e 'poder cibernético'. O 'domínio do ciberespaço' é definido, hoje, como o quinto domínio da guerra, após a terra, o mar, o ar e o espaço.

Durante o curso da história mundial, o desenvolvimento de novas tecnologias induz à reflexão sobre os efeitos que essas novas invenções poderiam trazer para a sociedade e para as relações entre Estados. O domínio dos mares levou à discussão do 'poder naval', o domínio aéreo à reflexão a respeito do 'poder aeronáutico' e, até mesmo, o 'poder espacial'. (NYE JR., 2010, p. 124).

A grande distinção do 'domínio cibernético', que cria curiosidade e instiga a pesquisa cientifica, é o fato de esse novo domínio foi criado pelo próprio homem, sendo, ainda objeto de mudanças rápidas e constantes, que alteram o curso da história e podem, cada vez mais, alterar os rumos das relações de poder entre os atores internacionais. A facilidade de manipulação do domínio cibernético, que não possui limites reais, e a dificuldade de se construir barreiras legais que possam proteger esse domínio, leva a uma instabilidade ainda maior das relações internacionais complexas. (PREBLE, 2011, p. 72).

O domínio cibernético é um campo de características ainda mais hostis e complexas, que facilitam a instauração de uma guerra, pois são árduas as possibilidades de se estabelecer um controle do que ocorre no espaço cibernético. É, portanto, grande a dificuldade de se fiscalizar e exigir que os Estados e demais atores internacionais obedeçam às normas de Direito Internacional no domínio cibernético e, consequentemente, não ajam de forma a viabilizar a violação de direitos, no mundo real. (LIBICKI, 2009, p.12).

O espaço cibernético é terreno fértil para a violação de normas jurídicas, em especial as de Direito Internacional, pois trata-se de local de fácil acesso, frequentado por inúmeros 'jogadores', difíceis de serem identificados, que atuam

em prol de seus interesses, e, além disso, a dissimulação no meio eletrônico é de mais difícil detecção. (NYE JR., 2010, p. 126).

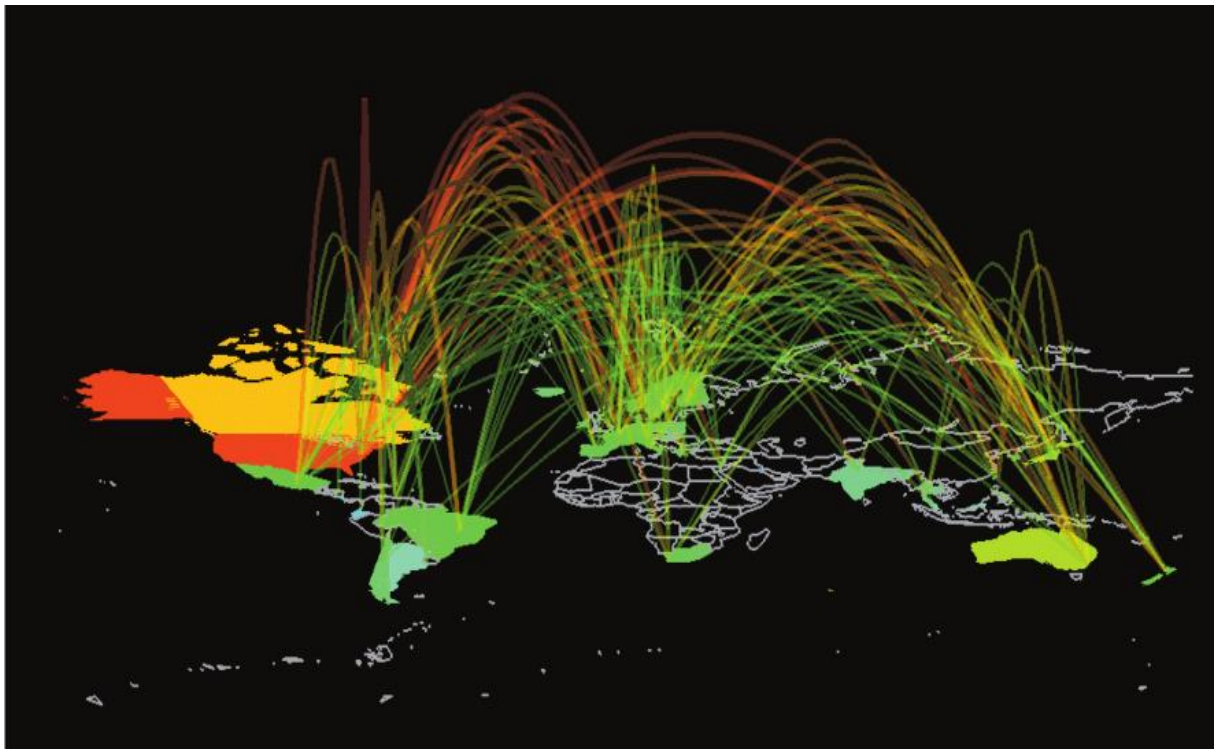
Outro fator de preocupação, para os Estados, está no fato de que, no âmbito cibernético, é praticamente impossível determinar qual ator internacional possui um maior poder, uma vez que não é necessário ser economicamente ou militarmente poderoso para obter bons resultados, na luta pelo poder, através desse meio. Na realidade, o Estado que possui um grande avanço, no conhecimento da cibernética, e, conta com esse recurso, para a ação em momentos de guerra pode, caso sofra um ataque ao seu sistema cibernético, colocar em risco toda a sua estratégia militar, os seus mecanismos de segurança e a sua influência no cenário internacional. (PREBLE, 2011, p. 104).

A realidade complexa do ciberespaço exige dos atores internacionais, em especial dos Estados, o investimento em dois setores distintos: na utilização da cibernética, como arma para a proteção e atuação e na criação de mecanismos de defesa ao domínio cibernético militar, a fim de evitar a insegurança diante dos ataques cibernéticos, que podem ser realizados pelos mais diversos atores.

Os geógrafos ingleses Martin Dodge e Rob Kitchin fizeram uma tentativa de mapear o ciberespaço para compreender o seu funcionamento. O mapeamento realizado comprova a existência de relações em redes complexas difíceis de serem catalogadas de forma precisa e na linearidade cartográfica que se espera de um mapa. Na figura seguinte, extraída da obra “Atlas do Ciberespaço”[38], tem-se uma ideia da complexidade das relações em rede estabelecidas entre os inúmeros novos atores da sociedade internacional e das dificuldades que se apresentam para o Direito Internacional.

[38] Nome original do livro editado em inglês e traduzido para o português pela autora: “Atlas of Cyberspace”, de 2001.

ILUSTRAÇÃO 3 – Mapa Mundial do Ciberespaço



Fonte: "Atlas do Ciberespaço", obra dos autores Martin Dodge e Rob Kitchin. (DODGE, KITCHIN, 2001, p.72).

Desde 2009, os Estados Unidos da América criaram o Comando Cibernético norte-americano (USCYBERCOM).[39] Trata-se de uma organização militar, subordinada ao Comando de Estratégias Militares, com o objetivo de utilizar a informação tecnológica e a Internet, como uma arma de guerra. O Comando Militar Cibernético centraliza as operações cibernéticas, organiza os recursos do domínio cibernético e sincroniza as táticas de defesa das redes do exército estadunidense. (U.S. DEPARTMENT OF DEFENSE, 2011).

O poder militar estadunidense reconhece que o espaço cibernético consiste em um novo domínio que deve ser cuidado e utilizado para estratégias militares. WILLIAM J. LYNN III, secretário de defesa norte-americana, afirma que:

> 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, tradução nossa).[40]

[39] United States Cyber Command (USCYBERCOM)

[40] "Right now, more than 100 foreign intelligence organizations are trying to hack into the digital networks that undergird U.S. military operations. The Pentagon recognizes the catastrophic threat

A crescente dependência na tecnologia de informação, pelos atores internacionais, criou a necessidade de se aumentar a proteção digital das redes e infraestruturas tecnológicas do Estado. O presidente Barack Obama, preocupado com a necessária conscientização a respeito do perigo da utilização da cibernética, como meio de guerra, que ameaça a soberania do Estado, decretou o mês de outubro de 2011 como o mês da consciência da ameaça nacional à segurança cibernética.

> No início da minha Administração, nós começamos a atualizar nossos programas e políticas de segurança cibernética. Nós desenvolvemos um plano compreensível que assegura uma resposta nacional coordenada aos principais eventos cibernéticos disruptivos. Nesse mês de maio, nós também propomos ao Congresso um plano de fortalecimento da proteção de nosso poder estrutural, sistemas de água e outros meios críticos de infraestrutura. E porque nós já constatamos os benefícios e riscos que cibernética – e das informações relacionadas à tecnologia podem ocasionar pelo mundo, esse ano nós apresentamos a primeira visão internacional detalhada para o futuro do Internet. Ela ajusta uma agenda para a parceria com outras nações e define melhor como nós podemos assegurar a livre circulação da informação segura e promover direitos universais, privacidade, e prosperidade. (...)
> AGORA, CONSEQÜENTEMENTE, eu, BARACK OBAMA, presidente dos Estados Unidos da América, em virtude da autoridade investida em mim pela constituição e pelas leis dos Estados Unidos, proclamo, por meio deste, outubro de 2011 como o mês nacional da consciência de Segurança Cibernética. Eu convido os povos dos Estados Unidos para reconhecer a importância do segurança cibernética e para observar este mês com atividades, eventos, e treinamentos que realçarão nossas segurança nacional e superação. (OBAMA, 2011, tradução nossa).[41]

É impossível para o Estado não se utilizar das ferramentas desenvolvidas pela tecnologia, em prol do seu beneficio, seja no âmbito nacional ou internacional, entretanto, desenvolver estratégias que possam aumentar a segurança dos Estados, quando utilizarem-se desses mecanismos, na defesa de seus interesses, é de inquestionável necessidade, principalmente diante da crescente ameaça

---

posed by cyber warfare, and is partnering with allied governments and private companies to prepare itself". (LYNN III, William J. 2010, p.1).

[41] Early in my Administration, we began updating our Nation's cybersecurity programs and policies. We developed a comprehensive plan that ensures a coordinated national response to major disruptive cyber events. This May, we also proposed to the Congress a plan to strengthen protection of our power grids, water systems, and other critical infrastructure. And because we have seen the benefits and risks of cyber- and information-related technologies play out across the world, this year we laid out the first comprehensive international vision for the future of the Internet. It sets an agenda for partnering with other nations and better defines how we can ensure the secure, free flow of information and promote universal rights, privacy, and prosperity. (…)NOW, THEREFORE, I, BARACK OBAMA, President of the United States of America, by virtue of the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim October 2011 as National Cybersecurity Awareness Month. I call upon the people of the United States to recognize the importance of cybersecurity and to observe this month with activities, events, and trainings that will enhance our national security and resilience. (OBAMA, 2011).

apresentada pelos outros atores internacionais. Os ataques cibernéticos aos sistemas governamentais têm sido uma prática constante, que exigem a atuação dos Estados em prol do desenvolvimento, em cada um deles, de sistemas de segurança virtual, que preservem as informações, e, principalmente, as estratégias militares dos Estados.

A importância da informação tem feito com que o domínio cibernético seja utilizado como o grande teatro para os conflitos internacionais. Os conflitos contemporâneos sejam eles de natureza econômica, política ou militar, têm sido reproduzidos e estimulados nas redes cibernéticas (Internet, intranets[42], etc).

O termo 'guerra cibernética', eleito como objeto desse trabalho, limita-se à análise da utilização da tecnologia cibernética para a violação de informações militares dos Estados e às consequências jurídicas que essa quebra de segurança pode acarretar à sociedade e ao direito internacionais.

> O termo 'guerra cibernética' só cobre uma estreita subseção dos ataques cibernéticos. Do ponto de vista militar, ela deve dizer respeito à parte das informações de guerra. Para determinar a substancia e relevância do conceito de 'guerra cibernética', nós requeremos não apenas uma definição léxica, mas também uma diferenciação as dimensões operacionais e estratégicas da guerra cibernética. (CAVELTY, 2011, p.1, tradução nossa).[43]

É complexa a atividade de distinguir quais seriam as ações, no domínio cibernético, que são classificados como ações de guerra cibernética ou não. Imagina-se que identificar o ofensor à informação militar do Estado pudesse ser um indicativo, mas nem sempre essa identificação é fácil. Outro critério poderia ser os objetivos pelos quais o ataque foi realizado e as possíveis consequências desse ataque. Quanto mais consequências nefastas à segurança do Estado, mais possível será de se identificar um ato de guerra cibernética. (WENBT, 2011, p. 2).

---

[42] Intranet – "rede de computadores privada que assenta sobre a suíte de protocolos da Internet, porém, de uso exclusivo de um determinado local, como, por exemplo, a rede de uma empresa que só pode ser acessada por seus usuários ou colaboradores internos". (TORQUE COMUNICAÇÃO E INTERNET, 2014).

[43] The term "cyber war" only covers a narrow sub-section of all cyber attacks. From a military point of view, it should be regarded as part of information warfare. In order to determine the substance and relevance of the concept "cyber war", we require not only a lexical definition, but also a differentiation between the operative and strategic dimensions of cyber war. (CAVELTY, 2011, p.1)

Os crimes cibernéticos ou ‘cibercrimes’ são conceituados como “qualquer atividade criminal que usa um computador como instrumento, alvo ou meio de perpetuar outros crimes”. (PARTHASARATHI, 2011, tradução nossa).[44]

Esses crimes no ciberespaço não serão, necessariamente, atos de guerra cibernética, dependendo-se dos agentes envolvidos, do bem jurídico atingido e das vítimas de cada caso.

Na Resolução 65/230 da Assembleia Geral da ONU solicitou-se à Comissão contra o Crime Prevenção e Justiça Criminal para estabelecer um relatório sobre os crimes cibernéticos, em conformidade com o n.º42 da declaração de Salvador realizada no Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal que tratou em abril de 2010 sobre as "Estratégias Globais para Desafios Globais: A Prevenção do Crime e o Desenvolvimento dos Sistemas de Justiça Criminal em um Mundo em Transformação". (ONU, 2010).

No intitulado “Estudo Compreensivo sobre crimes cibernéticos”[45] realizado por diferentes estudiosos que constituem a “Comissão sobre Prevenção ao Crime e Justiça Penal” da ONU, traçou-se o novo perfil das relações criminosas no ciberespaço. Os principais problemas encontrados no combate dos crimes cibernéticos foram a diversidade e complexidade das relações na sociedade internacional; a utilização de métodos tradicionais que não mais atendem a nova realidade do ciberespaço; a necessidade de se criar um novo conceito de território na apuração das competências criminais no âmbito do ciberespaço; a não uniformidade das leis nacionais de combate a esses crimes; a necessidade de um apoio de técnicos da tecnologia da informação a todo o momento e a necessidade de uma visão sistêmica, holística internacional, para a criação de mecanismos de defesa dos Estados contra esses crimes. (ONU, 2013).

A ONU afirma que definir os cibercrimes como um tipo penal fechado, como se faz nas legislações nacionais, é impossível, tendo em vista o fato deles

---

[44] “Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime”. (PARTHASARATHI, 2011).

[45] O título original do relatório realizado pela ONU é “Comprehensive Study on Cybercrime” nesse texto traduzido como “Estudo Compreensivo sobre crimes cibernéticos”. Esse relatório foi realizado com para o grupo de peritos Intergovernamentais que tratam do assunto na ONU, com o intuito de combater o Crime organizado. Os autores foram Steven Malby da Universidade de Goettingen, na Alemanha, Robyn Mace da Universidade de Michigan, Anika Holterhof, da Universidade de Amsterdã, Cameron Brown da Universidade Nacional da Austrália, Stefan Kascherus, da Universidade de Oxford e Eva Ignatuschtschenko, da Universidade de Viena.

abrangerem um conjunto de atos, e não somente um ato, que se utiliza do ambiente eletrônico para causar violações a bens juridicamente tutelados. (ONU, 2013)

A pesquisadora chefe do ‘Grupo de Pesquisa de Risco e Resiliência’, do Instituto Federal Suíço de Tecnologia, em Zurique, Myriam Dunn Cavelty (1976–) afirma que existem diferentes cibercrimes, menos gravosos, que antecedem a guerra cibernética. O crime de consequências mais brandas seria o crime de ‘vandalismo cibernético’ que envolve a modificação ou destruição virtual de dados. Esse crime costuma ter o objetivo de chamar a atenção pública, mas como é realizado de forma muito pulverizada, não cria grandes consequências para os Estados. O segundo crime mais gravoso é o de ‘espionagem cibernética’, geralmente realizado contra as grandes corporações, para a obtenção de segredos industriais. Esse crime também poder ser cometido contra os Estados e tem se provado cada vez mais comum no cenário internacional. O último crime, antes de se chegar à guerra cibernética, é o de ‘terrorismo cibernético’ ou ‘ciberterrorismo’, através do qual, atores não estatais tem o objetivo de utilizar o meio eletrônico para intimidar o Estado, através do terror da população civil. (CAVELTY, 2011, p.2). Todos esses crimes, pelo fato de serem realizados no ciberespaço, demandam uma normatividade nacional e internacional, ainda difícil de ter sua metodologia definida devido à complexidade das relações estabelecidas.

A guerra cibernética distingue-se de todos os crimes descritos, pois se caracteriza por ações características de guerra, realizadas por meio eletrônico, tendo consequências virtuais e reais. É uma guerra da informação, primordial para a definição de como agir diante do Estado inimigo, uma vez que o ataque cibernético tem a principal função de buscar informações sobre os pontos fracos do inimigo, para atacá-los. A guerra cibernética reflete a crescente utilização da tecnologia para a guerra, na era da informação. (CAVELTY, 2011, p.2).

O potencial para os danos realizados por uma guerra cibernética é incalculável, uma vez que acreditar que a guerra no meio virtual, teria consequências somente virtuais, é uma visão irrealista dos pontos determinantes das relações internacionais, como, por exemplo, a constante disputa de poder existente entre os Estados. (CLARKE; KNAKE, 2010, p.11).

Analisa-se que mesmo que as ações de guerra, por meio eletrônico, sejam parte de uma nova realidade complexa a ser enfrentada pela sociedade

internacional, os aspectos do Direito Internacional que visam a proteção dos direitos humanos e a luta contra a utilização da guerra como meio de solução de controvérsias, se mantém intactos. O grande desafio que se apresenta está na possibilidade de se efetivar a aplicação de um Direito Internacional que mantenha seu caráter ideal de proteção aos atores internacionais e aos direitos humanos e que tenha efetividade em sua aplicação, apesar do árduo rastreamento das relações interativas e ocorridas no meio eletrônico.

O presente trabalho é fruto, portanto, da análise crítica do ciberespaço como uma nova fronteira da guerra, devendo ser, assim, objeto de regulação pelo Direito Internacional, em prol da defesa dos direitos, nos casos de possíveis guerras cibernéticas.

5 O DIREITO INTERNACIONAL E O ESTADO DE GUERRA CIBERNÉTICA

No livro intitulado “Da Guerra” de 1873, Carl Von Clausewitz (1780–1831), define de forma tradicional a guerra como “um ato de força para obrigar o nosso inimigo a fazer a nossa vontade”. (CLAUSEWITZ, 2014, p. 75). A guerra até então é vista como uma forma de dominação por meio da força.

> A guerra nada mais é do que um duelo em grande escala. Inúmeros duelos fazem uma guerra, mas pode ser formada uma imagem dela como um todo, imaginando-se um par de lutadores. Cada um deles tenta, através da força física, obrigar o outro a fazer a sua vontade. O seu propósito imediato é derrubar o seu oponente de modo a torná-lo incapaz de oferecer qualquer outra resistência. (CLAUSEWITZ, 2014, p. 75).

Michel Foucault (1926–1984), na obra “Em Defesa da Sociedade”, questiona esse posicionamento de visão da guerra somente como uma utilização de força, quando afirma que “a guerra não é mais que a continuação da politica por outros meios"; ela "não é somente um ato político, mas um verdadeiro instrumento da política". (FOUCAULT, 2005, p.22).

Atualmente, as definições tradicionais de ‘estado de guerra’ se relacionam à existência de conflitos armados, geralmente prolongados, ao envolver violência organizada entre Estados, por motivos políticos. Entretanto, esse conceito se demonstra limitado na contemporaneidade, uma vez que trabalha a guerra de forma unidimensional, ao imaginar que somente a força ou a política estabelecem esse embate entre Estados.

O novo domínio da guerra, chamado de ‘ciberespaço’, chega para colocar em questionamento esses conceitos de guerra vinculados a atuação física dos Estados. O ciberespaço é um domínio peculiar, ainda não compreendido em toda sua extensão, para se determinar as consequências de uma ação de guerra nesse novo domínio. Por um lado, o ciberespaço é similar aos domínios comuns da guerra (terra, mar, ar e espaço), mas como não é um domínio físico, encontrado na natureza, sendo assim, a liberdade de conexões que ele permite, o faz completamente imprevisível.

O ciberespaço e suas regras relacionais devem ser vistos de forma nova, o que não quer dizer ser impossível aplicar regras dos outros domínios a ele. Entretanto, algumas peculiaridades desse novo domínio, merecem uma análise específica pelos atores internacionais. Não há forma de se compreender o que se

constitui no estado de guerra no ciberespaço sem entender o novo palco dos conflitos cibernéticos. (LIBICKI, 2009, p. 369).

O ciberespaço e a noção de uma sociedade internacional complexa, ao envolver atores variados que interagem em rede, no âmbito cibernético internacional, faz com que surjam definições mais abrangentes da expressão 'estado de guerra', vinculadas à pluralização dessa sociedade.

Definições recentes, sensíveis à pluralização dos atores internacionais e ao deslocamento da violência, referem-se ao estado de guerra como um ato de força realizado por um Estado, grupo terrorista, cartel de drogas, grupo revolucionário, ou coalizão de Estados para obrigar o inimigo a fazer a própria vontade, aceitar uma ideologia ou ação específicas.

A existência de um "estado de guerra", entre atores internacionais, não está mais vinculada à logica centralizadora da guerra somente entre Estados, há o aumento de possibilidades de novos atores promoverem a guerra, mesmo os não identificados como sujeitos de Direito Internacional. Além disso, a "força" como elemento de guerra deixa de ser somente a força militar e passa a ser uma vinculação de combinações de forças de 'hard power', 'soft power' e 'cyber power', todos articulados de forma inteligente pelo 'smart power', como já discutido.

A legitimação da violência nas guerras mais recentes é menos centrada nos Estados, devido, em parte, por causa dos limites não tão bem delineados na sociedade internacional e no ciberespaço cheio de interações entre as relações inter e intra-estatais. Além disso, as causas de uma guerra se modificaram de forma significativa por meio da expansão das relações geopolíticas, do nacionalismo militarista e das preocupações ideológicas com conflitos entre diversas identidades.

A Organização das Nações Unidas define o ciberespaço como "o sistema global de sistemas de computadores, infraestruturas de comunicação internética, entidades de conferência on-line, bancos de dados e utilitários de informação geralmente conhecidas como a Net". (ANDRESS; WINTERFELD, 2011, p.349, tradução nossa).[46] Entretanto, essa definição é simplista diante da complexidade

[46] "The global system of systems of Internetted computers, communications infrastructures, online conferencing entities, databases and information utilities generally known as the Net." (ANDRESS; WINTERFELD, 2011, p.349).

do ciberespaço. O ciberespaço vai além do domínio da internet, em especial quando se estuda o ciberespaço como um campo de guerra.

Diante da complexidade do domínio cibernético, não é simples definir como se dá o estado de guerra no ciberespaço. O Departamento de Defesa do governo dos Estados Unidos define o ciberespaço como “o ambiente teórico em que a informação digitalizada é comunicada através de redes de computadores”. (JENKINS, 2002, p.13). É o local de domínio global, no ambiente da informação, que consiste de interações vinculadas à tecnologia da informação, Internet, redes de telecomunicação e sistemas de computadores. Operações e atuações no ciberespaço utilizam de todas as capacidades tecnológicas dos atores internacionais, com o objetivo inicial de interagir no ciberespaço e, em um segundo momento, outros domínios não virtuais. Essas interações podem levar à cooperação, competição, conflitos e à guerra.

No caso do ‘estado de guerra no ciberespaço’ não se pode adotar o discurso da autoridade estatal para determinar a existência da guerra. Questiona-se, também, se metodologicamente a visão militar seria a abordagem correta da temática, uma vez que há um aumento dos atores atuantes no ciberespaço e a possibilidade deles também participarem da guerra cibernética, apesar de não possuírem a legitimidade de representação política estatal.

Jason Andress e Steve Winterfeld acreditam que a abordagem militar seja a correta para se discutir o estado de guerra no ciberespaço, mas que os princípios geográficos clássicos precisam ser abandonados, além de se adaptarem aos ditames de guerra do Direito Internacional, nesse novo domínio. Eles afirmam que utilizar o termo ‘estado de guerra no ciberespaço’ não é adotar uma visão somente militarista da questão e muito menos com consequências apenas virtuais. É necessário explorar outras opções de controle da guerra, pois os sistemas estão ligados em uma mesma sociedade internacional, campo de batalha em que os atores estão lutando, utilizando-se da tecnologia como arma de guerra. (ANDRESS; WINTERFELD, 2011, p.296).

As motivações para a existência de uma guerra cibernética são as mais variadas possíveis, sendo que a principal está na constante sobreposição de interesses dos atores, nas redes relacionais da sociedade internacional. Tradicionalmente, vencia os embates internacionais aquele que possuíam mais poder militar, mas hoje o poder de uma rede não é determinado somente por

recursos militares e econômicos, mas pelo número de conexões, que equivale ao poder de informação / influência. A atuação no ciberespaço com o objetivo de guerra ocorre por meio de acesso a informações exclusivas, redes de classificados, interconexões em uma rede social, aplicações ou dados de entes privados ou públicos ou sistemas que executam ataques à infraestrutura cibernética de defesa de outros atores. (ANDRESS; WINTERFELD, 2011, p.297).

As infraestruturas em redes da atualidade são os principais alvos para o ataque cibernético, porque o ciberespaço tem se desenvolvido ao ponto de organizar os sistemas de comando e controle, gerenciar a logística, permitir o planejamento e a atuação da equipe de operações, sendo a espinha dorsal das capacidades de inteligência dos Estados e atores internacionais.

Nos EUA, por exemplo, a maioria dos sistemas de comando e controle dos Estados-membros, bem como os próprios sistemas de defesa e desenvolvimento de armamentos, estão ligados à Rede Global de Informação (RGI)[47]. A RGI é globalmente interligada, voltada para a administração do conjunto de recursos de informação para a coleta, processamento, armazenamento, disseminação e gerenciamento de informações sobre a demanda de combatentes, políticos, e pessoal de apoio dos EUA. (ANDRESS; WINTERFELD, 2011, p.299).

O uso da tecnologia em rede no estabelecimento de táticas de defesa e administração dos recursos de poder é o que determina a força do Estado, mas a falta de um cuidado em defender essas informações pode se transformar também em uma fraqueza, pois Estados rivais ou outros atores interessados, poderiam, por meio do ciberespaço, descobrir esses segredos. Um inimigo pode entender as intenções e habilidades do outro por meio de uma investigação e violação do sistema. Além de descobrir informações, alterar, destruir ou furtar dados; o impacto pode ser desastroso.

Há o que se chama hoje de ‘estratégia cibernética’ de manipulação do poder que seria a aplicação da teoria de Joseph Nye Jr. sobre o ‘smart power’ em uma perspectiva de sistema de redes ligados à Internet e intranet. Há uma articulação da diplomacia, informação, inteligência tecnológica, militarismo e economia nas relações internacionais. Não há uma mudança completa nas estratégias relacionais

[47] O nome original em inglês dessa instituição é “Global Information Grid (GIG)” e foi traduzida nesse texto para o vernáculo com o nome de “Rede Global de Informação (RGI)”.

dos Estados, mas uma utilização do poder cibernético em prol da luta pelo poder. (ANDRESS; WINTERFELD, 2011, p.407).

A guerra é regida por princípios que orientam os Estados a agir de forma estratégica. Esses princípios chefiam a conduta dos militares e são genéricos, ao demonstrar o que se deve ter em mente em uma ação militar. Ao longo da história diversas obras foram escritas para orientar e determinar quais deveriam ser esses princípios que hoje são distintos de um Estado para o outro. Sun Tzu (544a.C-496a.C) foi um dos primeiros a falar sobre princípios da guerra em sua famosa obra "A Arte da Guerra".

O princípio básico dos ensinamentos de Sun Tzu é o de que a guerra é uma questão de vida ou morte, ou seja, se todos os guerreiros compreenderem esse princípio terão a motivação para a guerra.[48] Os princípios de Sun Tzu são "a doutrina, o tempo, o espaço, o comando, a disciplina".(TZU, 2006, p.12).

O Barão Antoine-Henri Jomini (1779-1869), autor do livro "Sumário da Arte da Guerra", traçou princípios para a guerra e estabeleceu cinco atividades basilares da guerra: estratégia, grande tática, logística e tática menor. (DE JOMINI, 2008, p.11).

Além desses autores, o teórico que mais contribuiu para a definição de princípios para a guerra foi o militar britânico John Frederick Charles Fuller (1878-1966), na obra "Os Fundamentos da Ciência da Guerra" uma principiologia para a guerra, ao se preocupar em tratá-la não como uma arte, mas como uma ciência. Fuller desenvolve a noção de que a guerra tem diversas facetas e uma principiologia na esfera mental, moral e física. A sua maior contribuição está na elaboração de nove princípios para a ciência da guerra que são seguidos por muitos Estados. Os princípios de Fuller são: princípio da direção, da concentração, da distribuição, da determinação, da surpresa, da resistência, da mobilidade, da ação ofensiva e da segurança. (FULLER, 1993, p.221).

O maior questionamento em relação aos princípios de guerra é se essas diretrizes adotadas pelos Estados se aplicariam também para a guerra no ciberespaço. Alguns princípios não são fáceis de serem aplicados, mas, como

[48] "A guerra tem importância crucial para o Estado. É o reino da vida e da morte. Dela depende a conservação ou a ruína do império. Urge bem regulá-la. Quem não reflete seriamente sobre o assunto evidencia uma indiferença condenável pela conservação ou pela perda do que mais se preza. Isso não deve ocorrer entre nós". (TZU, 2006, p.12).

todas as ações de guerra no ciberespaço, podem ocasionar consequências também no mundo real, é importante que os Estados não menosprezem as suas atuações nesse novo domínio e apliquem suas diretrizes.

O Brasil adota princípios para sua ação na defesa do Estado, definidos na Portaria Normativa nº113 da Secretaria de Política, Estratégia e Assuntos Internacionais de 1º de fevereiro de 2007. Os onze princípios adotados pelo Estado brasileiro são: objetivo[49], ofensiva[50], simplicidade[51], surpresa[52], segurança[53], economia de forças ou de meios[54], massa[55], manobra[56], moral[57], exploração[58], prontidão[59] e unidade de comando[60]. (BRASIL, 2007). Os princípios são aplicados

[49] Objetivo: "Princípio que diz respeito ao estabelecimento de objetivos claramente definidos e atingíveis, a fim de obter-se os efeitos desejados". (BRASIL, 2007).

[50] Ofensiva: "Princípio que se caracteriza por levar a ação bélica ao inimigo, de forma a se obter e manter a iniciativa das ações, estabelecer o ritmo das operações, determinar o curso do combate e, assim, impor sua vontade". (BRASIL, 2007).

[51] Simplicidade: "Princípio que preconiza a preparação e a execução de ordens e planos com concepções claras e facilmente inteligíveis, a fim de reduzir a possibilidade eventual de equívocos na sua compreensão, sem prejuízo da precisão e da flexibilidade necessárias. Caracteriza-se, também, pelo estabelecimento de uma relação de comando clara, direta e ininterrupta". (BRASIL, 2007).

[52] Surpresa: "Princípio que consiste em golpear o inimigo onde, quando ou de forma tal que ele não esteja preparado. O comandante que obtém o efeito da surpresa poderá alterar a seu favor, de forma decisiva, a correlação das forças em combate". (BRASIL, 2007).

[53] Segurança: "Princípio que consiste nas medidas essenciais à liberdade de ação e à preservação do poder de combate necessário ao emprego eficiente das forças armadas, tendo por finalidades: negar ao inimigo o uso da surpresa e do monitoramento; impedir que ele interfira, de modo decisivo, em nossas operações; e restringir-lhe a liberdade de ação nos ataques a pontos sensíveis de nosso território ou de nossas forças". (BRASIL, 2007).

[54] Economia de Forças ou de Meios: "Princípio que se caracteriza pelo uso econômico das forças e pela distribuição e emprego judiciosos dos meios disponíveis para a obtenção do esforço máximo nos locais e ocasiões decisivos". (BRASIL, 2007).

[55] Massa: "Princípio que compreende a aplicação de forças superiores às do inimigo, em termos de quantidade, qualidade e eficiência, em um ponto decisivo, no tempo devido, com capacidade para sustentar esse esforço, enquanto necessário". (BRASIL, 2007).

[56] Manobra: "Princípio que se caracteriza pela capacidade de movimentar forças de forma eficaz e rápida de uma posição para outra, contribuindo para obter superioridade, aproveitar o êxito alcançado e preservar a liberdade de ação, bem como para reduzir as próprias vulnerabilidades". (BRASIL, 2007).

[57] Moral: "Princípio que define o estado de ânimo ou atitude mental de um indivíduo, ou de um grupo de indivíduos, que se reflete na conduta da tropa". (BRASIL, 2007).

[58] Exploração: "Princípio caracterizado pela intensificação das ações ofensivas para ampliar o êxito inicial, sempre que for obtido um sucesso estratégico ou tático, ou houver evolução favorável na situação". (BRASIL, 2007).

[59] Prontidão: "Princípio que se define como a capacidade de pronto atendimento das forças armadas para fazer face às situações que podem ocorrer em ambiente de combate". (BRASIL, 2007).

[60] Unidade de Comando: "Princípio que é caracterizado pela atribuição da autoridade a uma só pessoa, ou seja, à pessoa do comandante". (BRASIL, 2007).

inicialmente com o Estado traçando um objetivo claro na sua atuação, levando a ação bélica ao inimigo quando se mostrar estritamente necessário. A sua organização e determinações de comando devem ser simples, para serem bem entendidas e executadas, sendo que o momento de agir e as estratégias tomadas devem ser uma surpresa para o inimigo. Todas essas ações devem preconizar a segurança dos agentes militares e do próprio Estado. Além disso, deve-se buscar uma economia de forças ou de meios para a obtenção dos resultados, ou seja, gasto mínimo com resultados máximos. O sucesso depende do emprego de forças mais potentes que a do inimigo (massa) com a aplicação de manobras bem estudadas.

A atitude das tropas deve ser de moral elevado, em prol da defesa dos interesses do Estado com a exploração de ações ofensivas inicialmente chocantes, se for necessário. Também, as forças armadas devem estar em prontidão para atender às necessidades do Estado, sempre com uma unidade de comando, para que se evite a pulverização de forças. Esses princípios se aplicam a toda estratégia de defesa do Brasil no âmbito internacional e consequentemente à sua atuação nas interações no ciberespaço.

As infraestruturas em rede dos sistemas de defesa dos Estados são os alvos principais para ataques cibernéticos. Não se fala mais em estudar estratégias e táticas de guerra de um Estado para buscar entender quais são suas intenções. Na contemporaneidade, o que se ganha com o aparato tecnológico para traçar o sistema de defesa, militar e de organização do Estado, se torna também uma fragilidade diante da possibilidade dos outros atores invadirem os sistemas. O estudo e a busca de avanços cibernéticos são importantes para o Estado e para a sociedade internacional, em especial para aqueles que querem preservar suas informações em sigilo. A capacidade de se sustentar, no cenário internacional, como um verdadeiro sujeito de direitos define-se pela possibilidade de se estabelecer de forma inteligente a utilização de forças, negociações, armas, equipamentos e recursos, sendo tudo controlado por rede de computadores. (ANDRESS; WINTERFELD, 2011, p.398).

5.1 Ameaças no ciberespaço: cibervandalismo, crimes na internet, espionagem cibernética, ciberterrorismo e guerra cibernética

O desenvolvimento de novas tecnologias causa inúmeros impactos na sociedade, em especial na capacidade dessa coletividade manter a sua ordem interna e externa. O avanço da tecnologia e o estabelecimento de relações no ciberespaço fazem com que essas novas mudanças do cenário das relações humanas possam ser utilizadas tanto para a melhoria da ordem, como para o aumento da desordem dos sistemas já existentes. O desafio está na falta de barreiras físicas do ciberespaço, uma vez que as ações de desordem e os crimes cometidos podem ser realizados por qualquer pessoa, entidade ou coletividade, de qualquer lugar do mundo para produzir prejuízos em qualquer Estado. Ocorre, portanto, uma crise de tipificação legal dessas condutas, pois as categorias legais apresentam-se inadequadas diante da falta de territorialidade dos crimes cometidos. (BRENNER, 2009, p.288).

Os problemas são também orçamentários. As relações estabelecidas em redes de computadores estão sujeitas a mudanças constantes, pois não basta aprender como utilizar um computador hoje e nunca mais se atualizar, ou seja, há uma curva de aprendizagem essencialmente contínua para a tecnologia cibernética. Essa constante evolução e modificação dos sistemas exige que na investigação de crimes cibernéticos haja um investimento constante do Estado, para viabilizar a aplicação da lei e o treinamento de seus agentes. Isso também significa que todos os atores, que se utilizam da tecnologia de computador, devem ter os recursos para continuar a atualizar o software[61] e hardware[62] que lhes são necessários. Portanto, a lei encontra dois obstáculos importantes: a necessidade de grandes gastos financeiros para atualização da tecnologia de hardware e software em prol da investigação criminosa e o investimento em treinamento daqueles responsáveis pelas investigações. (BRENNER, 2009, p.326).

Os efeitos dessas dificuldades são reforçados pelas características de incerteza das ameaças que vêm do ciberespaço, dos mais diversos atores

[61] "Software é uma sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. Também pode ser definido como os programas que comandam o funcionamento de um computador". (MARTINS, 2015).

[62] "O hardware é toda a parte física que constitui o computador, por exemplo, a CPU, a memória e os dispositivos de entrada e saída". (MARTINS, 2015).

internacionais. O ciberespaço permite que a ação de ataque de Estados, criminosos e terroristas parta de qualquer ponto do globo e a identidade do ator dificilmente é descoberta.

O ciberespaço, portanto, aumenta significativamente a complexidade das interações das relações internacionais e, em especial, dos desafios jurisdicionais de investigação da aplicação da lei, seja no âmbito nacional ou internacional. Buscar entender a aplicação do direito nesse cenário de relações sistêmicas e dinâmicas é primeiro compreender as formas possíveis de ameaças cibernéticas existentes.

É cada vez mais difícil categorizar ameaças cibernéticas e ciberataques, levando-se em consideração somente os atores envolvidos, como se fazia na teoria clássica de guerra entre Estados do Direito Internacional. Não é possível partir do que se conhece da doutrina jurídica internacional para definir a diferenciação entre um crime cibernético e uma ação de guerra cibernética. Entretanto, o elemento axiológico do agente ao realizar o ataque é fundamental para a distinção dos diferentes atos de ameaça cibernética realizados no ciberespaço. (CAVELTY, 2011, p.1).

A primeira ameaça existente é a do chamado ciberhacktivismo ou cibervandalismo que envolve a atuação de um agente que busca chamar a atenção da sociedade por meio da modificação ou vandalização de websites ou sistemas de computador. (CAVELTY, 2011, p.1). Em novembro de 2012, por exemplo, hackers atacaram a página do google Paquistão e substituíram o logotipo por uma imagem de dois pinguins que andam em uma ponte ao pôr do sol, uma mensagem em turco e a frase “Paquistão abatido”, em inglês. (BALOCH, 2014).

O cibervandalismo é a forma mais comum de ameaça, por possuir uma grande atenção pública e ser de livre acesso àqueles que tiverem o conhecimento tecnológico. Os efeitos são pouco significativos diante da dinâmica da sociedade internacional, pois são facilmente revertidos e servem somente para chamar a atenção da opinião pública.

Em um segundo nível, estão os crimes de Internet e a espionagem cibernética, que consistem em uma tentativa de obtenção de informações por meio digital. Esses ataques são ocorrências rotineiras no âmbito das relações nacionais e internacionais, em especial quando se trata de espionagem industrial, tipificando-se como ilegais, na maioria dos casos. Pode-se fazer uma pesquisa pública de

dados, o que não se caracterizaria como uma espionagem ilegal, mas a partir do momento que a pesquisa adentra o ambiente privado e restrito, torna-se um ato ilegal e passível de punição. (EZEKIEL, 2013, p.652).

O dicionário da Universidade de Oxford alerta para a existência da espionagem cibernética no âmbito das relações internacionais interestatais quando a define como “o uso de redes de computadores para obter acesso ilícito a informações confidenciais, guardadas por um governo ou outra organização”. (UNIVERSIDADE DE OXFORD, 2014). Existem inúmeros exemplos de espionagem cibernética realizadas no mundo, como o caso de espionagem da Petrobrás realizada pela Agência de Segurança Nacional dos EUA e descoberto pelo governo brasileiro em setembro de 2013.

Outro tipo de ameaça cibernética é o ciberterrorismo que consiste basicamente na utilização da tecnologia cibernética para a prática de atos terroristas. O ciberterrorismo viabiliza o ataque por agentes não estatais contra computadores, redes e sistemas com o objetivo de intimidar e causar terror na população civil. A tipificação do ciberterrorismo depende da concretização da violência física contra pessoas ou propriedades ou a consequência de um medo extremo da população. (ENGHELBERG, 2012, p.201).[63]

O uso de redes de computadores para desestabilizar, degradar ou até mesmo destruir informações alocadas em outras redes caracteriza o ataque cibernético. Define-se o ataque como cibernético pelo fato, tanto das armas quanto dos alvos,

[63] Exemplo de ciberterrorismo ocorreu, em 24 de novembro de 2014, quando os computadores da Sony Pictures, assim que foram iniciados, apresentaram mensagem na tela dizendo que tinham sido hackeados por um grupo que se autodenomina guardiões da paz (GOP). A violação maciça resultou no vazamento de dezenas de milhares de documentos, incluindo e-mails confidenciais e informações pessoais.
Os GOP também prometeram um "destino amargo" e advertiram os cinéfilos para "manterem-se distantes" dos cinemas que estiverem passando o filme “Entrevista”, invocando lembranças dos ataques do 11 de setembro de 2001. Trata-se de uma comédia que conta a história de dois jornalistas frustrados recrutados pela Agência Central de Inteligência (CIA) para assassinar Kim Jong-un, líder fictício norte-coreano. Em junho de 2014, a Coreia do Norte considerou o enredo do filme, de um "ato de guerra" e mais tarde elogiou a pirataria como uma "escritura de justiça".
A Sony que tinha agendado lançar o filme no Natal de 2014, desistiu de fazê-lo. O ataque causou dezenas de milhões de dólares em danos aos computadores da Sony Pictures, ao destruir arquivos valiosos, vazar cinco filmes, e informações pessoais de mais de 47.000 (quarenta e sete mil) pessoas que trabalharam na companhia. O presidente Barack Obama prometeu responder "proporcionalmente" ao que chamou de "cibervandalismo", depois que o Federal Bureau of Investigation (FBI) atribuiu a culpa à Coreia do Norte. Dirigindo sua conferência anual de notícias, de final de ano, na Casa Branca, Obama disse Sony "cometeu um erro" em cancelar o lançamento do filme e que "não podemos ter uma sociedade na qual um ditador de um lugar pode começar a impor censura aqui". A Coreia do Norte respondeu afirmando que não está envolvida no ataque cibernético e que afirmações dos EUA foram uma "difamação infundada". (IANS, 2014).

estarem presentes no ciberespaço. Esses ataques, em regra, se utilizam de códigos para produção de danos e os efeitos são os mais diversos possíveis.

O caso mais sério de ataques no ciberespaço é o da guerra cibernética que estabelece conflitos de guerra com consequências de violação de informações dos sistemas de defesa dos Estados e até mesmo consequências reais de uma guerra física. A guerra cibernética se refere é uma guerra de informação e tecnologia, na qual os atores buscam se utilizar de todas as outras formas de ataque, em prol de seus interesses na sociedade internacional.

ILUSTRAÇÃO 4 – Potencialidade dos conflitos no ciberespaço

Fonte: CAVELTY, 2011, p.2, tradução nossa.

O termo guerra cibernética se refere a um conflito bélico no ciberespaço que envolve principalmente a arma de tecnologia da informação para disputa de interesses. O objetivo é, por meio do acesso a informações privilegiadas e secretas, buscar descobrir quais são as estratégias de guerra do inimigo, em prol da possibilidade de influenciar as suas decisões políticas e a forma como ele se utiliza de suas forças armadas.

Além desse aspecto estatal, há a possibilidade de se influenciar a atitude das populações, por meio do acesso a informações privadas. A guerra cibernética é um reflexo da utilização da tecnologia da informação em todos os setores de gestão das relações estatais, em especial no setor militar, e da computadorização das relações públicas e privadas. (CAVELTY, 2011, p.2).

Diante dessa nova realidade, os Estados desenvolvem três atividades de sobrevivência nas operações de computadores em rede: ação de ataques de rede de computadores (ofensiva), de exploração (ofensiva para obtenção de vantagens reais) e de defesa (defensiva, para evitar ataques). A potencialidade de danos que podem ser

causados por uma guerra cibernética é enorme e, por mais que se imagine que uma guerra virtual pudesse ter menos perdas de vidas, raramente pode-se imaginar uma guerra que ocorra exclusivamente no âmbito do ciberespaço e que não tenha consequências reais. (CAVELTY, 2011, p.2).[64]

Drones são veículos aéreos não tripulados, ou seja, aviões controlados por pilotos que ficam em solo, ou até mesmo não pilotados, pois alguns possuem tecnologia para voar determinada rota autônoma de uma missão pré-programada. Alguns drones são utilizados para fins de reconhecimento e vigilância, em uma espécie de espionagem, e, outros, são armados com mísseis e bombas para um ataque ostensivo. **Os bombardeios realizados por drones são a efetivação da utilização da cibernética, para a produção de efeitos reais, em um ataque de guerra que é ao mesmo tempo cibernético e real**. (ZENKO, 2012, p.3).

Essa nova prática de ataques por meio da utilização de drones leva a uma impossibilidade de perdas de vidas nacionais, pois os militares permanecem em solo nacional, sem qualquer perigo real. Entretanto, quando se analisa a questão da conscientização dos efeitos da guerra a ação de drones é temerosa, pois o soldado não vê mais seu inimigo de frente, ao perder uma vida, vê apenas um ponto ou vários pontos de calor se apagando. Hoje, cada vez mais, a guerra se dá por intermédio da tecnologia e da cultura, ao vincular, desde a infância, a guerra e a morte por meio de jogos de vídeo games. Isto faz com que o homem perca a noção de que vidas estão sendo perdidas, na distância física da tecnologia.[65]

---

[64] Apesar de não restarem dúvidas do desenvolvimento tecnológico dos Estados, para utilização como recurso contra outros Estados, ainda é muito complexo determinar a extensão dessa evolução. Essa dificuldade se deve à impossibilidade de se medir a quantidade de armas cibernéticas, como se fazia em outros domínios de guerra.
Exemplo contundente de utilização de um ataque cibernético ocorreu na invasão do Iraque em 2003, quando o governo dos EUA foi acusado de ter desligado as redes de telefones celulares locais e de computadores, com o objetivo de evitar uma articulação de resistência insurgente. (CAVELTY, 2011, p.2). Outro exemplo, ocorreu após o início da guerra quando os EUA confirmaram o uso de “drones” no Iraque e no Afeganistão.

[65] Com o objetivo de ilustrar essa realidade deve-se examinar o caso do jogo “America’s Army”, traduzido como “Exército dos EUA”. O jogo em questão está disponível gratuitamente, para download, na Internet e foi desenvolvido pelo exército estadunidense, como um dos jogos militares mais tecnologicamente avançados da atualidade. Seus objetivos são bastante simples. Os indivíduos são obrigados primeiro a passar por um treinamento básico, no qual praticam pontaria e aprendem os princípios básicos da doutrina do exército. Após o treinamento, passam a fazer parte de uma missão para defender uma estação de bombeamento de petróleo do Alasca, de um ataque terrorista. O grande objetivo é utilizar o jogo como uma ferramenta de recrutamento e de publicidade do exército estadunidense, sendo esses os motivos que o fazem estar disponível para download gratuito. O jogo coloca como meta comandar dois grupos de soldados contra um ditador cruel do país fictício do “Zakistão”. Após tentativas de negociações na ONU não lograrem êxito, com a ajuda da Organização do Tratado do Atlântico Norte (OTAN),

O jogo ‘Exército dos EUA’, exemplo clássico de utilização da cibernética como arma de recrutamento de guerra e criação de uma ideologia militarizada, baseia-se na exacerbação do nacionalismo e no estabelecimento de uma ficção para o ambiente de guerrilha.

Pela mensagem inicial do jogo compreende-se, a sua função, na criação de uma ideologia e recrutamento de jovens, que serão os futuros soldados cibernéticos.

> Eu sou um soldado americano.
> Eu sou um guerreiro e um membro de uma equipe.
> Eu sirvo ao povo dos Estados Unidos e vivo os valores do exército.
> Eu vou sempre colocar em primeiro lugar a missão.
> Eu nunca vou aceitar a derrota.
> Eu nunca vou desistir.
> Eu nunca vou deixar um companheiro caído.
> Sou disciplinado, fisicamente e mentalmente forte, treinado e proficiente em minhas tarefas de guerreiro e testes.
> Eu sempre preservo meus braços, meu equipamento e eu.
> Eu sou um especialista e eu sou um profissional.
> Eu estou pronto para implantar, engajar e destruir os inimigos dos Estados Unidos da América no combate físico.
> Eu sou um guardião da liberdade e do modo de vida americano.
> Eu sou um soldado americano. (EXÉRCITO DOS EUA, 2002, tradução nossa).[66]

Apesar de o exército admitir que o jogo ‘Exército dos EUA’ é uma forma de recrutamento, no site do jogo afirma-se ser somente uma "estratégia de comunicação" que "fornece insights virtuais sobre o exército”, fazendo com que crianças, adolescente e seus pais não tenham ideia da intenção dos jogos. Exemplos como esses, dos drones e dos jogos, dão uma ideia inicial sobre a forma

---

resolvem invadir o país. A ideia é misturar realidade com ficção de forma manipulável, pois em todas as invasões os soldados nunca encontram nenhuma criança, idosos ou mulheres, apenas soldados inimigos. (LUGO, 2006, p. 12-13).

[66] I am an American Soldier.
I am a Warrior and a member of a team.
I serve the people of the United States and live the Army Values.
I will always place the mission first.
I will never accept defeat.
I will never quit.
I will never leave a fallen comrade.
I am disciplined, physically and mentally tough, trained and proficient in my warrior tasks and drills.
I always maintain my arms, my equipment and myself.
I am an expert and I am a professional.
I stand ready to deploy, engage, and destroy the enemies of the United States of America in close combat.
I am a guardian of freedom and the American way of life.
I am an American Soldier. (EXÉRCITO DOS EUA, 2002).

como a tecnologia vem sendo utilizada como arma de guerra, mesmo que pareça uma ação positiva de reafirmação nacional.

Apesar de ter ratificado, em 2002, o “Protocolo Facultativo à Convenção sobre os Direitos da Criança Relativo à Participação de Crianças em Conflitos Armados” desenvolvido na Assembleia Geral da ONU e o transformado em lei federal, os Estados Unidos têm praticado o recrutamento de crianças, tendo como contundente exemplo o jogo ‘Exército dos EUA’. (ONU, 2002).

A estratégia do exército estadunidense de recrutamento infantil é plantar, desde cedo na cabeça das crianças, a ideologia da guerra e da luta nacionalista pelo exército estadunidense. A tática mais ousada foi criar o polêmico ‘Army Experience Center’, em tradução literal, ‘Centro de Experiência do Exército’, no shopping de Franklin Mills, não muito longe do centro da Filadélfia, local improvável para o exército buscar novos recrutas, mas ideal para encontrar jovens a serem incentivados a participar da guerra. (MCLEROY, 2015).[67]

Inicialmente, quando o centro foi aberto, o exército afirmava que a intenção não era recrutar jovens para o exército, mas mudar a percepção da guerra. O slogan do centro era “O exército é mais do que você pensa que é” e militares do exército, à paisana, vestidos com camisas polo pretas, eram responsáveis por viabilizar um tour no centro com os jovens interessados. (MCLEROY, 2015).

Durante os seus dois anos de funcionamento, mais de quarenta mil pessoas visitaram o ‘Centro de Experiência do Exército’ e utilizaram o simulador Humvee e de Black Hawk (helicóptero médio bimotor de transporte utilitário e assalto), além de jogarem os jogos de vídeo game e empregarem da tecnologia de touch screen para aprender sobre o exército.

O Centro foi fechado, em julho de 2010, e os ativistas pacificadores, que protestavam contra a sua abertura desde o início, viram o seu fechamento como uma vitória da causa. Entretanto, o exército estadunidense afirma que o fechamento ocorreu devido à mudanças do mercado de trabalho estadunidense. (ROSE, 2015).

[67] O “Centro de Experiência do Exército” consistia em um verdadeiro simulador de treinamento militar, com helicóptero que se utilizava do mais alto grau de tecnologia e simuladores de Humvee (Veículo de rodas multiuso de alta mobilidade) que custam milhões de dólares. Desde o início do seu funcionamento, em agosto de 2008, ocorreram protestos diários contra a sua abertura e funcionamento. (MCLEROY, 2015).

Quando foram elaborados planos para o ‘Centro de Experiência do Exército’, em 2007, as guerras no Iraque e no Afeganistão radicalizaram, a economia foi crescendo e o exército tinha dificuldade de cumprir suas metas de recrutamento, o que não ocorre mais com a crise laboral. (ROSE, 2015).

Na atualidade, o exército dos Estados Unidos tem duas novas táticas de recrutamento: a primeira é a colocação de recrutadores em escolas de ensino médio, com o intuito de iniciar um trabalho de manipulação ideológica dos jovens a partir dos 14 anos, para que, quando ele estiver com a idade adequada, possa ser devidamente aproveitado. A outra tática, que ainda está para ser totalmente aprovada, é a possibilidade de reconsideração dos requisitos de força física para participar do exército, visando a criação de um grupo de ‘ciber guerreiros’ mais habilitado, com o slogan de que “A ameaça está apenas a um click de distância”. Esse recrutamento cibernético já acontece, o único passo que falta para se efetivar o novo conceito de ‘ciber guerreiros’ é fazer com que os requisitos de força física não sejam mais exigidos deles.

ILUSTRAÇÃO 5 – Folder de divulgação de recrutamento de guerreiros cibernéticos do exército estadunidense

Fonte: ESTADOS UNIDOS DA AMÉRICA, 2015, tradução nossa.[68]

[68] Tradução dos dizeres do Folder de divulgação de recrutamento de guerreiros cibernéticos do exército estadunidense: “Ciber Guerreiros: A ameaça está apenas a um click de distância”. “Torne-

A nova realidade, de existência de uma guerra constante no ciberespaço, faz com que os Estados se movimentem para a preparação de enfrentamento dos inimigos nesse novo domínio. O caso dos Estados Unidos, aqui citado, é um indício da nova realidade da guerra cibernética, que os sujeitos de Direito Internacional são obrigados a enfrentar. Além dos questionamentos éticos suscitados pelo Direito Internacional e pelas teorias das relações internacionais, deve-se atentar que esse novo domínio, não limitado por regras físicas, mas somente virtuais, apresenta-se como um desafio para as relações interestatais.

5.2 As ações de guerra por meio eletrônico e a soberania no ciberespaço

O desenvolvimento e implantação de novas tecnologias fazem com que o seu potencial ofensivo se apresente como um novo ponto de tensão nas relações pacíficas entre Estados. As vulnerabilidades criadas pela informatização da administração pública e das táticas militares levantam questões sobre o que seria uma ação cibernética legal e o que seria uma conduta inadmissível.

Ataques militares são geralmente ilegais, com exceção da legítima defesa ou quando autorizados pelo Conselho de Segurança da ONU. A grande questão, que se apresenta diante da cibernética, é a análise de como caracterizar ações de guerra no ciberespaço e a violação da soberania dos Estados, por meio eletrônico. Será que o ciberespaço está além dos limites da soberania dos Estados?

A rápida evolução tecnológica e a criação do domínio do ciberespaço têm impactado sobre quase todos os aspectos da vida humana. A relação de complexidade das relações internacionais, com a possibilidade de multiplicação de interações em rede entre os mais diversos atores internacionais, modificou o modo de vida dos homens e, consequentemente, a organização dos Estados. Se por um lado, a possibilidade de novas interações é uma perspectiva positiva para a união de indivíduos e povos, essa mesma tecnologia pode ser utilizada como arma de

---

se um membro de força altamente técnica e qualificada para satisfazer os requisitos de rede de computador e outras operações de computador. Estar na linha da frente para lidar com os tipos de tecnologia da informação e ciberameaças a rede de computador que enfrentamos no século XXI como uma Rede de Técnica Criptológica (CTN). Para mais informações visite navy.com". (ESTADOS UNIDOS DA AMÉRICA, 2015, tradução nossa).

guerra. O aumento de interações no âmbito internacional, no ciberespaço, representa um número crescente de desafios à segurança individual e coletiva.

Para Marshall McLuhan (1911–1980) “Nos tornamos o que nós criamos. Nós moldamos nossas ferramentas e daí em diante, nossas ferramentas nos moldam”. (MCLUHAN, 1964, p.32, tradução nossa).[69] A revolução da informação está mudando fundamentalmente sociedades. O crescimento dramático em tecnologias de computação e comunicação está transformando a natureza dos governos e a vivência da soberania no âmbito internacional, em especial, pelo aumento do papel dos atores não-estatais e pela importância do ‘cyber power’ na condução das políticas estrangeiras.

Pode-se ir mais longe e entender que a mudança no modo de comunicação tem tido um efeito substancial na distribuição de poder dentro da sociedade, na evolução social como um todo e sobre os valores e crenças que sustentam hoje o direito do Estado e o Direito Internacional.

As infraestruturas nacionais críticas, que dependem de redes de computadores, tornam-se cada vez mais vulneráveis a ataques cibernéticos. As relações interativas no ciberespaço e a ameaça da guerra cibernética, em particular, colocam pressão sobre as noções tradicionais de soberania, ao desafiar os Estados na aplicação da lei, para as operações cibernéticas, durante o conflito armado internacional. Com as capacidades cibernéticas, acentuam os níveis relacionais tanto das relações com sujeitos de Direito Internacional, como com atores não estatais, o princípio da soberania recebe o papel de fornecer clareza na imputabilidade de atores e caracterização de ações. (JENSEN, 2011, p.1).

Os ataques cibernéticos representam novas formas de se intrometer nas prerrogativas soberanas dos Estados. A lei tem lutado para manter o ritmo com a tecnologia. Tentativas recentes de identificar a aplicação do Direito Internacional na guerra cibernética são importantes, entretanto, muitas vezes, utiliza-se de uma doutrina limitada que não se encaixa na nova realidade ilimitada do ciberespaço.

Segundo Mário Lúcio Quintão Soares, a ideia de soberania absoluta é, em muitos aspectos, um conceito ultrapassado no Direito Internacional contemporâneo e existem vários fatores que contribuem para sua erosão. Como resultado da globalização, especialmente, há uma tendência crescente de interdependência e

[69] “We become what we behold. We shape our tools and thereafter our tools shape us”. (MCLUHAN, 1964, p.32).

cooperação entre os Estados. (QUINTÃO SOARES, 2008, p.95). Entretanto, a análise dos conceitos de soberania tradicionais são importantes para compreender o que se pode aproveitar desses conceitos e o que precisa ser repensado.

Na atualidade, existem quatro conceitos de soberania comumente usados no Direito Internacional. A primeira é a soberania nacional ou interna, que refere-se à organização de autoridade política dentro de um Estado e a capacidade de controle das relações internas. A segunda é a chamada soberania de interdependência, que se preocupa com a questão da capacidade de controle e decisão do Estado dos movimentos de integração que deseja tomar parte, como, por exemplo, integrar blocos econômicos. A terceira é a chamada de soberania jurídica internacional, que se preocupa com o estabelecimento do status ao Estado de uma entidade política, independente, no sistema internacional. Por fim, tem-se, ainda, a tradicional soberania de Westfália, entendida como um instituto estatal com o objetivo de organizar a vida política baseando-se na territorialidade, na exclusão dos fatores externos e no estabelecimento de estruturas de autoridade. (KRASNER, 1999, p.53). O que se percebe é que nenhum desses conceitos sozinho consegue explicar o conceito de soberania no novo paradigma sistêmico exigido pelo ciberespaço.

Luhmann esclarece que sociedades sistêmicas e autopoiéticas são soberanas, ao construírem suas identidades e diferenças. A soberania, no sistema autopoiético, é a possibilidade de utilizar-se das identidades e diferenças para tomar suas próprias decisões. Ou seja, não é possível um sistema estatal importar as identidades e as diferenças do mundo exterior ou de outros Estados. As decisões devem ser tomadas por meio da interação entre povos e instituições estatais, sem a violação desse diálogo democrático. (LUHMANN, 1986, p.42). Na teoria dos sistemas, a permissão da interação e a construção de identidades estatais é o verdadeiro exercício de soberania.

Sistemas sociais usam a comunicação como seu modo particular de vivência autopoiética. Seus elementos são as interações que são produzidas por uma rede de comunicações, agora, com mais facilidade, no ciberespaço. O grande questionamento que resta é: como pode haver respeito à soberania estatal nesse novo ciberespaço interativo?

O desenvolvimento do ciberespaço contou com opiniões divergentes de cientistas e militares desde a sua criação. O militarismo contribuiu com valores de

ordem, alto desempenho, baixo custo, apelo consumerista e simplicidade para o ciberespaço. Entretanto, os cientistas envolvidos trouxeram uma ideia mais democrática e anárquica para o ciberespaço, com valores como a descentralização de autoridade e aberto intercâmbio de informações. (BRATE, 2002, p.198)

Em meados do século XX, os acadêmicos, tais como o educador Herbert McLuhan, visualizaram a tecnologia e a interligação, que foi possível através de meios eletrônicos, como um meio de criar uma ‘aldeia global’. O sonho era ainda maior, alguns cientistas acreditavam que a evolução da tecnologia levaria também à evolução da psique humana. (BRATE, 2002, p.198)

O aumento das relações interativas entre os seres humanos e a facilidade de acesso à informação, levaria a humanidade a um nível elevado de inteligência, impossível até então de ser alcançado. Quanto mais a informação é compartilhada, a sociedade se torna mais livre e com um maior potencial de cooperação. Os cientistas acreditavam que esse ideal de liberdade do ciberespaço só seria alcançado se corporações e empresas não pudessem controlá-lo. (BRATE, 2002, p.198)

Abbie Hoffman (1936–1989) defendia que a "liberdade de imprensa pertence àqueles que possuem o sistema de distribuição." (HOFFMAN, 2005, p.71). Sendo assim, a informação só seria verdadeiramente compartilhada e livre, sem a influência estatal ou coorporativa. A crença que o ciberespaço deve ser livre de governo ou de interferência empresarial, levou à ideia de que o ciberespaço é, na verdade, imune à soberania dos Estados.

Apesar da tentativa idealista de se manter um ciberespaço vocacionado para a troca livre de informações, mantém-se os desafios à regra de respeito à soberania dos Estados. Percebe-se a necessidade de se regular punitivamente a ação daqueles que praticavam crimes nesse novo domínio. Além disso, nas relações interestatais, torna-se indispensável a manutenção da não-beligerância virtual, como uma doutrina legal, obrigatória, do Direito Internacional. A utilização desse preceito, pautado na neutralidade e respeito soberano dos Estados, faz-se útil para se determinar os limites da ação no âmbito cibernético, ao determinar as ações legais ou ilegais.

Mesmo com o ciberespaço, como um ‘território transnacional’ ou até mesmo como um local não dotado de nacionalidade, abertamente democrático, os Estados demonstram claramente suas preocupações em regulá-lo, pois não estão imunes

de soberania territorial, nem do exercício da jurisdição dos Estados. Prova disso é que os Estados têm exercido jurisdição penal sobre cibercrimes e regulado inúmeras atividades no ciberespaço.

Cinco razões são apontadas pelo Tenente Coronel Patrick W. Franzese da Universidade de Washington para provar a existência e a necessidade da presença da soberania no ciberespaço. A primeira razão é que uma entidade estatal deve controlar as atividades criminosas praticadas no ciberespaço, para que possa existir e funcionar de forma adequada e legítima; até porque os crimes cibernéticos, na maioria das vezes, possuem consequências reais que repercutem nos territórios estatais. Além disso, o ciberespaço para ser acessível requer uma estrutura física, porque sem ela, os usuários não teriam acesso a ele. Essa estrutura, no entanto, é por via terrestre com base na estrutura e lei dos territórios estatais. Aliás, há ainda a "Corporação da Internet para Atribuição de Nomes e Números" com a sigla em inglês de "ICANN" responsável por monitorar as relações na internet, como, por exemplo, atribuir nomes de domínio e números de endereços de IP (IP adresses)[70] aos computadores e dispositivos que usem a rede. (FRANZESE, 2015, p.10).

A terceira razão para a existência da soberania, no ciberespaço, apontada por Franzese está no fato de que, com o aumento das relações virtuais entre indivíduos que se submetem à legislação de um Estado, há a necessidade de uma regulação legal e fiscalização dessas relações. Tratando-se, por exemplo, das relações financeiras no ciberespaço, é necessário o estabelecimento de leis que possam reger essas transações. Se o ciberespaço fosse imune à soberania dos Estados, qualquer relação financeira estabelecida nele seria extremamente temerária, pois não gozaria de garantias jurídicas. (FRANZESE, 2015, p.12).

A quarta razão está no fato de que o conteúdo das informações enviadas através do ciberespaço detém importância no mundo 'real'. Por exemplo, o conteúdo de propagação da pornografia infantil e da pedofilia na internet é divulgado somente no mundo virtual, mas acarreta consequências jurídicas reais de grande preocupação para os Estados soberanos. Nesse caso, o Estado onde o dano foi ocasionado é responsável pela aplicação da lei punitiva que cabe em sua jurisdição territorial, de forma soberana. (FRANZESE, 2015, p.13).

---

[70] Endereço IP é uma identificação em números de um dispositivo em uma rede local ou pública. Cada computador na Internet possui um IP (Internet Protocol ou Protocolo de Internet) único, que é o meio em que as máquinas usam para se comunicarem na Internet. (PISA, 2005).

A quinta razão, mais ligada às relações internacionais, quando se percebe cada vez mais necessário para os Estados estarem presentes no ciberespaço para fazer valer seus direitos na sociedade internacional. A utilização da tecnologia cibernética é uma das principais opções feitas pelos Estados na organização de infraestrutura e operações de defesa nacional, o que faz com que esse ponto forte seja também uma questão arriscada, pois exige o cuidado no estabelecimento de táticas de defesa dos Estado no âmbito cibernético. (FRANZESE, 2015, p.13-14). Essa opção tem deixado muitos Estados, inclusive o Brasil, cada vez mais vulnerável.

Assim, a utilização do princípio da soberania, como sustentáculo do sistema internacional, ainda se aplica nas relações travadas no ciberespaço. Entende-se que a maioria dos princípios e regras de Direito Internacional devem ser mantidos, mas que, evidentemente, a interpretação desses institutos precisa se adaptar à nova realidade.

A soberania, com seu componente territorial, tem provado ser um princípio eficaz e organizador da sociedade internacional que pode ser aplicado ao ciberespaço sem grandes transformações. A condição para que haja respeito à soberania dos Estados está na própria cooperação entre os atores internacionais, que devem respeitar as normas internacionais e não agir somente a favor da luta pelo poder.

5.3 O ataque cibernético como ‘uso de força’ na sociedade internacional

As definições e atores que podem realizar um ataque cibernético são os mais variados possíveis. Ataques cibernéticos podem ser vistos de forma geral como atividades hostis que podem ser realizadas no ciberespaço contra alguém, seja uma pessoa física, jurídica ou um Estado. Essas atividades englobam a colocação de vírus maliciosos em um computador, desconfiguração de websites, espionagem industrial ou militar, destruição em grande escala de infraestruturas militares, dentre outras.

O ataque cibernético realmente seria de ‘uso de força’ na sociedade internacional? Ao tratar deste ataque cibernético, requer-se um entendimento

apurado da legislação internacional e da interpretação adequada ao ‘uso de força’ na contemporaneidade.

A regulação do ‘uso de força’ deve ser interpretada a partir da leitura do artigo 2º,item 4[71], da Carta das Nações Unidas, ou seja, os membros da ONU devem evitar o uso da ameaça ou força nas relações internacionais, resguardando esse direito somente nos casos do artigo 51[72], ou seja, na legítima defesa individual ou coletiva. (ONU, 1945). O uso de força coloca-se como uma exceção extrema no Direito Internacional, uma vez que objetiva solucionar as controvérsias entre os Estados, de forma pacífica, como preconiza os princípios da Carta da ONU.

Nas relações internacionais, no ciberespaço, questiona-se se um ataque cibernético constituiria ‘uso de força’, vedado, conforme o artigo 2º da Carta das Nações Unidas. Discute-se, também, se um ataque cibernético daria o direito ao Estado atacado de se defender utilizando-se da força, como preconizado pelo artigo 51 da Carta da ONU.

A grande dificuldade é mensurar a ‘força’ empregada no ciberespaço que justifique uma ação de legítima defesa. A resposta para essa pergunta está no teor da interpretação da expressão ‘uso de força’, que possui três análises distintas, segundo Matthew C. Waxman (1972 –). Waxman classifica a força em: ‘força como violência armada’, ‘força como coerção’ e ‘força como interferência’. (WAXMAN, 2015).

O conceito mais utilizado é o de ‘força como violência armada’, ou seja, para que se caracterize uma ação passível de legítima defesa faz-se necessário o emprego de violência física armada. Os adeptos dessa concepção consideram que a proibição do artigo 2º e a autorização de legítima defesa da Carta da ONU, só se

---

[71] “Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso de força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas”. (ONU, 1945, grifo nosso).

[72] “Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos Membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais”. (ONU, 1945).

aplicam nos casos de ataque militar ou de violência armada entre Estados. (WAXMAN, 2015).

Outras formas de solução de controvérsias, no âmbito internacional, como os embargos, o bloqueio econômico, a represália, a boicotagem, o rompimento de relações diplomáticas e até mesmo o ataque a redes de computadores, não são vistos como ‘uso de força’.

Ian Brownlie (1932–2010) usa, inicialmente, uma definição para o uso de força que exige dois requisitos: o uso de uma arma e o intuito de destruição da vida e propriedade alheias. Há, portanto, em sua concepção primária, a necessidade do uso de uma arma violenta que provoque danos à integridade física do ser humano. Entretanto, exigência conceitual da necessidade de uma arma violenta, foi questionada pelo advento dos ataques químicos e biológicos. (BROWNLIE, 2002, p.565).

Brownlie entende, então, que diante da especificidade das armas biológicas, apesar de não atuarem como os dispositivos tradicionais, a sua utilização deveria ser encarada como um ‘uso de força’, violadora do artigo 2º da Carta da ONU. Para Brownlie, o uso de armas químicas e biológicas realiza-se com o intuito de provocar a destruição de propriedades e da vida humana, característica elementar do uso de força. No progresso de sua análise, Brownlie eleva o conceito além do impacto físico da arma, para uma abordagem mais ampla, voltada para resultados negativos. (BROWNLIE, 2002, p.565-566).

Essa visão axiológica do conceito de ‘uso de força’, coaduna com o pensamento dos que defendem que somente há uso de força, quando o ataque cibernético produz resultados físicos.

Entretanto, a abordagem do uso de força voltada somente para os resultados, gera questionamentos, pois esquece-se de incluir nesses casos a coerção política e econômica, comum no ambiente internacional. Surge, então, como solução, o segundo conceito de ‘uso de força’ intitulado de ‘força como coerção’ que interpreta a Carta da ONU, de forma mais livre. Independente do instrumento usado, se houve coerção, há emprego de força. Força armada é, nessa visão, apenas um instrumento de coerção. (WAXMAN, 2015).

Myers McDougal (1906–1998), em sua obra “O Direito Internacional da guerra: coerção transnacional e mundial da ordem pública”, argumenta que força é meramente um grau de coerção principal e violência uma das escalas da força.

Assim, todas as formas de coerção são colocadas em escalas, como uso de força, e se resolve o problema da caracterização da coerção particular como admissível ou não-autorizada no âmbito internacional. (MCDOUGAL; FELICIANO, 1958, p.771). O ataque cibernético, ao empregar coerção sobre o Estado, seria ilegal nos termos do artigo 2º e justificaria, portanto, o exercício da legítima defesa, de acordo com o artigo 51 da Carta da ONU.

O grande problema dessa interpretação tem sido distinguir as diferentes realidades das relações internacionais, demarcadas por embates e conflitos diplomáticos com medições de interesses; das coerções, que seriam vistas como um 'uso de força' ilegal.

O terceiro conceito que se apresenta é o da 'força como interferência', considerada como ato de violação de direitos soberanos dos Estados. O conceito de força, nesse caso, deve ser associado ao princípio do respeito à soberania dos Estados, para que seja devidamente interpretado, evitando-se interferências indevidas que violem o Direito Internacional. (WAXMAN, 2015). Nessa perspectiva, o ataque cibernético pode ser visto como um ato de força ilegal, no cenário internacional, se violar os direitos e a soberania do Estado atingido.

A maioria dos Estados considera que o Estado pode responder ao ataque cibernético, utilizando-se da força, pautado no princípio de legítima defesa do Direito Internacional. Como as ações cibernéticas produzem prejuízos reais e violam os direitos e a soberania dos Estados a auto-defesa, seriam legalmente exercidas na defesa da integridade estatal. Assim, o ataque cibernético pode ser considerado como 'uso de força ilegal' que venha a desencadear o equivalente ataque armado. Os Estados Unidos, na sua estratégia internacional de 2011, para o ciberespaço, assim consideram:

> Quando garantidos, nós responderemos para atos hostis no ciberespaço, como faríamos para qualquer outra ameaça ao nosso país. Todos os Estados possuem um direito inerente à legítima defesa, e nos reservamos o direito de utilizar todos os meios necessários — diplomático, informativo, militar e econômico — para defender nossa nação, nossos aliados, nossos parceiros e nossos interesses.[73] (ESTADOS UNIDOS DA AMÉRICA, 2011, p.2, tradução nossa).

[73] "When warranted, we will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we reserve the right to use all necessary means—diplomatic, informational, military, and economic—to defend our Nation, our Allies, our partners, and our interests". (ESTADOS UNIDOS DA AMÉRICA, 2011, p.2).

Ao avaliar se um evento no ciberespaço constituiu ou não um ‘uso de força’ ilegal, deve-se avaliar todos os fatores envolvidos, incluindo o ator que o realizou, o seu contexto, os objetivos almejados, o alvo atingido, a localização territorial das consequências, os efeitos e a intenção, dentre outros possíveis problemas.

Não se aceita mais a separação da aplicação das normas de Direito Internacional para os espaços físicos e para o ciberespaço. As normas e princípios existentes devem ser aplicados a esse novo domínio passível de regulação e imputação de responsabilidade jurídica internacional.

6 A LEI DA GUERRA E O ESTADO DE GUERRA CIBERNÉTICA

Georges Abi-Saab (1933–) assevera que as necessidades e a forma de vivência militar são definidas pela evolução da tecnologia e do pensamento estratégico do ser humano. Portanto, se houve uma mudança tecnológica expressiva que fez com o homem modificasse a sua forma de comunicar, pesquisar e pensar, certamente a guerra sofrerá os impactos dessa mudança. Há necessidade de equilíbrio entre as formas objetivas de lidar com a guerra e os requisitos subjetivos da humanidade que as leis devem levar em consideração. (ABI-SAAB, 1984, p.265).

Assim, a maneira como a guerra se realiza reflete a sociedade, na qual ela ocorre, e na forma como essa sociedade tem administrado suas visões sobre a economia, ciência e a comunicação. A contemporânea revolução cibernética aliou-se ao militarismo, pois a própria sociedade modificou sua forma de se relacionar, pensar e produzir riquezas com a evolução da tecnologia.

Embora seja evidente que a tecnologia tem transformado as forças armadas, nos últimos anos, o impacto maior não ocorreu nas forças armadas, mas na forma do homem viver se relacionar interativamente. A revolução militar, na Era Cibernética, ocorre por meio da elevação do número de interações humanas no ciberespaço.

Além disso, a possibilidade de se trabalhar com melhor precisão na guerra, sem a utilização local de militares (utilizando-se de drones, por exemplo) e a junção dos avanços tecnológicos em sistemas de comando e controle, contribuem para a mudança da forma de se fazer guerra na contemporaneidade. Conceitos clássicos como ‘campo de batalha’ tornaram-se obsoletos, pois a abrangência das armas tecnológicas permite que Estados inteiros sejam almejados como campos de batalha, sem limitações físicas.

O propósito da guerra passa por transformações fundamentais. Na guerra do período industrial os objetivos políticos foram alcançados através da realização de objetivos estratégicos militares, que se impunham pela força militar ostensiva. Na Era Cibernética, o uso de força militar bruta realiza-se com mais sutileza, pois outros elementos, como a diplomacia e a exploração da inteligência no ciberespaço, permitem uma articulação mais hábil, na busca dos resultados almejados pelos atores internacionais. (DINNISS, 2012, p.22-23).

A adoção de uma guerra centrada em redes, com uma infraestrutura cibernética, permitiu uma melhor exploração do terreno inimigo, das suas condutas e doutrinas, na elaboração de táticas de guerra. A grande arma da guerra cibernética é a própria espionagem cibernética, que permite ao Estado antecipar os passos de seu inimigo, muitas vezes, sem deixar rastros de sua presença no território do ciberespaço. Entretanto, não pode-se entender que a guerra cibernética seja mais branda.

Talvez, pela extensão do domínio no qual o conflito ocorre e pela habilidade dos atores de esconderem seus efeitos reais, ela tenha a aparência de menos lesiva ao Direito Internacional, mas suas consequências e sua abrangência podem ser ainda mais nefastas. Esse fato pode, inclusive, fazê-la mais violadora de direitos que a própria guerra tradicional, uma vez que os atores, contando com a dificuldade de identificação dos criminosos, acreditam na impunidade e agem, cada vez mais, utilizando-se da força, de forma ilegal, no ciberespaço.

A guerra cibernética apresenta para o Direito Internacional desafios até então não explorados, que envolvem a necessidade de se aprender a lidar com esse novo domínio. A guerra travada no ciberespaço não pode ser analisada, de forma dissociada, da guerra convencional, pois é utilizada como uma nova capacidade de exploração da força, com novas dimensões e, portanto, modifica a forma como a guerra é realizada.

Na guerra cibernética, os elementos físicos, eletrônicos, estratégicos e lógicos de guerra, devem ser considerados fatores extremamente importantes.

Ao se analisar os atuais métodos utilizados na guerra, percebe-se que os Estados optam por atuar no âmbito cibernético, pois o ciberespaço e a luta pelo conhecimento desse domínio, cria um aparato de técnica, força e tática até então não experienciados, em termos de capacidade ofensiva e defensiva maior na guerra.

Uma ideia que tem ganhado adeptos para a regulação das relações internacionais no ciberespaço é a do conceito de ‘controle de armas’ ou ‘restrição de armas’. Na analogia, feita com a época da Guerra Fria, os sujeitos de Direito Internacional compreendiam que a existência de uma guerra nuclear seria prejudicial a todos e causaria uma destruição mútua. Os Estados, com poder nuclear, trabalharam juntos na elaboração de normas que regulassem e limitassem a exploração dessas armas, evitando a guerra.

Outra analogia se faz com o problema enfrentado das armas biológicas, ainda mais parecido com o da guerra cibernética, pois além dos Estados, qualquer um pode ter acesso a uma arma biológica e se tornar uma ameaça.

Os ataques cibernéticos ou a guerra cibernética exigem um grande investimento financeiro, tecnológico e sucessivamente militar. Pelo que não seria de interesse de nenhum ator utilizar-se dessa arma. Todos podem ser alvos de ataques cibernéticos e essa generalidade pode fazer com que, no futuro, se chegue a um denominador comum de regulação do ciberespaço. (ANDRESS; WINTERFELD, 2011, p.465).

Apesar dessa forma positiva de se pensar na sociedade internacional complexa, as demandas, que surgem, não são solucionadas com a guerra cibernética somente pela instituição de tratados que possam regular essas relações, pois no ciberespaço, os Estados não são os únicos atores que podem ameaçar a segurança e praticar a guerra e nem sempre pode-se contar com a boa-fé dos Estados na obediência dos tratados. Os atores não regulados pelo Direito Internacional não podem ser ignorados, pois se apresentam como possíveis partícipes de uma guerra cibernética. A possível solução para a regulação e punição de ataques cibernéticos, realizados por entes privados, não caracterizados como sujeitos de Direito Internacional, como indivíduos e empresas, deveria contar com as jurisdições estatais ou internacionais, dotadas de competência para punir as violações praticadas.

Na complexa realidade atual não é possível se calcular os danos que podem ser causados pela guerra cibernética, mas o Direito Internacional, assim como faz em relação ao controle de armas de destruição em massa, deve regular essas conexões. Não há como restringir as relações conexas em rede no âmbito cibernético, mas há como controlar ou até mesmo proibir o desenvolvimento de armas cibernéticas, hoje já chamadas de 'arma de ruptura em massa'[74]. (ANDRESS; WINTERFELD, 2011, p.472).

Redes de computadores criam novos espaços para atores com intenções maliciosas na sociedade internacional. Tais redes ainda são, e talvez sempre serão, vulneráveis à destruição virtual e real por ataques cibernéticos e físicos, tais como vírus ou bombas, por exemplo. Talvez o maior problema seja o ataque

[74] O termo utilizado em inglês é "weapons of mass disruption". (ANDRESS; WINTERFELD, 2011, p.472).

cibernético, pois as redes de computadores são os alvos de ‘ruptura em massa’. A economia ou a base de defesa de um Estado podem ser seriamente prejudicadas pela guerra cibernética, sob a forma de invasões de computadores ou ciberterroristas, ao redor do mundo.

No passado, as ameaças à segurança ocorriam por meio de ataques físicos contra infraestruturas ou eram ataques em busca de informações. Esses setores eram tratados de forma isolada, como atividades ‘compartimentadas’ e independentes. No século XXI, ataques cibernéticos causam uma verdadeira ruptura da organização social, pois envolvem todos os setores; ou seja, há consequências físicas, econômicas, sociais e militares que se entrelaçam e causam um verdadeiro caos nas relações internacionais.

É exatamente pela facilidade de se destruir os mais diversos setores da sociedade, com um ataque cibernético, e pela dificuldade de se controlar os efeitos de um ataque, que tem se identificado as armas utilizadas (como vírus e invasores), com o nome de ‘armas de ruptura em massa’. (ANDRESS; WINTERFELD, 2011, p.473).

A primeira premissa para se estudar um Direito Internacional regulatório do estado de guerra cibernética, que toda sociedade internacional hoje vive, é entender que embora ataques de rede de computador suscitem questões desafiadoras para as atuais leis de conflito armado, na maior parte, as leis existentes são capazes de se adaptarem à nova tecnologia.

Com efeito, a ‘cláusula Martens’ sugerida por Fyodor Fyodorovich Martens (1845-1909), aplica-se à realidade cibernética atual, pois preconiza a aplicação das leis e costumes de guerra atuais para a solução de demandas ainda não contempladas pelos textos legais dos tratados. (CASSESE, 2005, p.160-161).

> Até que tenha sido emitido um código mais completo das leis da guerra, as altas partes contratantes consideram conveniente declarar que, em casos que não constantes os regulamentos adotados por eles, os habitantes e os beligerantes permanecem sob a proteção e a regra dos princípios da lei das Nações, tal como resultam os usos estabelecidos entre os povos civilizados, das leis da humanidade e os ditames da consciência pública. (HAIA, 1907, tradução nossa). [75]

[75] “Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience”. (GENEBRA, 1977).

Não há um campo de batalha exclusivamente virtual, completamente dissociado da realidade do mundo real, no qual a guerra cibernética ocorra e que justifique a necessidade de uma legislação completamente nova para sua regulação. A guerra ainda é vivida nos espaços físicos, mas também utiliza-se das redes virtuais para se propagar e provocar prejuízos de ruptura em massa.

6.1 A Guerra Cibernética e a Jurisdição Real (não virtual)

Como previamente discutido, alguns cientistas, que idealizaram o ciberespaço, tinham a ilusão anárquica de que este seria dotado de uma completa liberdade interativa, pois não se submeteria a qualquer ente estatal ou coorporativo; seria um território universal.

Apesar do território do ciberespaço ser virtual e seu espaço não possuir características limitadoras físicas, a localização dos atores que interagem no seu espaço é real e física, pois cada ente, seja pessoa física ou jurídica, de direito público ou privado, submete-se à jurisdição de um Estado e possui uma localização geográfica passível de especificação. Esse fator ocasiona consequências jurídicas importantes para se começar a delinear respostas aos desafios da guerra cibernética.

Segundo Sean Kanuck (1968–) a localização física dos atores internacionais e os links que os conectam às vítimas, são de importância central, para que haja uma responsabilização adequada, pelos Estados, dos violadores de direitos por meio do ciberespaço. A força da interação, preconizada pela Era Cibernética, também pode ser utilizada a favor do combate dos crimes virtuais, de forma transnacional, quando necessário. A não limitação física dos atos criminosos exige uma assistência legal mútua a ser instituída com ajuda do Direito Internacional. (KANUCK, 2010, p.1573).

Os componentes de cada informação, que circula no mundo, estão sujeitos aos interesses dos proprietários da infraestrutura que leva a informação, seja uma empresa privada ou um Estado soberano. Não há ambiente virtual sem estrutura física, patrocinada por alguém e instalada no território de algum Estado, que a mantenha. Essa limitação estrutural física determina ligação jurídica fundamental do mundo virtual à jurisdição territorial dos Estados.

Cada fio de cobre, cabo de fibra óptica, torre de retransmissão de microondas, satélite transponder[76], ou roteador de Internet são produzidos, instalados e mantidos por alguma entidade, cujos representantes legais mantêm a sua propriedade e esperam proteção legal e policial das autoridades do Estado soberano beneficiado pela infraestrutura.

Assim, quando se colocam os elementos de infraestrutura dentro de fronteiras de um território, sejam elas terrestres, marítimas ou aéreas, o Estado passa a exercer sua autoridade soberana sobre estes. Além disso, nos casos de ações realizadas fora do limite territorial dos Estados, aplicam-se princípios e regras de Direito Internacional, para solucionar possíveis demandas. (KANUCK, 2010, p.1571-1572).

No âmbito internacional, a natureza do sistema jurídico baseia-se no princípio da soberania dos Estados e organiza-se por meio da divisão geográfica do exercício desses poderes, com a chancela da ONU. A era da guerra cibernética ainda é vivida nos espaços físicos e utiliza-se das redes virtuais para se propagar e provocar prejuízos cada vez maiores.

Apesar do ambiente do ciberespaço não poder ser delineado como território de um Estado, limites jurídicos podem ser impostos sobre os meios pelos quais as comunicações sem fio e transmissões de mídia são propagadas. A regulação legal nacional e as diretrizes da União Internacional das Telecomunicações (UIT), agência da ONU especializada em tecnologias de informação e comunicação, determina quais são as frequências eletromagnéticas de comunicação regulares e veda qualquer prática de interferência não autorizada. (KANUCK, 2010, p.1574).

Alguns Estados, em nome da segurança, decidem por interferir no conteúdo das mídias eletrônicas, determinando de forma específica o que pode ser disponibilizado à sua população.(KANUCK, 2010, p.1574). Essa prática é muito criticada pelos defensores da liberdade de imprensa e do acesso à informação no Estado Democrático de Direito, mas a primazia da soberania estatal tem servido como justificativa para o exercício da chamada ‘segurança de informação internacional’, restritiva dos conteúdos de mídia.

[76] O satélite transponder de comunicações é um conjunto de unidades interligadas que formam um canal de comunicação entre o receptor e as antenas de transmissão. É usado principalmente em comunicações por satélites para transferir sinais recebidos. (KANUCK, 2010, p.1571).

A Organização de Cooperação de Xangai (OCX) preconiza essa postura ao afirmar que se o conteúdo consiste em uma ameaça potencial à segurança, este deve ser regulamentado como forma de defesa do Estado e de seu povo. (ORGANIZAÇÃO DE COOPERAÇÃO DE XANGAI, 2008).

A análise ideológica dessas limitações à informação não faz parte da discussão dessa tese, mas ressalta-se a preocupação com a restrição excessiva dos direitos humanos, no controle de conteúdos de mídia eletrônica e de comunicações, além do abuso do emprego da ameaça cibernética como justificativa para violação desses direitos.

Conclui-se que não há dúvidas de que toda a infraestrutura e os conteúdos partilhados no ciberespaço estão sujeitos à soberania e, consequentemente, à jurisdição dos Estados.

O desafio é viabilizar que o controle e exercício dessa soberania seja eficaz e que as normas jurídicas consigam trazer respostas adequadas para os atos violadores de direitos praticados no ciberespaço, dentre os quais, a guerra cibernética.

Nos casos em que haja dificuldade de se determinar a aplicação da jurisdição nacional, o próprio Direito Internacional pode trazer respostas às questões não solucionadas, ao primar pela defesa de seus princípios e dos direitos humanos, em especial, a máxima proibitiva do uso de força e da utilização da guerra, como forma de solução de conflitos.

6.2 O Ciberespaço como um ‘condomínio global’ cobiçado na luta pelo poder

A interação constante no ciberespaço dos atores tornou-se uma característica desafiadora da atual sociedade internacional, que cada vez mais demonstra ser dotada de uma profunda interdependência dos Estados e de uma grande interferência de atores não estatais. Como resultado, Barry R. Posen (1952–) 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". (POSEN, 2003, p.9, tradução nossa).[77]

O ciberespaço pode ser ou não denominado como um 'condomínio global'? Essa resposta é complexa, devido ao nível de especificidade desse domínio, que desafia a capacidade humana de estabelecer conceitos lineares. Alguns autores, como Janice Stein (1943–), têm defendido o ciberespaço como 'condomínio global', mas, ao mesmo tempo, também como território delimitado por fronteiras dos Estados soberanos. (STEIN, 2003). Apesar da característica global do ciberespaço, os Estados têm se esforçado na delimitação territorial desse domínio.

Para Misha Glenny (1958–) o ciberespaço ou, possivelmente, um 'condomínio global', não foi ainda definido, de forma satisfatória, para o Direito Internacional. É necessário identificar se o ciberespaço pode realmente ser limitado como um 'condomínio global', pois as características desse domínio precisam ser analisadas diante do conceito de espaço global. (GLENNY, 2011, p.22).

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.

Os indivíduos submetem-se a essas regras, quando necessário, mas sem habitualidade. Por exemplo, não se viaja internacionalmente de avião ou navio todos os dias, mas quando esse fato ocorre, há uma obediência às normas internacionais que regulam esses espaços. Entretanto, no caso do ciberespaço, a realidade é diferente, pois esse espaço é utilizado todos os dias pelos mais variados indivíduos de nacionalidades e características distintas. (GLENNY, 2011, p.22).

O ciberespaço vê-se regulado pelos Estados de forma doméstica e internacional. Há uma regulação extraoficial, realizada pelas atividades diárias dos indivíduos na Internet. Essa pluralidade faz com que a regulação seja moldada por forças não identificadas pelos Estados e pelo Direito Internacional como legítimas, mas a multiplicidade de atores é a grande característica do ciberespaço. (GLENNY, 2011, p.22).

---

[77] "...areas that belong to no one state and that provide access to much of the globe." (POSEN, 2003, p.9).

Brett Solomon, co-fundador e diretor executivo da ONG ‘Access Now’ (Acesso Agora), que promove o acesso aberto e seguro à Internet como meio para a realização dos direitos humanos, afirma que os usuários da Internet veem o ciberespaço como um espaço coletivo.

Na Internet, a sociedade percebe a possibilidade de se comunicar, mobilizar e difundir a informação e, essa liberdade, faz com que a base de usuários seja cada vez maior e o mais diversificada possível. Diante dessa extensão, o ciberespaço se define como um ‘condomínio global’, mas o problema são as ameaças que surgem, nesse domínio, das mais diversas fontes possíveis, partindo do governo, militares, coorporativas e de hackers. (SOLOMON; MITNICK, 2015).

Para se tornar esse espaço seguro, as ameaças precisam ser analisadas como desafios a serem solucionados, desde que essas soluções não sejam utilizadas como formas de censura e monitoramento dos usuários pelos Estados e pelas corporações.

Outra questão importante é não permitir uma privação coorporativa exacerbada do ciberespaço, de tal forma que haja a exclusão de usuários que não sejam consumidores. Além disso, a Internet também não pode se tornar um espaço de combate militar, pois o objetivo de defesa de direitos é mantido no ciberespaço. (SOLOMON; MITNICK, 2015).

Tem-se, portanto, no ciberespaço, um ‘condomínio global’ completamente novo e distinto dos outros domínios comuns já explorados. O desafio é traduzir as normas convencionais de Direito Internacional para o ciberespaço, uma vez que não há espaço físico territorial.

Estes ‘condomínios globais’ deveriam ser governados, coletivamente, para o benefício comum de toda a humanidade (incluindo Estados soberanos, indivíduos, empresas privadas, dentre outros.). Entretanto, o que se percebe é que, na luta pelo poder, os Estados que almejam a hegemonia política e militar, tais como os Estados Unidos da América entendem esses espaços como uma oportunidade de dominação hegemônica. (POSEN, 2003, p.4).

O comando dos espaços comuns (‘global commons’) é o fator fundamental para um Estado se destacar na posição de força hegemônica, na sociedade internacional. Esse controle permite a sustentação da hegemonia política, econômica e militar. Além disso, aquele que possuir o comando dos ‘condomínios globais’ terá ainda mais força para enfraquecer seus adversários, ao restringir o

seu acesso à assistência econômica, militar, política e, inclusive, cibernética. A era da informação manifesta-se sobre o controle dos ‘condomínios globais’ e estes serão os campos de batalha da luta pelo poder, em especial, o ciberespaço. (POSEN, 2003, p.6).

Na perspectiva da economia política, o ciberespaço, vivenciado sem regulações e de forma anárquica, não satisfaz os critérios lógicos de regulação do Direito Internacional, que aspira a legalização desse domínio como um ‘condomínio global’, sem incentivar a luta pelo poder, na busca da hegemonia política. O Direito Internacional precisa ter como base dois pressupostos para iniciar a regulação desse domínio global: o primeiro é a necessidade de proteção dos recursos físicos de difusão da informação, que estarão necessariamente protegidos pelos direitos de propriedade privada. O segundo é a necessidade de identificação positiva dos usuários legítimos do ciberespaço, assim como, a exclusão de usuários ilegítimos, sempre com a cautela de proteção dos direitos humanos. Também deve-se considerar as implicações econômicas da designação do ciberespaço como um ‘condomínio global’.

A experiência internacional tem demonstrado que tais sistemas necessitam de investimentos adequados e de inovação, desde que nenhum ator internacional se torne o único beneficiário de seus próprios investimentos. A melhor forma de se operar um ‘condomínio global’ é reduzindo os gastos de manutenção desse domínio, de tal forma que os atores mais prósperos economicamente, não possam se utilizar da fraqueza econômica dos outros atores, como uma arma de dominação do ‘condomínio global’. Esse é um tortuoso desafio para o ciberespaço, carecedor de investimentos frequentes em desenvolvimento de novas tecnologias.

Apesar das dúvidas que surgem sobre a aplicação do Direito Internacional e do conceito de ‘condomínios globais’ (‘global commons’) ao ciberespaço, algumas lições e princípios ainda podem ser aproveitados dos quadros jurídicos existentes e potencialmente aplicados à esse novo domínio.[78]

---

[78] Um exemplo pertinente diz respeito ao arquipélago polar de Svalbard que, apesar de estar sob soberania da Noruega, segundo o Tratado de Svalbard, assinado em Paris no dia 9 de fevereiro de 1920, está sujeito a um regime específico de acesso aos seus recursos naturais pela sociedade internacional, pois seus bens naturais foram designados para o benefício comum de várias nações. Nesse caso, a Noruega tem a responsabilidade legal e o custo de administrar a maior parte do território das ilhas, mas sua soberania é incompleta e serve principalmente para preservar esses recursos nos termos dos interesses da sociedade internacional. (KANUCK, 2010, p.1580).

Um segundo paradigma jurídico que se assemelha com o ciberespaço é a regulação do tráfego marítimo internacional. Nesse caso, embora os Estados adjacentes mantenham certos direitos

O desafio de se investir em tecnologia e preservação do ciberespaço, em prol dos interesses de toda sociedade internacional, em muito se assemelha com os exemplos de condomínios globais do arquipélago de Svalbard e do sistema internacional de regulação de águas navegáveis. Os Estados ou organizações internacionais, mais capazes de protegerem o ciberespaço, possam assumir a sua administração e não a sua soberania ou tutela, no sentido de atuar, proteger e investir para que todos possam usufruir desse espaço comum. Na visão do Realismo Político, seria impossível se chegar a esse acordo e essa proposta deve ser vista com cautela, diante da realidade de luta constante de poder no cenário internacional.

Entretanto, a ameaça constante dos ataques cibernéticos e da guerra cibernética podem levar os Estados investidores perceberem que proteger o ciberespaço seria também uma autoproteção, que os preservariam de ataques e violações de direitos, a despeito de beneficiarem toda a sociedade internacional.

O desafio se apresenta a partir da premissa de que entender o ciberespaço como um ‘condomínio global’ exigiria a relativização parcial da soberania dos Estados e estabelecimento de direitos de propriedade sobre mantenedora da comunicação no ciberespaço, nas mais diferentes jurisdições estatais. Nenhum domínio global, como o espaço aéreo, marítimo ou espacial é tratado como um ‘condomínio global’ sempre, entretanto, qualquer estrutura de governança coletiva para ciberespaço exigiria uma ampliação desse conceito.

6.3 O Direito Internacional aplicado ao Ciberespaço

O Direito Internacional, ao analisar a cooperação na sociedade internacional e o respeito à sua principiologia jurídica, divide suas normas em regras de governança do ciberespaço, política pública multilateral e segurança internacional (virtual e real).

Diante dessas preocupações, surge o termo ‘governança da Internet’, bem definido na ‘Cúpula Mundial da Sociedade da Informação’, que ocorreu em dois

---

soberanos, seu controle não é absoluto e deve ser equilibrado com os interesses de seus vizinhos ribeirinhos, bem como as necessidades de navegação internacional, de forma pacífica. Essa conjunção de exercício soberano com o uso do espaço marítimo por toda sociedade internacional, distingue o domínio marítimo como um “condomínio global”. (KANUCK, 2010, p.1580).

eventos patrocinados pela ONU, para discussão sobre a nova realidade cibernética internacional.

Os eventos ocorreram em 2003, em Genebra, e, em 2005, em Túnis. Acordou-se que o termo ‘governança da Internet’ deveria ser entendido como “o desenvolvimento e aplicação pelos governos, o setor privado e sociedade civil, em suas respectivas funções, de princípios, normas, regras, procedimentos decisórios e programas que dão forma a evolução e a utilização da Internet". (CÚPULA MUNDIAL DA SOCIEDADE DA INFORMAÇÃO, 2005, tradução nossa).[79]

Portanto, a ‘governança da Internet’ refere-se à organização, padronização, e administração técnica das infraestruturas de rede, em obediência aos ditames do Direito Internacional.

Reconheceu-se, nesses encontros internacionais, que:

> ...a Internet evoluiu para um ambiente global disponível para o público e sua governança deve constituir uma questão central nas preocupações da sociedade da informação. A gestão internacional da Internet deveria ser multilateral, transparente e democrática, com a plena participação dos governos, o setor privado, sociedade civil e organizações internacionais. Deve garantir uma distribuição equitativa dos recursos, facilitar o acesso para todos e garantir um estável e seguro funcionamento da Internet, sendo a pluralidade linguística uma das preocupações. (CÚPULA MUNDIAL DA SOCIEDADE DA INFORMAÇÃO, 2005, tradução nossa).[80]

Outra importante análise é a de que o enfoque multilateral da governança da Internet destina-se a descrever questões jurídicas que seriam de preocupação nacional, mas que pela natureza interconectada da informação e comunicação e pela infraestrutura global do ciberespaço, exigem uma abordagem transnacional. Essas regulações jurídicas envolvem a cooperação de execução transfronteiriça, o estabelecimento de normas internacionais contra crimes e ataques cibernéticos, a harmonização das normas regulatórias da privacidade de dados, a proteção dos direitos humanos e liberdades civis no cibesrespaço e o respeito às soberanias estatais com o intuito de se coibir a guerra cibernética.

---

[79] "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet." (CÚPULA MUNDIAL DA SOCIEDADE DA INFORMAÇÃO, 2005).

[80] “...the Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism”. (CÚPULA MUNDIAL DA SOCIEDADE DA INFORMAÇÃO, 2005).

O histórico da humanidade de utilizar da tecnologia como uma aliada da guerra assombra o homem desde os registros das primeiras guerras. O financiamento militar da ciência tem um poderoso efeito transformador sobre a prática e produtos da pesquisa científica desde o início do século XX. Particularmente desde a Primeira e Segunda Guerras Mundiais, avançadas tecnologias têm sido vistas como elementos essenciais de um sucesso militar. (ROLAND, 2015).

A incidência de atividades militares no ciberespaço gera preocupações de segurança nacional que alguns Estados estão buscando solucionar, através de tratados e acordo multilaterais. Na Assembleia Geral da ONU, registra-se essa inquietação, desde 1998, com a edição da Resolução sobre “Desenvolvimentos no campo da informação e telecomunicações no contexto de segurança internacional” que esboçou as primeiras dúvidas da sociedade internacional diante do ciberespaço. (ONU, 1998).

Os Estados foram conclamados a discutir sobre questões de segurança da informação; definir noções básicas relacionadas com a segurança no ciberespaço, incluindo interferências não autorizadas e desenvolver princípios internacionais que pudessem aumentar a segurança global das informações e sistemas de telecomunicações, além de ajudar a combater o terrorismo e a criminalidade. (ONU, 1998).

Além da Resolução de 1998, a Comissão de Segurança da Assembleia Geral da ONU editou a Resolução intitulada "Desenvolvimentos no campo da informação e das telecomunicações no contexto da segurança internacional". Os Estados-membros foram convidados a fornecer seus pontos de vista oficiais sobre a segurança da informação internacional. Entretanto, percebeu-se que cada uma das respostas dada pelos Estados demonstrava a visão do ciberespaço atrelada a conceitos regionais específicos, ou expressão de um ponto de vista nacional, que se repetia quando esses Estados encaravam os desafios apresentados, no âmbito internacional.

Diante desse resultado, a Assembleia Geral juntamente com sua Comissão de Segurança, esforçou-se por discutir o problema da cibernética além dos quadros nacionais dos Estados, ao alertar a sociedade internacional de seu caráter transfronteiriço. As resoluções da Assembleia Geral da ONU de 2005 a 2010

tiveram a intenção de conscientização da internacionalização do problema relacional da segurança no ciberespaço. (KANUCK, 2010, p.1582).

O Instituto das Nações Unidas para Pesquisas sobre Desarmamento (UNIDIR) realizou inúmeras reuniões entre 1999 e 2008 com o intuito de colocar em debate a segurança das informações no ciberespaço. Algumas organizações internacionais regionais, como a Organização do Tratado do Atlântico Norte (OTAN), a União Europeia e a Organização de Cooperação de Xangai, têm desenvolvido instrumentos regulatórios das relações interestatais no ciberespaço, atentos à ameaça e existência da guerra cibernética e, evidentemente, buscando resguardar seus interesses nesse novo domínio.

6.3.1 *As fontes tradicionais de Direito Internacional aplicadas ao Ciberespaço*

A solução dos problemas de regulação do ciberespaço e, em especial, a positivação de normas que possam regular a guerra cibernética, são questões que o Direito Internacional deve enfrentar na contemporaneidade. Entretanto, nada impede que a guerra cibernética possa usufruir dos princípios, normas e costumes do Direito Internacional reguladores da guerra tradicional. É necessário repensar a aplicação das fontes de Direito Internacional em prol de uma regulação do ciberespaço.

As fontes tradicionais de Direito Internacional geralmente levam os estudiosos ao artigo 38 do Estatuto da Corte Internacional de Justiça da ONU, no qual a doutrina encontra conforto na enumeração de quais são as fontes jurídicas utilizadas pela Corte, em sociedade dotada da característica de extrema pluralidade e relativa anarquia. As principais fontes são, portanto, os tratados internacionais reconhecidos pelos Estados soberanos, o costume internacional e os princípios gerais de direito; além das fontes auxiliares da jurisprudência internacional e a doutrina. (ONU, 1945).

A realidade internacional, por ser extremamente complexa nas suas interações, sempre apresentou-se como desafio para o direito e sua regulação positivista nacional. Nesse sentido, além das fontes formais de Direito Internacional, a doutrina adota a postura de reconhecimento da existência de

fontes materiais, que caso sejam regras comprovadas pela sua existência fática, passam a ser passíveis de vinculação jurídica formal como normas de *hard law*[81].

Nada poderia ser mais crítico para a regulação do sistema internacional que um contexto como o do ciberespaço; que agrava as condições de instabilidade das relações e coloca-se como um desafio jurídico pela ausência de precedentes históricos e regras codificadas.

Os Estados têm se preocupado em elaborar novas normas internacionais, ao declarar suas políticas de segurança nacional e formular doutrinas militares para o ciberespaço. Talvez possa ser desenvolvido um instrumento internacional para o ciberespaço, no futuro, mas isso parece improvável no curto prazo. Até então, a prática dos Estados e de pequenas ações regionais, continua a ser a principal fonte do Direito Internacional no ciberespaço.

6.3.2 *Jus ad Bellum no Ciberespaço*

É inquestionável que o Direito Internacional, em toda a sua doutrina contemporânea, defende a solução pacífica das controvérsias na sociedade internacional, sem permitir que a força seja usada de forma injustificada. Entretanto, a Teoria da Guerra Justa, originária nos estudos de Cícero, Santo Agostinho, São Tomás de Aquinio e Hugo Grócio, defende que o ato de guerra seria uma das características do ato de governar, apesar de não serem todas as guerras justificáveis moralmente.

O que se objetiva, na verdade, com a Teoria da Guerra Justa é regular e restringir o uso de força no âmbito internacional, por meio do estabelecimento de regras de combate. As união das normas tradicionais de combate e a preocupação originária na teologia cristã de Aquino ajudou a formar as regras da guerra do Direito Internacional. O conjunto de regras conhecido como “convenções de guerra” é constituído por essas normas morais e preceitos legais. (O’BRIEN, 2015, p.183).

A doutrina da guerra justa tem sido cada vez mais revivida pelos Estados na contemporaneidade. Mantém-se a premissa do Direito Internacional de que a

[81] O termo ‘hard law’ refere-se a normas de vinculação jurídica obrigatória, na sociedade internacional. O seu oposto são normas de ‘soft law’ não dotadas de obrigatoriedade e força cogente, mas que servem para regular as relações internacionais com base na sugestão de regras relacionais.

guerra não é uma forma legal de solução de controvérsias, entretanto, os mandados morais e limitações da doutrina de guerra têm sido evocados para complementar as prescrições legais do direito positivo da guerra. (O'BRIEN, 2015, p.183).

Historicamente, a doutrina da guerra justa e do Direito Internacional da guerra desenvolveram-se de forma concomitante. Essa postura se justifica pela necessidade, em alguns casos, de se obter um direcionamento de conduta de guerra diante de novos desafios, como a guerra cibernética. (O'BRIEN, 2015, p.184).

As evidências mais significativas da relevância e da importância da doutrina da guerra justa estão nas decisões políticas tomadas pelos Estados. Percebe-se que os Estados têm tido a preocupação de justificar com argumentos legais e morais as suas decisões de usar a força armada no âmbito internacional.

Faz-se a distinção entre o *jus ad bellum* e o *jus in bello.* As regras de *jus ad bellum* determinam as circunstâncias que justificam a entrada de um Estado em guerra e as regras do *jus in bello* servem como um regramento para a luta justa, após o início da guerra. (ZIOLKOWSKI, 2013, p.137).

As normas internacionais de *jus ad bellum,* reguladoras de conflitos armados, aplicam-se em todos os casos nos quais esse conflitos ocorram, mesmo que a guerra não tenha sido declarada ou, até mesmo, que os Estados não reconheçam a existência do conflito.

Entretanto, apesar da ampla aplicação dessas normas, não há, ainda, normas efetivas que regulem de forma explícita os ataques cibernéticos, no Direito Internacional. Portanto, examina-se se as normas de *jus ad bellum* aplicam-se às relações internacionais travadas no ciberespaço e, em caso positivo, quais seriam as circunstâncias nas quais um ataque cibernético poderia efetivamente provocar a aplicação do Direito Internacional.

6.3.3 *Princípios de Direito Internacional Aplicados à Guerra Cibernética*

Tratar da guerra e de sua regulação jurídica requer um estudo apurado do Direito Internacional Público, delineadas pelo artigo 38 do Estatuto da Corte Internacional de Justiça.

A sociedade internacional, segundo o artigo 38 do Estatuto da Corte Internacional de Justiça, deve ser regulada pelos "princípios gerais de direito reconhecidos pela Nações civilizadas". (ONU, 1945).

A Carta da ONU prevê, em seu artigo 2º, os princípios reguladores das relações internacionais, e estes princípios podem ser utilizados para as interações internacionais no ciberespaço. O grande desafio que se apresenta é a conscientização, entre os atores internacionais, de que os princípios de Direito Internacional também devam ser respeitados no ciberespaço.

A soberania é a noção básica para a instituição de um Estado Moderno e o princípio axiomático, no qual, o Direito Internacional se pauta. Nas palavras da Corte Internacional de Justiça, o princípio da soberania "deve ser plenamente respeitado e não comprometido, de nenhuma maneira, por atividades militares e paramilitares que são proibidas pelos princípios de Direito Internacional"[82]. (CIJ, 1984).

O respeito à soberania dos Estados está previsto no Artigo 2º, item 1[83], da Carta da ONU, sob a forma da expressão de "igualdade soberana", garantidora da equidade jurídica dos Estados, no âmbito internacional. Aplicar o princípio da igualdade soberana no ciberespaço é entender que o respeito à autonomia e à independência dos Estados se mantém nesse domínio.

A noção de soberania de Westfália e o sistema legal horizontal das relações internacionais são complementares e devem ser interpretados, de forma alargada, no ciberespaço, diante da pluralidade de aspectos políticos, econômicos e sociais que envolvem as relações em rede entre Estados, empresas transnacionais, povos, sociedades e indivíduos. (ZIOLKOWSKI, 2013, p.156).

Apesar das mudanças interpretativas do princípio da liberdade soberana dos Estados, a premissa basilar do Direito Internacional, de respeito e igualdade dos Estados, mantém-se como o princípio mais importante para a sua estruturação no combate as práticas de guerra, inclusive no ciberespaço, sem tolher a soberania estatal.

---

[82] Decisão da Corte Internacional de Justiça no Caso das Atividades Militares e Paramilitares na e Contra a Nicarágua (Nicarágua v. Estados Unidos da América) de 1984-1991.

[83] Artigo 2º. A Organização e seus Membros, para a realização dos propósitos mencionados no Artigo 1º, agirão de acordo com os seguintes Princípios:
1. A Organização é baseada no princípio da igualdade de todos os seus Membros. (ONU, 1945).

O segundo princípio importante de ser abordado é o da autopreservação dos Estados, consequência lógica da igualdade soberana. No parecer consultivo da Corte Internacional de Justiça sobre a “Licitude da Ameaça ou Uso de Armas Nucleares”, de 1996, reconhece-se o direito de cada Estado lutar pela sua própria sobrevivência, nos termos do artigo 51 da Carta da ONU que positiva a autorização do uso de força nos casos de legítima defesa. (CIJ, 1996).[84]

Diante do alto grau destrutivo das armas nucleares e da similar insegurança causada pela guerra cibernética, o princípio de autopreservação aplica-se ao ciberespaço nos mesmos termos, ou seja, quando justificado pela legítima defesa.

Entretanto, a complexidade relacional aumenta no ciberespaço pela dificuldade de se entender quais tipos de ataques cibernéticos seriam caracterizados como ataques armados, ensejadores do uso de força e resguardados pela legítima defesa. Os Estados não têm se debruçado sobre essas definições de forma satisfatória, uma vez que muitos entendem que a falta de uma definição viabiliza a manipulação política, no cenário internacional, o que pode ser ponto de estratégia política.

Em termos gerais, de acordo com a Corte Internacional de Justiça e a doutrina, um “ataque armado” não necessita do uso de um tipo de arma específico para se caracterizar como tal e poderia, nesse caso, ser conduzido por meios cibernéticos. Apesar das discussões ainda não terem se findado, percebe-se que ataques armados estão presentes nos principais casos de uso de força nas relações internacionais. (ONU, 1945).

Os termos do artigo 2º, item 4, da Carta da ONU devem ser respeitados e os Estados devem evitar o uso de força ou ameaça internacionais, entretanto, a mensuração das medidas e limites das relações deixam na obscuridade os limites impostos pelo Direito Internacional. (ONU, 1945).

Além disso, como o ciberespaço permite a presença de atores não estatais no centro de suas relações, sendo capazes, inclusive, de ensejar consequências de ataques armados, o Direito Internacional precisa se posicionar diante da nova realidade do alargamento dos chamados sujeitos/atores de Direito Internacional.

---

[84] “Tendo em vista o estado atual do Direito Internacional, bem como os elementos de fato de que dispõe, a Corte não pode, entretanto, concluir definitivamente se a ameaça ou uso de armas seria lícita ou ilícita em uma circunstancia extrema de legítima defesa, na qual a própria sobrevivência de um Estado estivesse em jogo”. (CIJ, 1996).

A teoria que tem se demonstrado mais eficaz na punição desses atores não-estatais é a que aplica o pensamento da punição do Estado nacional não punidor. Defende-se, portanto, que os Estados que tiverem uma postura leniente ou demonstrarem-se incapazes de impedir ou punir as atividades prejudiciais de atores não-estatais, devem ser considerados responsáveis por esses atos e punidos por eles no âmbito internacional.

Assim, as atividades cibernéticas conduzidas por atores não-estatais, podem ganhar a qualificação de “ataque armado”, nos casos de omissão ou incapacidade do Estado de coibi-las. Entende-se que nesse caso o Estado se torna cúmplice da conduta violadora do Direito Internacional. Essa nova visão do direito, exige que os Estados invistam no combate ao crime cibernético, ciberterrorismo e a todas as práticas que possam justificar a sua punição, no âmbito internacional, por não ter apenado indivíduos ou grupos de atores, que realizem ataques armados cibernéticos a partir de seu território. (ZIOLKOWSKI, 2013, p.162).

O respeito à soberania territorial e à jurisdição dos Estados também é fundamental para se estabelecer relações internacionais no ciberespaço de forma pacífica. O aspecto da soberania territorial, ou seja, o exercício da autoridade plena e exclusiva sobre um território, protege componentes físicos da internet (infraestrutura cibernética) que estão localizados no território de um Estado, sob a sua exclusiva jurisdição. Entretanto, o fato dos componentes transmissores da Internet estarem localizados nos territórios dos Estados, não determina que a jurisdição territorial é o único aspecto a ser examinado.

Os Estados não podem se ater somente ao caráter territorial nacional da jurisdição, uma vez que apesar de se aplicar o princípio da jurisdição territorial a noção de domínio global também deve ser adotada, como previamente discutido nesse trabalho. Devido à natureza global da Internet e à não limitação física do ciberespaço, entende-se que a soberania territorial é violada por quaisquer atos causando efeitos físicos em outro território e, além disso, as violações a redes e sistemas de computadores também são atos violadores da soberania do Estado, em um aspecto extraterritorial cibernético.

O argumento da necessidade exclusiva da consequência física, para se ter a violação de soberania, torna-se irrelevante no contexto cibernético, pois percebe-se que esse domínio também tem a proteção do princípio da independência soberana dos Estados além do território estatal. As atividades cibernéticas de conteúdo

malicioso podem provocar efeitos extremamente negativos à segurança dos Estados, e, por esse motivo, tem-se adotado a postura de defesa da soberania no âmbito cibernético. (ZIOLKOWSKI, 2013, p.164).

Outro importante princípio, a ser defendido no ciberespaço, é o princípio da não-intervenção nas relações internas (nacionais) ou nos negócios estrangeiros de outro Estado. O preceito da não-intervenção encontra-se consagrado na Carta da ONU, art. 2º, alínea 7[85] e é endossado em convenções regionais como, por exemplo, os artigos 16 a 19[86] da Carta da OEA. (OEA, 1997).

Esse princípio, também é defendido pela Corte Internacional de Justiça como uma regra de costume internacional, ao alertar, em especial, no caso Nicarágua *versus* EUA[87] que nem a assistência humanitária é uma forma de intervenção legalizada pelo Direito Internacional. A intervenção ilegal ocorre quando um Estado interfere com os assuntos internos ou externos de outro Estado com o objetivo de coagir o outro a certos comportamentos. (CIJ, 1991).

O fenômeno da globalização e da integração e o crescimento da interdependência e cooperação dos Estados têm feito com que pouquíssimos assuntos permaneçam nos limites da competência nacional pura. Entretanto, o que se percebe que deve ser respeitado, sem a intervenção de Estados estrangeiros, é a jurisdição e o tratamento legal que os Estados destinam aos seus entes nacionais.

Contudo, o desafio é presente, pois as relações de comunicação travadas no ciberespaço não podem ser consideradas como um assunto exclusivamente interno de cada Estado. As telecomunicações internacionais são reguladas pelo

---

[85] "Nenhum dispositivo da presente Carta autorizará as Nações Unidas a intervirem em assuntos que dependam essencialmente da jurisdição interna de qualquer Estado ou obrigará os membros a submeterem tais assuntos a uma solução, nos termos da presente Carta". (ONU, 1945).

[86] "Artigo 16 - A jurisdição dos Estados nos limites do território nacional exerce-se igualmente sobre todos os habitantes, quer sejam nacionais ou estrangeiros.
Artigo 17 - Cada Estado tem o direito de desenvolver, livre e espontaneamente, a sua vida cultural, política e econômica. No seu livre desenvolvimento, o Estado respeitará os direitos da pessoa humana e os princípios da moral universal.
Artigo 18 - O respeito e a observância fiel dos tratados constituem norma para o desenvolvimento das relações pacíficas entre os Estados. Os tratados e acordos internacionais devem ser públicos.
Artigo 19 - Nenhum Estado ou grupo de Estados tem o direito de intervir, direta ou indiretamente, seja qual for o motivo, nos assuntos internos ou externos de qualquer outro. Este princípio exclui não somente a força armada, mas também qualquer outra forma de interferência ou de tendência atentatória à personalidade do Estado e dos elementos políticos, econômicos e culturais que o constituem". (OEA, 1997).

[87] Decisão da Corte Internacional de Justiça no Caso das Atividades Militares e Paramilitares na e Contra a Nicarágua (Nicarágua v. Estados Unidos da América) de 1984-1991.

Direito Internacional e contam com a ajuda especial da União Internacional de Telecomunicações (UIT) que possui uma Convenção Internacional que regula a comunicação desde 1992. (UIT, 1992).

A convenção afirma o seu compromisso com o respeito ao “direito soberano de cada Estado para regulamentar suas telecomunicações” e leva em conta “a importância crescente das telecomunicações para a preservação da paz e o desenvolvimento social e econômico de todos os Estados Partes”. (UIT, 1992).

A comunicação no ciberespaço ocorre além dos limites da fronteira territorial dos Estados e, portanto, não pode ter uma regulação exclusivamente nacional, restrita pelos limites fronteiriços de um Estado. Além disso, por ter a natureza de um domínio globalmente público, a Internet facilmente viabiliza o compartilhamento mundial de softwares maliciosos e destrutivos, violadores de direitos. Essa globalidade da Internet e dos crimes nela cometidos, exige uma abordagem internacionalizada dos valores, direitos e regras a serem protegidos e estipulados diante do ciberespaço, por meio de práticas de cooperação judiciais. O segredo é encontrar um equilíbrio entre o princípio da não-intervenção e da cooperação dos povos, no enfrentamento desse novo desafio.

Outro princípio com o objetivo de eliminação de conflitos é o dever de não prejudicar os direitos dos outros Estados soberanos, como defendido pela Corte Internacional de Justiça no primeiro caso submetido a ela, em 1947, em uma disputa entre Reino Unido e Albânia, referente a incidentes no Canal de Corfu. Em síntese, a Corte decidiu que os prejuízos causados ao Reino Unido pela Albânia deveriam ser indenizados, pois todos os Estados têm o dever de não prejudicar ninguém, e, caso o façam, devem ser responsabilizados. (CIJ, 1947).

O dever de não prejudicar vai além, pois inclui a obrigação dos Estados de tomar medidas preventivas em casos concretos, em que seja possível lesar os direitos de outros sujeitos de Direito Internacional, caso tenha conhecimento. Esse princípio se aplica, por exemplo, nos casos de desenvolvimento de armas químicas, biológicas e cibernéticas.

A manutenção da paz e segurança internacionais apresenta-se como o objetivo primordial das Nações Unidas e princípio basilar do Direito Internacional consagrado no artigo 1º, item 1[88] da Carta da ONU. A consagração da defesa da

[88] Artigo 1. Os propósitos das Nações unidas são:

paz e da segurança têm sido sistematicamente reiterada pelo Direito Internacional nos mais diferentes órgãos, blocos econômicos e grupos internacionais, com o intuito de assegurar a todos uma maior estabilidade e menor anarquia.

A existência da paz não deve ser compreendida como uma ausência de guerra declarada ou qualquer tipo de conflito armado, pois é muito mais do que isso. A paz tornou-se um movimento multidimensional que requer uma série de medidas ativas, tomadas coletivamente pelos Estados e povos, ao objetivar a remoção das mais variadas ameaças à paz e segurança. (ZIOLKOWSKI, 2013, p.172).

A manutenção da paz e segurança exige a obediência ao princípio da proibição do uso de força ou ameaça no âmbito internacional, como estipula-se no artigo 2º, número 4[89], da Carta da ONU, já mencionado nesse trabalho. (ONU, 1945). O uso de força no âmbito cibernético ainda é um ponto nebuloso de ser caracterizado, pois muitas vezes é difícil de se identificar a ação armada dos Estados.

Entretanto, a Corte Internacional de Justiça no caso Nicarágua *versus* Estados Unidos[90] se pronunciou afirmando que o termo 'força' não se limita ao emprego de armamento militar, no sentido comum do termo, e pode ser também uma referência à utilização 'indireta' ou 'não-militar' da força armada, como, por exemplo, espalhando fogo na fronteira ou inundando o território do outro Estado. (CIJ, 1991). Nessa perspectiva, vislumbra-se que um ataque cibernético poderia caracterizar-se como uma forma de utilização ilegal da força, na maioria das vezes não-militar.

Como consequência da obrigação de não se recorrer à força desenvolve-se o princípio da solução pacífica de controvérsias, consagrado pelo artigo 2º, item 3 da Carta da ONU. O princípio limita a liberdade soberana de eleger as formas

---

1. Manter a paz e a segurança internacionais e, para esse fim: tomar, coletivamente, medidas efetivas para evitar ameaças à paz e reprimir os atos de agressão ou outra qualquer ruptura da paz e chegar, por meios pacíficos e de conformidade com os princípios da justiça e do Direito Internacional, a um ajuste ou solução das controvérsias ou situações que possam levar a uma perturbação da paz. (ONU, 1946).

[89] Artigo 2. A Organização e seus Membros, para a realização dos propósitos mencionados no Artigo 1, agirão de acordo com os seguintes Princípios:
(...)
4. Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso de força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas. (ONU, 1945)

[90] Decisão da Corte Internacional de Justiça no Caso das Atividades Militares e Paramilitares na e Contra a Nicarágua (Nicarágua v. Estados Unidos da América) de 1984-1991.

como soluciona seus litígios, uma vez que determina que todos os Estados por mais que gozem de soberania devem liquidar seus embates de forma pacífica, evitando, portando perturbar a paz e segurança internacionais. Os meios pacíficos de solução de controvérsias consistem em medidas político-diplomáticas (por exemplo, negociação, inquérito, mediação, conciliação) e medidas judiciais (contenciosos e arbitragem). (ZIOLKOWSKI, 2013, p.175).

O princípio geral de cooperação internacional nem sempre consagrado pelos doutrinadores se apresenta diante do desafio jurídico e relacional do ciberespaço. O dever dos Estados de cooperação tem um caráter normativo, sempre que ele é aprovado nos tratados internacionais que estabelecem e que regem, em especial, organizações regionais, como por exemplo, a União Europeia e o MERCOSUL.

Entretanto, o dever de cooperação interestatal como o princípio, diante das demandas do ciberespaço não deve ser visto somente diante do positivismo de *hard law* estabelecido nos tratados internacionais, que o consagram. O que se vislumbra na sociedade internacional é a existência de um dever (querer) geral de cooperação entre Estados, que vivem a nova realidade de total descontrole das relações no ciberespaço.

Na perspectiva do compartilhamento de conexões nesse novo domínio global, que pode se tornar um domínio de guerra, passa a ser de interesse dos Estados cooperar para encontrar soluções para os novos desafios que forem se apresentando. O princípio de cooperação internacional dos Estados, diante da ameaça da guerra cibernética, não se apresenta como um ideal utópico, mas como uma necessidade que assume a característica de princípio jurídico. A cooperação serve para tentar organizar e legalizar o domínio do ciberespaço em prol da manutenção da paz e segurança.

Em resumo, são princípios gerais de Direito Internacional aplicáveis ao ciberespaço com o intuito de coibir a guerra cibernética e preservar a paz: a igualdade soberana dos Estados, incluindo o direito dos Estados de autopreservação, independência e respeito à jurisdição nacional. O princípio da não-intervenção nos assuntos da competência interna de outros Estados, coibindo, inclusive a espionagem cibernética. A abstenção do uso de força ou ameaça nas relações internacionais; a solução pacífica de controvérsias e o dever (necessidade) de cooperação internacional na resolução de problemas internacionais, em especial diante das ameaças do ciberespaço.

6.3.4 *A Futura Regulação do Ciberespaço pela Sociedade Internacional*

A complexidade da sociedade sistêmica internacional, que se agrava pela nova realidade das relações de incessantes interconexões de atores no ciberespaço, faz com que o exercício de desenvolvimento de uma única legislação linear e uniformizadora no âmbito internacional, seja contraditória a toda base filosófica que sustenta esse trabalho. Não se objetiva pensar que seja possível compreender aos olhos lineares da linguagem humana escrita e científica cartesiana, a complexidade da realidade internacional que se apresenta e, em especial, conseguir trazer uma única solução para essa sistemática.

Tem-se a ideia de que as soluções devem ser plurais, mas objetiva-se nesse momento discutir possíveis princípios que possam sustentar e ajudar o Direito Internacional a viabilizar a busca da paz e segurança em tempos de relações internacionais travadas no ciberespaço.

Os chamados de ‘global commons’, nesse trabalho traduzidos como ‘condomínios globais’, podem ser um ponto de partida interessante para uma discussão jurídica a respeito do tratamento que deve ser dado ao ciberespaço, também caracterizado como domínio global. Exemplos desses domínios são o alto mar, o espaço e a Antártida. Alguns princípios gerais básicos do Direito Internacional, que regem a proteção do meio ambiente, poderiam ser identificados e aplicados ao ciberespaço caracterizando-o como um recurso global compartilhado e / ou como um espaço comum de toda a sociedade internacional.

Entretanto, entende-se que refletir sobre o futuro do Direito Internacional, na Era Cibernética, só pode ser feito no âmbito principiológico, pois qualquer outra digressão seria tentar solucionar o problema sem antes estudar e conhecer as necessidades da sociedade internacional. Além disso, diante da pluralidade e variedade de relações conexas travadas no ciberespaço, não há maturidade social para a compreensão jurídica adequada das consequências da evolução cibernética nas relações internacionais. Assim, a seguintes deliberações de *lege ferenda* irão considerar princípios específicos aplicados aos ‘global commons’, relacionando-os ao novo domínio global do ciberespaço.

A primeira enunciação passível de aplicação é o princípio do desenvolvimento sustentável, mencionado inicialmente, no âmbito das Nações Unidas, na década de 1970, e, posteriormente, conceituado no Relatório de Brundtland de 1987, no qual se afirma que: "Desenvolvimento sustentável significa suprir as necessidades do presente sem afetar a habilidade das gerações futuras de suprirem as próprias necessidades". (ONU, 1987).

Defende-se a regra do uso sustentável dos recursos, como mais que um princípio, mas consiste em norma de direito interacional, devido à sua previsão em um vasto número de tratados internacionais que cuidam da preservação ambiental. Além disso, essa regra vê-se reafirmada pelo princípio de utilização equitativa dos recursos compartilhados (domínios globais), reconhecido como um princípio geral de Direito Internacional, além de encontrar-se consagrado em vários tratados internacionais, Resoluções da Assembleia Geral da ONU, declarações políticas e ser confirmado pela jurisprudência internacional. (ZIOLKOWSKI, 2013, p.180).

Assim, a regra de utilização sustentável e equitativa dos recursos dos domínio globais, pode ser considerada como um princípio geral de Direito Internacional ambiental e pode ser aplicada ao ciberespaço, também considerado como um condomínio global. Nesses termos, o ciberespaço e a Internet como outro recurso global compartilhado, estabelece a obrigação legal dos Estados de cooperar no seu uso sustentável e equitativo, nos termos já estabelecidos para os outros domínios comuns. (CHOUCRI, 2015).

Essa conclusão não parece tão óbvia de ser tomada, uma vez que o ciberespaço e a Internet apresentam-se inicialmente como domínios não físicos, virtuais, que poderiam ser de exploração inofensiva na relação internacional sustentável. Como imaginar que seria necessário explorar o ambiente virtual de forma sustentável, para preservar sua exploração para as gerações vindouras?

Em uma análise leiga, imagina-se que o ciberespaço e a Internet seriam um domínio incapaz de ser explorado e esgotado, sendo, portanto, livre da necessidade da utilização sustentável. Entretanto, a Internet e o ciberespaço se limitam pela estrutura dos meios pelos quais são instalados e já passou por um grande impasse de esgotamento em 2011.

A conectividade na Internet se dá de forma singular e requer um endereço individual de 'IP' ('*Internet Protocol'* ou Protocolo de Internet)[91] e como a geração desses endereços codificados se limita pela capacidade do servidor de emiti-los é possível haver o esgotamento da exploração do sistema, o que seria uma exploração não sustentável. (ICANN, 2013).

O sistema de IP versão 4, que fornecia aproximadamente 4 bilhões de números de IP's, deixou de ser suficiente desde fevereiro de 2011, segundo o Relatório Anual da Corporação da Internet para Atribuição de Nomes e Números – ICANN. (ICANN, 2013).

Como tentativa de solucionar o esgotamento da exploração do sistema, desenvolveu-se o protocolo de Internet versão 6 (IPv6) que pode fornecer aproximadamente 340 sextilhões de endereços de IP, que considera-se como mais do que suficiente para o mundo, cuja população é de aproximadamente 7 bilhões de pessoas. (ICANN, 2013).

Entretanto, mesmo o IPv6, implantado desde 2012, não é compatível com IPv4 e, portanto, utilizado apenas em algumas partes do mundo, o que ainda limita a exploração do ambiente virtual. (ICANN, 2013). Além disso, hoje vislumbra-se que essa quantidade de IP's emitidos pelo IPv6 sejam suficientes, mas o avanço tecnológico tem exigido cada vez mais da estrutura que o mantém, o que pode fazer com que no futuro seja necessário a criação de um novo sistema, que aumente a capacidade do domínio.

Além da questão do cuidado com o espaço de dados, a obrigação legal do uso sustentável da Internet e do ciberespaço, reconhecendo as necessidades e os interesses das gerações futuras, também pode resultar em uma obrigação dos Estados de empreender toda a sua estratégia política, sua normas jurídicas e administrativas na busca de preservação da dignidade humana nesse novo domínio, em dimensão ética da sustentabilidade. (CHOUCRI, 2015).

Outro princípio fundamental a ser explorado é o de defesa do patrimônio comum da humanidade, no qual se baseia a instituição da proteção dos bens encontrados nos 'condomínios globais'. O Tratado de Montego Bay[92], de 1982, por

[91] "Endereço de IP (*Internet Protocol* ou Protocolo de Internet), de forma genérica, é uma identificação de um dispositivo (computador, impressora, etc) em uma rede local ou pública. Cada computador na internet possui um IP único, que é o meio em que as máquinas usam para se comunicarem na Internet." (PISA, 2005).

[92] Também conhecido como Convenção das Nações Unidas sobre o Direito do Mar de 1982.

exemplo, na sua parte XI, trata sobre o fundo do mar, como uma herança da humanidade. (ONU, 1982).

O espaço, no artigo 1º do Tratado do Espaço de 1967[93] também é definido como um patrimônio da humanidade passível de proteção. (BRASIL,1969). Outro exemplo é a Antártida entendida como patrimônio mundial como explicitado no parágrafo 8º[94] do preâmbulo do Protocolo sobre a Proteção ambiental do Tratado da Antártida de 1991. (ESTADOS ANTÁRTICOS, 1991).

A aplicação do princípio defesa do patrimônio comum da humanidade é realizada de forma variável diante da pluralidade de sujeitos de Direito Internacional que o interpretam dentro de seus sistemas, costumes e culturas jurídicas, entretanto, tem-se observado um padrão interpretativo que utiliza-se de basilares premissas de Direito Internacional, o que pode ser de muita valia na aplicação da defesa desse princípio do ciberespaço. A primeira questão é excluir qualquer visão que possa ser imbuída de resquícios do imperialismo da soberania territorial, ou seja, não se pode interpretar que o patrimônio da humanidade passa a ser 'patrimônio do Estado que reivindica a posse do bem', pois esses domínios globais, assim como o ciberespaço, devem ser abertos e utilizados por todos de forma democrática.

Ademais, a administração desses domínios, dentre os quais o gerenciamento da Internet, deve ser compartilhado de forma internacional, justamente para evitar a dominação da vontade de uns sobre os outros a limitação de acessos. Há também a obrigação internacional de cooperação no uso e exploração dos domínios globais, por meio da distribuição igualitária dos benefícios adquiridos a toda humanidade. Por fim, não se pode olvidar da preocupação com os interesses das gerações futuras, quando explora-se esses domínios e o entendimento de que a única forma legal e aceitável de compartilhamento é com objetivos pacíficos. (CLANCY, 1998, p. 601).

A noção de ciberespaço apresenta-se como um desafio para aplicação desses princípios de forma análoga aos domínio globais, uma vez que seu funcionamento possui natureza virtual não territorial, mas depende de mecanismos

---

[93] O nome completo do tratado é: "Tratado sobre Princípios Reguladores das Atividades dos Estados na Exploração e Uso do Espaço Cósmico, inclusive a Lua e demais Corpos Celestes".

[94] "Convencidos de que o desenvolvimento de um regime abrangente de proteção ao meio ambiente antártico e aos ecossistemas dependentes e associados interessa a toda a humanidade". (ESTADOS ANTÁRTICOS, 1991).

de funcionamento que encontram-se em territórios estatais. Não se questiona mais, nesse trabalho, a característica de globalidade do ciberespaço, vinculada às interconexões travadas na Internet, como um domínio universal, conceitual, virtual e não físico, no qual se preserva um banco de dados de memória compartilhada global da humanidade.

Entretanto, a aplicação dos princípios de defesa do ciberespaço, como domínio global, esbarra na questão física e territorial dos componentes técnicos instalados nos territórios dos Estados que permitem a existência e funcionamento desse domínio. Conclui-se, portanto, que os componentes físicos e técnicos do ciberespaço estão sujeitos à soberania territorial de diversos Estados, embora, em conjunto formem domínio global de exploração sustentável, compartilhada com objetivos pacíficos.

Outra interessante analogia proposta pela jurista alemã Katharina Ziolkowski, está na utilização da experiência da Organização Mundial da Saúde (OMS) para a criação de uma organização reguladora da ‘saúde’ do ciberespaço. Não se trata, literalmente, da saúde humana, mas da capacitação de uma entidade aos moldes da OMS para controlar e regular os impactos das ameaças cibernéticas em segurança nacional e internacional, e viabilizar maior estabilidade na exploração dos avanços tecnológicos na crescente rede global interconectada do ciberespaço. A autora propõe, ainda, que algumas regras do Regulamento Sanitário Internacional (RSI) de 2005, que entrou em vigor no Brasil em 2009, fossem adaptadas ao ciberespaço. Algumas medidas interessantes seriam reforçar as capacidades nacionais para vigilância e resposta cibernética; elaboração de relatórios de incidentes de quebra de segurança; determinação de quarentenas para redes infectadas por vírus e programas maliciosos estipulação de um glossário específico e universal determinação de normas básicas de segurança e pureza cibernética; delimitação de regras de publicidade e propaganda na rede e criação de medidas de defesa de emergência. (ZIOLKOWSKI, 2013, p.184).

7 A SOCIEDADE INTERNACIONAL E O SEU QUADRO LEGAL PARA A PROTEÇÃO DO CIBERESPAÇO CONTRA AÇÕES DE GUERRA CIBERNÉTICA

Nos sistemas jurídicos atuais, o território dos Estados e os interesses da sociedade internacional servem como base legal para a regulação dessas relações. As sociedades possuem quatro tipos de sistemas legais para o enfrentamento do problema da guerra cibernética: *civil law*, *common law*, direito consuetudinário e normas ligadas à religião. O Direito Internacional divide-se, ainda, em Direito Internacional Público, regulador da relação da sociedade internacional; Direito Internacional privado, que aborda a jurisdição legal, em especial dos conflitos de leis no espaço e direitos dos estrangeiros e o de direito supranacional, com quadro jurídico em que os Estados estão vinculados pelos acordos regionais que realizam, mas que esses acordos se tornam inaplicáveis quando em conflito com preceitos supranacionais, como os princípios de *jus cogens*.

No âmbito nacional, o *civil law* é o tipo mais difundido de sistema jurídico, no qual leis são organizadas e positivadas em códigos escritos e sistemáticos. No *civil law,* as fontes dotadas de obrigatoriedade são primeiro as leis escritas e, secundariamente, os costumes. Além desse sistema, o *common law* adota a noção de que os precedentes jurídicos têm o caráter vinculante, ou seja, o juízo futuro pode declarar-se vinculado a decisões anteriores, em face da identidade de casos. (BROWNLIE, 2002, p.49).

O direito consuetudinário, representa um conjunto organizado de regras não positivadas, aprovadas pelos membros da sociedade, que regulam as relações sociais. Embora o direito consuetudinário inclua sanções para as infrações legais, a tendência tem sido de que as soluções oferecidas para os conflitos de costumes tendam à conciliação, ao invés de ter um caráter meramente punitivo.

Enfim, tem-se as normas religiosas influenciadoras das relações na sociedade internacional, mesmo que grande parte dos Estados adotem uma postura de laicidade. Os principais tipos de sistemas jurídicos religiosos são o Sharia adotado pelo Islã, o Halachá do sistema judaico e o direito canônico aplicado a alguns grupos cristãos. Além desses sistemas, alguns tem o caráter de serem pluralistas, pois misturam a lei com elementos dos costumes ou da religião. (TETLEY, 2005).

A diversidade regulatória cultural e de sistemas jurídicos existente na sociedade internacional é indiscutível, entretanto, problemas capazes de causar prejuízos a toda humanidade, como a guerra e os ataques cibernéticos, merecem atenção legal além da jurisdição nacional específica de cada Estado.

A dificuldade enfrentada está no fato de que cada um desses sistemas lida com guerra cibernética de maneiras diferentes e, por isso, cria-se uma situação de pluralidade jurídica difícil de ser solucionada, uma vez que não se tem uma única forma de resolver um impasse coletivo com a regulação do ciberespaço. Mas será que a uniformização de uma única resposta legal, para um problema dotado de tamanha complexidade, seria a solução?

Os sistemas jurídicos nacionais baseiam-se em seus próprios princípios fundamentais e confiam no critério geográfico, limitador dos territórios, para determinar quais leis regularão os imprevistos enfrentados. Além disso, as leis são escritas em um ritmo lento, diante das questões cibernéticas que se desenvolvem na alta velocidade da inovação tecnológica.

Caso interessante de ser citado é o caso do *worm*[95] 'eu te amo'[96] em 2000. A investigação chegou a identificar o programador responsável que era das Filipinas, mas como não havia naquele tempo leis sobre a liberação de 'malware'[97] na Internet, ele não foi responsabilizado. O ataque do vírus 'eu te amo' é historicamente notável, pois ficou evidente que as empresas realmente dependiam da Internet e do e-mail, diante da queda na produtividade provocada. Os desenvolvedores de software, como a Microsoft passaram, então, a investir em segurança e não somente no desenvolvimento de novos produtos. A grande consequência jurídica foi a percepção de que o cibercrime é, de fato, um problema internacional e que a aplicação de Direito Internacional nesses casos seria crucial para a segurança nesse novo domínio. (HULME, 2015).

---

[95] "Worm é um programa semelhante aos vírus, com a diferença de este ser auto-replicante, ou seja, ele cria cópias funcionais de si mesmo e infecta outros computadores. Tal infecção pode ocorrer através de conexões de rede locais, Internet ou anexos de e-mails". (MARTINS, 2015).

[96] O nome do *worm* foi traduzido literalmente do seu nome original em inglês "I Love You".

[97] "Malware é um nome abreviado para "software malicioso" Malware é qualquer tipo de software indesejado, instalado sem o seu devido consentimento. Vírus , worms e cavalos de troia são exemplos de software mal-intencionado que com frequência são agrupados e chamados, coletivamente, de malware."

A tendência do jurista, muitas vezes voltado ao positivismo cartesiano, buscar estabelecer único sistema jurídico internacional regulador do ciberespaço, que consiga abranger a pluralidade cultural e religiosa da sociedade internacional.

Entretanto, diante do número de conexões interativas e do alargamento do número de atores internacionais, capazes de ativamente produzirem efeitos negativos nessa relação de guerra, entende-se que talvez a solução não seja a elaboração de um único tratado, mas do estabelecimento de fundamentos principiológicos que possam nortear a vivência da sociedade internacional no ciberespaço. Apesar de ser importante entender que a resposta jurídica legal não será elaborada por uma única solução para o problema, é importante pesquisar sobre como os diferentes grupos de atores internacionais têm enfrentado e regulado juridicamente o dilema da guerra cibernética.

7.1 As contramedidas ao ataque cibernético e a legítima defesa

O exercício da legítima defesa é regulado pelo Direito Internacional e diante da guerra cibernética se encontra em um impasse de definições. A questão é sobre quais seriam os possíveis ataques cibernéticos, que se elevariam à qualidade de violações do Direito Internacional, para justificar o legítimo exercício da defesa pelos Estados, por meio de contramedidas.

A legítima defesa, até então citada na Carta da ONU como um princípio, é defendida no “Projeto de artigos sobre a responsabilidade dos Estados para atos internacionalmente ilícitos” elaborado pela Assembleia Geral da ONU, em 2001, de forma concreta, por meio do direito dos Estados de tomar contramedidas em face de seu Estado ofensor. Essas contramedidas são definidas como atos que em circunstâncias contrárias seriam vistos como ilegais no Direito Internacional, realizados para buscar o fim ou a reparação do ataque inimigo. (ONU, 2001).

No âmbito do ciberespaço, demonstra-se impossível para o Direito Internacional definir de forma objetiva quando um ataque cibernético é ilegal e passível de legítima defesa. A análise é genérica, mas aplica-se no domínio cibernético, uma vez que entende-se que quando um Estado realiza uma violação no âmbito internacional, o Estado lesado tem o direito de responder de forma legalizada na defesa de sua soberania, independente do meio pelo qual o ataque

foi executado. Além disso, alguns ataques cibernéticos serão caracterizados como violadores do Direito Internacional, mas não poderão ser identificados como ataques armados, utilizadores da força ostensiva. Entretanto, mesmo que um ataque cibernético não se caracterize pelo uso de força, o simples fato de ter ocorrido um ataque, permite a identificação da violação do princípio da não intervenção, previsto pelo Direito Internacional, o que admite uma contramedida proporcional. (HATHAWAY *et al*; 2012, p. 45).

O objetivo de se admitir o exercício de contramedidas é viabilizar a proteção real do direito de legítima defesa dos Estados, e, portanto, não se tolera a aplicação de contramedidas de forma abusiva, desnecessária ou até mesmo quando a violação já tenha se findado. O objetivo das contramedidas é cessar a vitimização dos sujeitos de Direito Internacional, dando-lhes ferramentas legais para a legítima defesa. Nesse sentido, cessada a violação, não se justifica a aplicação das contramedidas de forma posterior. Ademais, não há contramedidas que possam justificar legalmente a violação dos direitos humanos. (HATHAWAY *et al*; 2012, p. 46).

Os ataques cibernéticos caracterizam a violação do dever dos Estados de não intervir em outros Estados soberanos, mesmo que seja pelo meio virtual. Contabilizados os prejuízos com o ataque, o Estado vitimizado poderá empregar, nos termos da Carta da ONU e do princípio da legítima defesa, contramedidas legítimas. As respostas mais efetivas, nesses casos, costumam ser as chamadas pela doutrina de ‘defesas ativas’, que buscam desmantelar a fonte do ataque.

Exemplo de defesa ativa seria a realização de contra-ataques cibernéticos com o objetivo de destruir programas e estruturas de computador que estão ativamente lesando o Estado vítima. Há também as ‘defesas passivas’ que não atacam, mas criam barreiras para impedir e proteger o Estado de futuros ataques, no âmbito do ciberespaço. Exemplo dessa defesa seria a instalação de *firewalls*[98] mais potentes no sistema operacional estatal. (HATHAWAY *et al*; 2012, p. 47).

Na atualidade, o grande atrativo para um Estado escolher realizar seus ataques no âmbito cibernético, é a alta possibilidade de impunidade, pois conta com a probabilidade de nunca ser descoberto em seu intento ilegal. Entretanto,

[98] "Firewall é uma barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, mas sem impedir que os dados que precisam transitar continuem fluindo. Na informática, os firewalls são aplicativos ou equipamentos que ficam entre um link de comunicação e um computador, checando e filtrando todo o fluxo de dados." (MACHADO, 2015).

essa instabilidade do domínio cibernético, não justifica a aplicação de contramedidas ativas sem o cuidado de apuração do real responsável pela violação de direitos. Não há contramedida legal, sem a certeza do agente responsável pela violação e da necessidade de aplicação da medida.

Caso contrário, o ato deixa de ser caracterizado pelo exercício de legítima defesa e se diferencia como outro ataque cibernético, violador do Direito Internacional. Os princípios da proporcionalidade e necessidade sempre devem ser norteadores no exercício da legítima defesa, por meio da aplicação de contramedidas ativas.

7.2 Os Regimes Jurídicos Internacionais que regulam diretamente os ataques cibernéticos e a guerra cibernética

A pluralidade da sociedade internacional se manifesta nos regimes jurídico-legais que regem as relações dos atores no ciberespaço, pois não há tratado internacional unificado que seja responsável pela regulação global dessas relações. Apesar da pluralidade é importante se analisar os mecanismos legais criados no âmbito de cada uma das coletividades da sociedade internacional, a fim de se vislumbrar padrões de respostas, limites e regramentos para um futuro Direito Internacional cibernético.

Analisa-se, portanto, o que está sendo desenvolvido no âmbito da Organização das Nações Unidas (ONU); União Europeia (UE); Organização dos Estados Americanos (OEA); Organização de Cooperação de Xangai (OCX) e pela Organização do Tratado do Atlântico Norte (OTAN). Pesquisa-se, também, o quadro jurídico brasileiro diante do novo domínio no ciberespaço e suas principais medidas legais.

7.2.1 A ONU e as políticas legais de segurança cibernética

A Organização das Nações Unidas, tem se manifestado na formação de uma cultura de alerta sobre a importância da segurança cibernética e o suporte para discussões de soluções globais para as ameaças virtuais existentes e emergentes.

Em dezembro de 2011, o Conselho Econômico e Social da ONU, com o objetivo de difundir a cultura da segurança cibernética, realizou um encontro mundial no qual salientou que os problemas enfrentados pelo Direito Internacional, no ciberespaço, são um dos principais pontos de desestabilização da sociedade internacional e dependem do debate jurídico global para se estabilizarem. (ECOSOC, 2011).

A ideia de disseminar a conscientização cultural da necessidade de políticas globais de segurança cibernética, tem influenciado diversos órgãos da ONU que lutam pela paz e segurança. Entretanto, o Conselho de Segurança ainda não se manifestou sobre as ameaças ao Direito Internacional experienciadas no ciberespaço, de forma efetiva. A única manifestação do Conselho de Segurança se deu com a Resolução 1.113 de 2011, na qual define o conceito de guerra cibernética:

> 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, tradução nossa).[99]

Entretanto, de forma específica, não há qualquer decisão do Conselho sobre casos fáticos de guerra ou ataques cibernéticos. Todos os pronunciamentos, até hoje realizados, nos casos de envolvimento do domínio do ciberespaço, têm-se limitado à análise clássica do Direito Internacional e se olvidado do novo aspecto. A decisão em relação ao ataque do Irã em 2010, por exemplo, ignorou completamente os questionamentos cibernéticos apresentados pelo caso. (MAURER, 2011, p.14).

Não obstante, a segurança cibernética é uma preocupação, abordada, de forma reiterada, pela Assembleia Geral da ONU, que visa estimular o debate global sobre os novos desafios que o ciberespaço apresenta ao Direito Internacional. O processo de elaboração de normas sobre o ciberespaço, da Assembleia Geral da

---

[99] "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).

ONU, divide-se em duas correntes principais de negociações: de um lado transações de caráter político-militares e de outro trabalha-se as questões econômicas vinculadas à cibernética.

As discussões político-militares são voltadas para a preocupação de como a informação e o ciberespaço podem ser utilizados para objetivos incongruentes com a dinâmica de manutenção de paz e estabilidade internacionais. Além disso, esse grupo se preocupa em endereçar questões vinculadas à proteção dos direitos dos sujeitos de Direito Internacional, em especial os Estados, na Era Cibernética. O grupo destinado às discussões econômicas busca soluções para o uso indevido da tecnologia de informação para ganhos econômicos e suas consequências na perturbação da sociedade internacional. (MAURER, 2011, p.15).

Nessa divisão, a guerra cibernética e o cibercrime são termos alternativos para as duas correntes, político-militar e econômica, respectivamente. A guerra cibernética pode ser entendida como a penetração não autorizada na rede de computador de um Estado, ou na realização de qualquer atividade que coloque em perigo ou ataque essa rede. Os cibercrimes são realizados entre atores internacionais distintos, mas tem o objetivo de ruptura econômica e não política.

Há uma ação conjunta de diversos órgãos da ONU na análise da problemática da segurança do ciberespaço. No âmbito político militar, foi instituído o chamado de Primeiro Comitê de Assembleia Geral da ONU, como órgão Intergovernamental, responsável para a lidar com a esfera político-militar do ciberespaço. Esse Comitê é assistido pela União Internacional de Telecomunicações (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, p.17).

A UIT é a agência da ONU responsável por tecnologias da informação e comunicação e tem o papel de desenvolver normas técnicas de promoção segura do acesso à tecnologia do ciberespaço. A UIT elaborou o documento intitulado de 'Política de Segurança Global Cibernética'[100] para defender uma maior cooperação internacional no desenvolvimento de medidas de segurança global cibernética. (UIT, 2007). A UIT determina cinco pilares para segurança cibernética que inclui medidas jurídicas, medidas técnicas e procedimentos, estruturas de organização,

[100] No original em inglês: "Global Cybersecurity Agenda".

capacitação e cooperação internacional. (UIT, 2007). Além disso reitera o seu compromisso de reforçar a segurança no ciberespaço, ajudando a construir a confiança no uso das tecnologias de informação e comunicação, bem como treinamento e conscientização sobre segurança cibernética. (UIT, 2007).

O Instituto das Nações Unidas para a Pesquisa sobre o Desarmamento (UNIDIR) promove a pesquisa independente sobre o desarmamento e a cooperação na procura de soluções para problemas emergentes como as demandas do ciberespaço. As ameaças cibernéticas em particular são cobertas pelo Instituto sob o título de ameaças emergentes. (PAKALNIŠKIS, 2011, p.17)

A Força-Tarefa de Implementação do Combate ao Terrorismo (CTITF) tem como objetivo unir esforços na luta contra o terrorismo do sistema internacional das Nações Unidas. Seu foco é especifico no combate ao terrorismo e, por consequência, se responsabiliza pela coibição do uso do ciberespaço e da Internet como meios de propagação do terrorismo. (ONU, 2006).

O Terceiro Comitê da Assembleia Geral da ONU e o Conselho Econômico e Social (ECOSOC) são os órgãos intergovernamentais responsáveis pela discussão da segurança cibernética no aspecto econômico. Esses órgãos recebem o apoio do Escritório das Nações Unidas sobre Drogas e Crime (UNODC) e do Instituto de Investigação Inter-regional de Crime e Justiça das Nações Unidas (UNICRI). (MAURER, 2011, p.18).

Os estudos e discussões realizados pelo Terceiro Comitê e seus órgãos auxiliares são de extrema importância social econômica, uma vez que esses órgãos tem o dever de tentar solucionar os embates socioeconômicos oriundos da relação internacional no ciberespaço. Os trabalhos desenvolvidos por esses órgãos, terão importância para a análise jurídica da temática central desenvolvida nesse trabalho, quando houver influência desses aspectos na relação de segurança e guerra no âmbito cibernético.

Por fim, o Segundo Comitê da Assembleia Geral da ONU tem o objetivo de unir a ação do Primeiro e Terceiro Comitês, por meio do desenvolvimento de cultura de segurança cibernética que una os lados político-militar com o econômico da sociedade internacional. (MAURER, 2011, p.17).

ILUSTRAÇÃO 6 - Processo de elaboração de normas de segurança cibernética na Assembleia Geral da ONU

Fonte: MAURER, 2011, p.15.

Em outubro de 2013, as discussões travadas nos Comitês e órgãos da ONU, sobre a segurança cibernética, começaram a produzir frutos significativos com a aprovação consensual da “Relatório sobre os desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional”. Esse documento representa uma importante conquista para a manutenção da paz internacional e a estabilidade no ciberespaço.

O documento 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). O relatório estabelece uma base sólida para os Estados-Membros enfrentarem os riscos mútuos que surgem de forma emergente com a evolução das tecnologias e, consequentemente, ameaças cibernéticas à paz.

7.2.2 *A Convenção do Conselho Europeu sobre Crime Cibernético de 2001*

Na Europa, a união regional para uma defesa internacional conjunta tem sido o objetivo desde o Tratado de Amsterdã, entretanto, a evolução social e jurídica das relações internacionais e os problemas emergentes da guerra cibernética apresentam-se como desafios a serem enfrentados na luta pela segurança do continente.

O Conselho Europeu, instituição da União Europeia que reúne os chefes de Estado e de Governo dos países para debater as prioridades políticas da organização internacional regional, tem desenvolvido um avanço considerável na regulação de políticas de segurança cibernética.

A União Europeia tem defendido a ideia de que investir em segurança cibernética, ao proteger suas redes de sistemas de informação, é essencial para garantir a prosperidade, manter a economia online em execução e evitar ataques indesejados que possam desestabilizar suas relações soberanas. (PAKALNIŠKIS, 2011, p.28).

A União Europeia trabalha em várias frentes para garantir a segurança cibernética na Europa, desde fornecer a entrega da Internet com melhor qualidade para os usuários até a negociação de tratados de cooperação internacional sobre segurança cibernética e cibercrimes. (PAKALNIŠKIS, 2011, p.28).

A conhecida como Convenção de Budapeste sobre o Cibercrime, de 2001, foi o primeiro tratado internacional a abordar a questão da segurança cibernética, tendo sido elaborada no âmbito do Conselho Europeu. O objetivo da Convenção é estabelecer uma "uma política criminal comum visando a proteção da sociedade contra a cibercriminalidade" através do direito e da cooperação internacionais. (CONSELHO EUROPEU, 2001, tradução nossa)[101].

A Convenção permite que Estados não europeus ratifiquem o tratado internacional, sendo que os Estados Unidos o ratificou e, desde a sua criação, existem pressões para a ratificação do Brasil. Posteriormente, em 2003, foi aprovado o Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Atos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos. O Protocolo tem um texto mais polêmico, pois grande parte

[101] "a common criminal policy aimed at the protection of society cybercrime” (CONSELHO EUROPEU, 2001).

dos Estados entenderam que o seu texto é limitador da liberdade de expressão e resolveram não ratificá-lo. (PAKALNIŠKIS, 2011, p.28).

No âmbito da defesa cibernética, a União Europeia não tem autoridade formal no campo da proteção de infraestruturas de informação crítica do ciberespaço contra a guerra, contudo encara essas ameaças através do exercício de suas competências no que diz respeito à defesa de interesses do bloco. Mesmo não tendo um órgão central, específico, que cuide da defesa no ciberespaço, a União Europeia já se debruça sobre a questão de forma indireta com base no princípio de autopreservação da vontade soberana do bloco e dos Estados.

Em 2004, ao sentir a necessidade de ter um órgão responsável para gerir a segurança das informações dos entes privados europeus, foi criada a Agência Europeia para a Segurança das Redes e da Informação (ENISA). (SCHIBBERGES, 2015, p.18).

A ENISA cuida da segurança cibernética dos sujeitos não estatais e dos cidadãos europeus dotados do direito humano à privacidade de seus dados, muitas vezes violados pelo meio eletrônico. A segurança cibernética que envolve todas as medidas necessárias para proteger os sistemas de computador contra o acesso não autorizado, ataques ou fracasso é o objeto de defesa dessa agencia europeia. A ENISA é colocada como a chave para o monitoramento das relações cibernéticas da Europa com o mundo, estabelecendo-se como agência de apoio à União Europeia na defesa cibernética. A agência faz trabalho de prevenção, reação, mapeamento, análise, aconselhamento e comunicação de ameaças cibernéticas que possam atingir o cidadão ou pessoa jurídica de direito privado no exercício de suas liberdades no ciberespaço. (SCHIBBERGES, 2015, p.18).

Em 2014, o Parlamento Europeu adotou, com alterações, a diretiva em “alto nível de segurança de informações de rede em toda a União Europeia” proposta pela Comissão Europeia em 2013, ainda a ser aprovada pelo Conselho Europeu. Nas últimas resoluções aprovadas pelo Conselho, dentre elas a de segurança cibernética e defesa de 2012, a de estruturas militares de 2013 e a unificação de segurança cibernética de 2013, tem se reforçado a preocupação de acirrar a segurança do ciberespaço, na preservação dos interesses da União Europeia. (CIRLIG, 2015, p.9).

7.2.3 *A OEA e a estratégia de segurança cibernética interamericana*

A Organização dos Estados Americanos (OEA) tem manifestado a sua preocupação com as abordagens desconexas e não padronizadas que os Estados têm tomado em relação à guerra cibernética, dependendo de suas características econômicas, políticas, culturais, dentre outras.

A primeira manifestação oficial da OEA sobre a guerra cibernética foi em 1999, quando estabeleceu um grupo de trabalho sobre o crime cibernético, como o principal local de cooperação internacional na prevenção, investigação e repressão de crimes cibernéticos. Além disso, o fórum busca facilitar o intercâmbio de informações e experiências entre os seus membros e fazer as recomendações necessárias para melhorar e assegurar os esforços para combater esses crimes.

Em 2004, com o intuito de se atentar de forma institucionalizada para o perigo da guerra cibernética, a OEA elaborou, em sua Assembleia Geral, a Resolução intitulada: “A Estratégia Interamericana de Combate à Ameaça de Segurança Cibernética”. (OEA, 2004). O objetivo foi iniciar mudança de perspectivas e trabalhar a cultura de segurança cibernética no âmbito da organização. As aspirações futuras são assegurar que os Estados-membros da OEA tenham no Judiciário ferramentas necessárias para proteger os usuários de Internet e redes de informação. Além de se viabilizar a elaboração e promulgação de uma legislação eficaz de crimes realizados no ciberespaço, melhorando as dificuldades de acesso à justiça. (OEA, 2004).

7.2.4 *A China e a Organização de Cooperação de Xangai diante dos desafios do ciberespaço*

A Organização de Cooperação de Xangai (OCX) também tomou significativas ações preliminares para a cooperação na área de segurança cibernética. Na Declaração de Ecaterimburgo, de 2009, a OCX ressaltou a importância da segurança das informações internacionais no ciberespaço, como um dos elementos-chave para se estabelecer a segurança internacional. (OCX, 2009).

A OCX até agora tem adotado visão expansiva do conceito de ciberataques, ao afirmar serem ataques que usam a tecnologia para minar a estabilidade política.

As declarações da OCX são tímidas, como organização, com a exceção da China que tem se manifestado de forma mais incisiva, em prol de suas posições em relação à temática do ciberespaço.

Em 2014, a China abertamente demonstrou sua preocupação em colocar-se no centro dos debates sobre o futuro da governança da Internet. Em fevereiro do mesmo ano, o presidente Xi Jinping externou sua vontade de transformar a China em uma potência do ‘poder cibernético’ mundial. O escopo global destas ambições foi exibido em novembro de 2013, em uma reunião aberta, realizada na Primeira Conferência Mundial da Internet, em Wuzhen perto de Xangai.

A conferência foi para reforçar a influência da China no contexto internacional do ciberespaço, além de buscar apoio ao conceito de ‘soberania de Internet’, como parte dos argumentos de que a Internet deveria ser regulamentada pelos Estados-Membros. A declaração foi discretamente abandonada após protestos de alguns delegados ocidentais, mas algumas semanas depois, a China afirmou que vai perseverar na promoção da soberania de Internet como base para a governança cibernética.

De acordo com diplomatas em Pequim, a China está cada vez mais buscando negociar com outros governos soluções para problemas de natureza cibernética. A ideia é preservar a soberania dos Estados ao máximo nesse novo domínio e estender a jurisdição nacional também nesse domínio.

Como parte de sua estratégia de mudar regulamento da Internet para um sistema interestatal, a China está promovendo diversas iniciativas de lei a partir da ONU. Em setembro, o ministro Wang Yi aproveitou um reunião do Conselho de Segurança da ONU para requisitar a elaboração de um novo código de conduta para a indústria atuante no ciberespaço.

Isto ecoa anteriores esforços conjuntos por China e Rússia (e alguns aliados asiáticos Central) em Assembleia Geral para negociar um código de conduta para os Estados-Membros sobre segurança da informação. Em várias reuniões da ONU ao longo de 2014, a China deixou claro que continuará a usar todas as oportunidades que tiver em organismos internacionais para o debate da temática e para a colocação de sua solução: um direito cibernético interestatal.

7.2.5 *OTAN - Manual de Tallinn sobre as Leis Internacionais aplicáveis à Guerra Cibernética de 2013*

A Organização do Tratado do Atlântico Norte (OTAN) sempre preocupada com a defesa de suas informações e, em especial, com a manutenção de suas estratégias militares em segredo, encontra-se extremamente avançada na discussão da importância de políticas de defesa internacional. Entretanto, a ameaça da guerra cibernética é uma novidade na história humana e, por esse motivo, são novos os esforços da organização para se defender e regular suas relações nessa perspectiva. (HATHAWAY *et al*; 2012, p. 50).

O foco inicial na defesa contra a guerra cibernética concentra-se na relação da proteção das informações, mas, na atualidade, a OTAN preconiza que a guerra cibernética vai além da espionagem por meio eletrônico. (HATHAWAY *et al*; 2012, p. 50).

A OTAN iniciou suas discussões sobre o problema da segurança cibernética em 2002 e expandiu seu foco dos sistemas organizacionais para os sistemas de informações criando o órgão conhecido como 'Autoridade de Defesa Cibernética'[102]. Esse organismo foi substituído pelo 'Órgão de Administração de Defesa Cibernética'[103] que tem o objetivo de centralizar as capacidades operacionais de defesa no ciberespaço dos Estados membros do bloco e traçar estratégias diante da nova realidade internacional. Há também o Centro de Ciberdefesa Cooperativa de Excelência[104] da OTAN que busca a discussão de novas estratégias de defesa com os Estados membros da organização e Estados associados. (HATHAWAY *et al*; 2012, p. 50).

Em 2013, foi publicado o 'Manual de Tallinn sobre as Leis Internacionais aplicáveis à Guerra Cibernética' em uma parceria do Centro de Ciberdefesa Cooperativa de Excelência da OTAN com a Universidade de Cambridge.

O Manual de Tallinn é primeira tentativa de se examinar quais seriam as leis atuais de guerra capazes de serem aplicáveis ao domínio do ciberespaço e conta com a participação de vinte acadêmicos de Direito Internacional que se debruçaram sobre a temática e estabelecem 95 (noventa e cinco) regras para a

[102] NATO's Cyber Defence Management Authority (CDMA)

[103] NATO Cyber Defense Management Board (CDMB)

[104] Cooperative Cyber Defence Centre of Excellence

convivência no ciberespaço. As primeiras dezenove regras são divididas em regras de *jus ad bellum* e tratam da segurança no ciberespaço as demais regras falam, mais especificamente, do conflito armado e sua regulação no âmbito cibernético. (SCHMITT, 2013, p.1-5).

Entretanto, questiona-se qual seria a intenção da OTAN de fazer essa parceria com Universidade de Cambridge, pois por mais que o Manual seja extremamente tentador de ser utilizado como parâmetro para o estudo e base para produção normativa internacional o fato de ter sido encomendado pela OTAN, inspira ressalvas ideológicas.

7.2.6 *O Brasil e a sua regulação jurídica diante de uma possível guerra cibernética*

Em 18 de dezembro de 2008, foi promulgado e publicado o Decreto 6.703 que aprova a Estratégia Nacional de Defesa e demonstra, claramente, a preocupação brasileira com a nova realidade da ameaça cibernética. O Brasil reitera, no decreto, o seu compromisso com a solução pacífica de controvérsias, com a paz, a não intervenção como valores consagrados pelo povo brasileiro. A estratégia baseia-se na defesa e não na guerra, uma vez que a preocupação do dispositivo legal é a sobrevivência do povo brasileiro diante dos novos dilemas da contemporaneidade. O Brasil defende a “independência nacional, alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear”. (BRASIL, 2008).

O Estado brasileiro vai além, ao afirmar que “não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento”. (BRASIL. 2008). A abordagem da defesa é inclusive sistêmica, pois o texto normativo prevê:

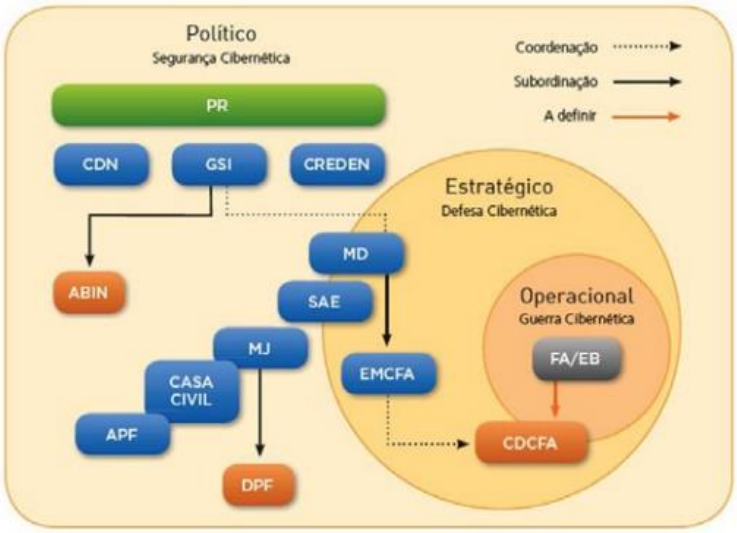
> Ao lado da destinação constitucional, das atribuições, da cultura, dos costumes e das competências próprias de cada Força e da maneira de sistematizá-las em estratégia de defesa integrada, aborda-se o papel de três setores decisivos para a defesa nacional: o espacial, o cibernético e o nuclear. Descreve-se como as três Forças devem operar em rede - entre si e em ligação com o monitoramento do território, do espaço aéreo e das águas jurisdicionais brasileiras. (BRASIL, 2008).

No Estado brasileiro há uma série de instituições estatais que cuida da segurança, no ciberespaço, ao combater desde pequenos crimes de vandalismo até à preservação da soberania por meio do combate à guerra cibernética.

A estrutura de defesa é hierarquizada, em diferentes instituições com competências específicas. A Presidência da República, responsável pela representação internacional do Estado brasileiro e pela gestão das forças armadas, comanda as estratégias de defesa. O Gabinete de Segurança Institucional (GSI), no topo da pirâmide hierárquica e em contato direto com a Presidência da República, é o órgão encarregado de lidar com todos os aspectos civis de segurança cibernética. Também é responsável por assuntos militares e pela defesa cibernética que faz parte do Conselho de Defesa Nacional, o CDN. O Departamento de Segurança da Informação e Comunicações (DSIC) é subordinado ao GSI e responsável por garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicação para a administração pública federal. Isto é coordenado em estreita consulta à Casa Civil, que também é responsável por supervisionar a concessão de certificados de segurança digital. Também dentro do GSI estão a Secretaria de Assuntos Estratégicos (SAE) e a Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (CREDEN), uma Comissão Consultiva para o Presidente. (DINIZ, MUGAH, GLENNY, 2005, p.17).

Outra instituição importante é o Departamento de Polícia Federal (DPF), sob a supervisão do Ministério da Justiça (MJ). Enquanto seu papel principal consiste na aplicação da lei federal, também tem unidades dedicadas à segurança cibernética. Além disso, a Agência Brasileira de Inteligência (ABIN), juntamente com o Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC), é responsável pela defesa e ataque nos casos de espionagem cibernética. Por fim, há o Ministério da Defesa (MD) que supervisiona as forças armadas e serve como um elo de ligação entre civis e militares na defesa da soberania do Estado brasileiro. (DINIZ, MUGAH, GLENNY, 2005, p.18).

ILUSTRAÇÃO 7 – Estrutura de Defesa Cibernética Brasileira



Fonte: (DINIZ, MUGAH, GLENNY, 2005, p.19).

Em abril de 2014, foi publicada a Lei 12.965, conhecida como Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Esta lei é um avanço no tratamento das relações privadas no ciberespaço, mas não abrange a temática da guerra cibernética.

8 CONCLUSÃO

O Direito Internacional vê-se desafiado pela nova realidade das relações interativas dos atores, no ciberespaço. Os conceitos lineares, baseados na ótica cartesiana, positivista, do Direito Internacional clássico, não conseguem solucionar sozinhos os novos desafios da Era Cibernética. É um momento de rupturas de paradigmas jurídicos, nos quais o Direito Internacional continua sendo aquele que regula a sociedade internacional, mas percebe-se um alargamento dos sujeitos ativos, passíveis de alterar a ordem das relações, por meio da interatividade cibernética.

Conclui-se pela potencialização da complexidade da sociedade internacional, no ciberespaço, por meio da constatação da grande diversidade dos sistemas legais e da heterogeneidade dos atores globais que se relacionam de forma interativa no meio virtual.

A complexidade das relações no ciberespaço leva a um aumento das fontes de Direito Internacional, no novo paradigma. As fontes tradicionais de Direito Internacional não são descartadas, mas surgem novas fontes de direito para a solução dos impasses apresentados pelos desafios do ciberespaço. A multiplicação das fontes ocorre com a influência das leis nacionais dos Estados, há via de consequência, intercruzamento normativo entre o direito interno e o Direito Internacional, com o objetivo de combater problemas comuns entre eles. As políticas de integração entre Estados, o reconhecimento da existência de normas de *jus cogens* e as alianças políticas pautadas nas disputas de poder, também são fatores que levam ao aumento das fontes de direito, no ciberespaço.

O desenvolvimento do ciberespaço se transforma em um desafio para o Direito Internacional a partir do momento em que a realidade internacional, pautada na insatisfação dos Estados, com a distribuição do poder, pode transformar esse espaço desenvolvido pelo homem, em um campo de guerra. A manipulação do poder, em prol da modificação do equilíbrio internacional, passa a ser também uma manipulação do ‘cyber power’, que trabalhado em conjunto com o ‘hard power’ e ‘soft power’ pode levar à mudança das relações políticas internacionais.

Os Estados, cientes de que o poder cibernético pode lhes ajudar na atuação, no âmbito das relações internacionais, buscam a dominação hegemônica política, no espaço cibernético e, também, em outros domínios, que se encontram fora do

mundo cibernético. O ideal para o Estado, que almeja mais poder, no cenário internacional, é utilizar-se de forma inteligente da força, da diplomacia e do ‘poder cibernético’, em prol dos seus objetivos.

O presente trabalho é fruto, portanto, da análise crítica do ciberespaço como uma nova fronteira da guerra, devendo ser, assim, objeto de regulação pelo Direito Internacional, em favor da defesa dos direitos, nos casos de possíveis guerras cibernéticas.

O ciberespaço e a noção de uma sociedade internacional complexa, envolvendo atores variados que interagem em rede, no âmbito cibernético internacional, faz com que surjam definições mais abrangentes da expressão ‘estado de guerra’, vinculadas à pluralização dessa sociedade. A existência de um estado de guerra, entre atores internacionais, não está mais vinculada à logica centralizadora da guerra somente entre Estados, pois há um aumento de possibilidades de novos atores promoverem a guerra, mesmo os não identificados como sujeitos de Direito Internacional.

A soberania ganha nova roupagem na sociedade cibernética internacional, organizada por meio da sistemática da *autopoiesis*. A soberania, no sistema autopoiético, é a possibilidade de utilizar-se das identidades e diversidades, para tomar suas próprias decisões, sem a aplicação de conceitos dotados de imposições universalistas territoriais.

Ou seja, não é possível um sistema estatal importar as identidades e diferenças do mundo exterior ou de outros Estados. As decisões devem ser tomadas por meio da interação entre povos e instituições estatais, sem a violação do diálogo democrático. A soberania, no ciberespaço, é respeitada a partir do momento que se permite a interação democrática popular e a discussão dialética das decisões jurídicas internas e internacionais, sobre os rumos dos Estados. Na teoria dos sistemas, a permissão da interação e a construção de identidades estatais é o verdadeiro exercício de soberania, pilar para o Direito Internacional.

O uso de força, no âmbito do ciberespaço, é outro ponto polêmico discutido no trabalho, pois sua caracterização leva ao início da guerra e permitiria o exercício da legítima defesa, nos ditames da Carta da ONU. Ao avaliar se um evento no ciberespaço constituiu ou não o ‘uso de força’ ilegal, deve-se analisar todos os fatores envolvidos, incluindo o ator que o realizou, o seu contexto, os objetivos almejados, o alvo atingido, a localização territorial das consequências, os efeitos e

a intenção, entre outros possíveis problemas. A tendência é que não haja mais separação da aplicação das normas de Direito Internacional para os espaços físicos e para o ciberespaço, mas que as normas e princípios existentes sejam aplicados a esse novo domínio passível de regulação e imputação de responsabilidade jurídica internacional.

Apesar dos novos desafios trazidos pela guerra cibernética levantarem questões desafiadoras para as atuais leis de conflito armado, no âmbito internacional, na maior parte, as leis existentes são capazes de se adaptarem à nova tecnologia do ciberespaço. Não há um campo de batalha exclusivamente virtual, completamente dissociado da realidade do mundo real, no qual a guerra cibernética ocorra e que justifique a necessidade de uma legislação completamente nova para sua regulação.

A guerra ainda é vivida nos espaços físicos, mas também utiliza-se das redes virtuais para se propagar e provocar prejuízos de ruptura em massa. O principal desafio é de mudança metodológica de interpretação jurídica da realidade complexa do ciberespaço. Portanto, conclui-se que é possível valer-se da atual legislação de Direito Internacional para regular o ciberespaço, desde que se faça uma adaptação com o novo paradigma das relações interativas do sistema cibernético complexo.

Conclui-se pelo entendimento de que as fontes tradicionais de Direito Internacional, em especial, os princípios, podem ajudar em muito, na solução dos problemas oriundos da guerra cibernética. São princípios gerais de Direito Internacional aplicáveis ao ciberespaço com o intuito de coibir a guerra cibernética e preservar a paz: a igualdade soberana dos Estados, ao incluir o direito dos Estados de autopreservação, independência e respeito à jurisdição nacional. O princípio da não-intervenção nos assuntos da competência interna de outros Estados, ao coibir, inclusive a espionagem cibernética. A abstenção do uso de força ou ameaça nas relações internacionais; a solução pacífica de controvérsias e o dever (necessidade) de cooperação internacional na Resolução de problemas internacionais, em especial diante das ameaças do ciberespaço.

A análise dos esforços globais para combater as novas e crescentes ameaças, através de diferentes organismos internacionais, demonstram a dificuldade dos grupos internacionais em concordar com uma resposta global e abrangente e talvez essa não seja a melhor solução. A tendência ainda é buscar

uma resposta única e linear para a problemática, muito mais complexa do que as antes enfrentadas pela normatividade do Direito Internacional.

Além disso, a colocação de uma única solução global, para os diversos desafios que surgem com a temática da guerra cibernética, gera o desconforto da imposição de soluções arbitrárias. O problema da guerra cibernética, como sua realidade, deve ser solucionado, de forma democrática, por meio do diálogo entre os atores que participam das relações interativas e da aceitação de uma pluralidade normativa internacional. Por mais que seja tentador determinar uma única solução global para o problema, essa imposição apresenta-se como mais uma forma de violação de direitos na sociedade internacional, ainda dotada de políticas de dominação ideológica ou tecnológica.

Entende-se, finalmente, que a guerra cibernética está bem orientada pelos princípios basilares de Direito Internacional de preservação da paz e segurança, respeito à soberania dos Estados e não utilização da força. Entretanto, deve haver uma consciência da nova realidade das relações internacionais, no âmbito do ciberespaço, para que esse domínio virtual não seja utilizado como justificativa para a violação do Direito Internacional e da soberania dos Estados. A realidade sistêmica interativa, do novo Direito Internacional cibernético, requer a ruptura de paradigmas lineares do direito e a aplicação de uma ótica democrática e interativa soberana, com o aumento da participação popular na tomada de decisões no âmbito internacional.

REFERÊNCIAS

ABI-SAAB, Georges. The Specificities of Humanitarian Law. In: SWINARSKI, C. (ed.). **Studies and Essays on International Humanitarian Law and Red Cross Principles in Honour of Jean Pictet**. Genebra: The Hague, 1984, p.265–280.

ASHBY, W. Ross. **An introduction to cybernetics**. Londres: Chapman & Hall, 1956.

ASHBY, W. Ross. **Statistical Machinery**. Londres: Chapman & Hall, 1951.

ANDRESS, Jason; WINTERFELD, Steve. **Cyber Warfare**: techniques, tactics and tools for security practitioners. Waltham: Elsevier, 2011.

BACHELARD, Gaston. **A formação do espírito científico**: contribuição para uma psicanálise do conhecimento. Tradução Esteia dos Santos Abreu. Rio de Janeiro: Contraponto, 1996.

BALOCH, Farooq. **Cyber vandalism**: Hackers deface Google Pakistan. The Express Tribune with the International New York Times Online, Paquistão, 25 nov. 2012. Disponível em: <http://tribune.com.pk/story/470924/cyber-vandalism-hackers-deface-google-pakistan/>. Acesso em: 01 ago.2011.

BEER, Stafford. **Platform for change**. London: John Wiley & Sons, 1975.

BUONOMANO, D. V. & MERZENICH, M. M. **Cortical plasticity**: from synapses to maps. Annual Review of Neuroscience, Los Angeles, California, v. 21, p. 149-186, 1998.

BOURDIEU, Pierre. **O poder simbólico**. Tradução Fernando Tomaz. Rio de Janeiro: Bertrand, 1989.

BRASIL. **DECRETO Nº 64.362, DE 17 DE ABRIL DE 1969.** Promulga o Tratado sobre Exploração e Uso do Espaço Cósmico. Brasília: Senado Federal, 1969.

BRASIL. **Portaria Normativa nº 113 da Secretaria de Política, Estratégia e Assuntos Internacionais de 1º de fevereiro de 2007**. Brasília: Ministério da Defesa, 2007.

BRATE, Adam. **Technomanifestos**: visions from the information revolutionaries. Cheshire: Texere, 2002. 208p.

BRENNER, Susan W. **Cyberthreats**: the emerging fault lines of the Nation State. Oxford: Oxford University Press, 2009.

BROWNLIE, Ian. **Principles of Public International Law**. New York: Oxford University Press, 2002.

CASSESE, Antonio. **International Law**. New York: Oxford University Press, 2005.

CONSELHO EUROPEU. **Convention on Cybercrime (2001)**. Disponível em: <http://bsu.ase.ro/oldbsu/anexe/lectures2010/CSS_Analysis_71.pdf>. Acesso em: 19 fev. 2015.

CAVELTY, Myriam Dunn. **Cyberwar**: concept, status quo, and limitations. Disponível em: <http://bsu.ase.ro/oldbsu/anexe/lectures2010/CSS_Analysis_71.pdf>. Acesso em: 11 out. 2011.

CHO, Adrian. **Ourselves and Our Interactions**: The Ultimate Physics Problem? Washington: Science, 2009.

CHOUCRI, Nazli. **The Convergence of Cyberspace and Sustainability**. Disponível em: <http://www.e-ir.info/2012/04/20/the-convergence-of-cyberspace-and-sustainability/#_ftn1>. Acesso em: 17 fev. 2015.

CIRLIG, Carmem-Cristina. **Cyber defence in the EU**: Preparing for cyber warfare? Disponível em: < http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf>. Acesso em: 21 fev. 2015.

CLANCY, Erin A. The Tragedy of the Global Commons. In: **Indiana Journal of Global Legal Studies**: Vol. 5: n. 2, artigo 12. Disponível em: <http://www.repository.law.indiana.edu/ijgls/vol5/iss2/12>. Acesso em: 17 fev. 2015.

CLAPHAM, Andrew. **Non-state Actors**. New York: Oxford University Press, 2009.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber War**: The next threat to national security and what to do about it. Washington: Amazon Digital Services, 2010.

CLAUSEWITZ, Carl Von. **Da Guerra**. Tradução Luiz Carlos Nascimento e Silva do Valle. Disponível em: <http://pensamentosnomadas.files.wordpress.com/2012/11/da-guerra-carl-von-clausewitz.pdf>. Acesso em: 29 jun. 2014.

CORTE INTERNACIONAL DE JUSTIÇA. Decisão da Corte Internacional de Justiça no Caso das Atividades Militares e Paramilitares na e Contra a Nicarágua (Nicarágua e Estados Unidos da América) de 1984-1991. Disponível em: <http://www.cedin.com.br/wp-content/uploads/2014/05/casos-conteciosos_1984_01.pdf>. Acesso em: 30 jan. 2015.

CORTE INTERNACIONAL DE JUSTIÇA. Decisão da Corte Internacional de Justiça no Caso do Canal de Corfu entre Reino Unido e Albânia de 1947. Disponível em: <http://sinus.org.br/2014/wp-content/uploads/2013/11/CIJ-Guia-online.pdf>. Acesso em: 15 fev. 2015.

CRIDDLE, Evan J.; FOX-DECENT, Evan. **A Fiduciary Theory of Jus Cogens**. Yale Journal of International Law, vol. 34, 2009.

CÚPULA MUNDIAL DA SOCIEDADE DA INFORMAÇÃO. **Relatório da Cúpula Mundial da Sociedade da Informação (2005)**. Disponível em: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>. Acesso em: 24 jan. 2015.

DE JOMINI, Antoine-Henri. **The Art of War**. Radford: Wilder, 2008.

DELMAS-MARTY, Mireille. **Três Desafios para um Direito Mundial***.* Tradução Fauzi Hassan Choukr. Rio de Janeiro: Lumen Juris, 2003.

DELMAS-MARTY, Mireille. **Internationalization of Law**: diversity, perplexity, complexity. Palestra proferida na American Society of International Law em 29 de março de 2012. Disponível em: <http://www.intlawgrrls.com/2012/03/internationalization-of-law-diversity.html>. Acesso em: 27 jun. 2014.

DINH, Nguyen Quoc; DAILLIER, Patrick; PELLET, Alain. **Direito Internacional Público**. Tradução Vítor Marques Coelho. Lisboa: Funsação Calouste Gulbenkian, 2003.

DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. Estrutura de Defesa Cibernética Brasileira. **Deconstructing Cyber Security in Brazil**: Threats and Responses. Disponível em: < http://en.igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf>. Acesso em: 01 mar. 2015.

DINNISS, Heather Harrison. **Cyber Warfare and the Laws of War**. Cambridge: Cambridge University Press*,* 2012.

DODGE, Martin; KITCHIN, Rob. **Atlas of Cyberspace**. Grã-Bretanha: Pearson Education Limited, 2001.

DUSSEL, Enrique. **1492: el encubrimiento del otro** - hacia el origen del mito de la modernidad. La Paz: Plural Editores, 1994.

ECOSOC – CONSELHO ECONOMICO E SOCIAL DAS NAÇÕES UNIDAS. **Navy Cyber Forces Mission Statement.** Disponível em: <http://www.public.navy.mil/fltfor/cyberfor/Pages/MISSION%20STATEMENT.aspx>. Acesso em: 09 jan. 2015.

ENGHELBERG, Hedi. **The evolution and fight against cyber terrorism a precision-delivery weapon**. Tradução para o inglês por Gail Tenzer. Washington: Edições Enghelberg, 2012.

ESTADOS UNIDOS DA AMÉRICA. **Navy Cyber Forces Mission Statement.** Disponível em: <http://www.public.navy.mil/fltfor/cyberfor/Pages/MISSION%20STATEMENT.aspx>. Acesso em: 09 jan. 2015.

ESTADOS UNIDOS DA AMÉRICA. **Department of Defense Cyberspace Policy Report:** a report to Congress pursuant to the national defense authorization

act for fiscal year 2011, section 934. Disponível em: <http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf>. Acesso em: 19 jan. 2015.

EZEKIEL, Alan W. Hackers, Spies, and Stolen Secrets: protecting law firms from data theft. **Harvard Journal of Law & Technology**, Cambridge, v. 26, n. 2, p.649-668, 2013.

FÓRUM ECONÔMICO MUNDIAL. **Global Risks 2014**. Genebra: Fórum Econômico Mundial, 2014. Disponível em: <file:///C:/Users/Felipe%20Furtado/Desktop/RENATA/WEF_GlobalRisks_Report_2014.pdf>. Acesso em: 19 jun. 2014.

FOUCAULT, Michel. **Em Defesa da Sociedade**. Tradução Maria Ermantlna Galvão. São Paulo: Martins Fontes, 2005.

FRANZESE, Lieutenant Colonel Patrick W. Sovereignty in cyberspace: can it exist? **Air Force Law Review**. Disponível em: <https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist>. Acesso em: 12 jan. 2015.

FULLER, John Frederick Charles. **The Foundations of the Science of War**. Kansas: U.S. Army Command and General Staff College Press, 1993.

GLENNY, Misha. **DarkMarket**: Cyberthieves, Cybercops and You. Toronto: Anansi Press, 2011.

GROTIUS, Hugo. **O Direito da Guerra e da Paz.** (1625). Tradução Ciro Mioranza. Florianópolis: Unijuí, 2004.

HAIA. **Convenção sobre a Resolução Pacífica de Controvérsias Internacionais (1907)**. Disponível em: <https://www.icrc.org/ihl/INTRO/195>. Acesso em: 19 jan. 2015.

HAYLES, N. Katherine. **Chaos bound**: orderly disorder in contemporary literature and science. Ithaca: Cornell University, 1991.

HOBBES, Thomas. **Leviatã**. Tradução João Paulo Monteiro e Maria Beatriz Nizza da Silva. 4 ed. São Paulo: Nova Cultural, 1988.

HATHAWAY, Oona A. *et al*. The Law of Cyber-Attack In: **California Law Review**, 2012. Disponível em: <http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf>. Acesso em: 18 fev. 2015.

HOFFMAN, Abbie. **Revolution for the Hell of It**. Boston: Da Capo Press, 2005.

HOMER-DIXON, Thomas. **The Upside of Down**: catastrophe, creativity, and the renewal of civilization. Toronto: Vintage Canada, 2006.

HULME, George V. **A Decade Ago, ILoveYou Worm Changed Security**. Disponível em: <http://www.darkreading.com/risk-management/a-decade-ago-iloveyou-worm-changed-security/d/d-id/1088821?>. Acesso em: 30 jan. 2015.

IAN. **Sony hacking**: cyber vandalism or cyber terrorism? Disponível em: <http://www.business-standard.com/article/news-ians/sony-hacking-cyber-vandalism-or-cyber-terrorism-comment-special-to-ians-114122300401_1.html>. Acesso em: 18 jan. 2015.

ICANN - CORPORAÇÃO DA INTERNET PARA ATRIBUIÇÃO DE NOMES E NÚMEROS. **Annual Report 2013:** a new season at ICANN. Disponível em: <https://www.icann.org/en/system/files/files/annual-report-2013-en.pdf>. Acesso em: 17 fev. 2015.

JANIS, Mark W.; NOYES, John E. **International Law**: cases and commentary. St. Paul: West Group, 2001.

JENSEN, Eric Talbot. **Sovereignty and Neutrality in Cyber Conflict**. New York: Fordham International Law Journal, 2011. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1952598>. Acesso em: 08 jul. 2014.

JERVIS, Robert. **System Effects**: Complexity in Political and Social Life. Princeton: Princeton University Press, 1997.

KANUCK, Sean. Sovereign Discourse on Cyber Conflict Under International Law. In: **Texas Law Review**, v.88, 2010. Disponível em: <https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Kanuck.pdf>. Acesso em: 22 jan. 2015.

KEOHANE, Robert O.; NYE JR., Joseph S. **Power and Interdependence**. New York: Longman, 1977.

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

KUHN, Thomas S. **A estrutura das revoluções científicas**. Tradução Beatriz Vianna Boeira e Nelson Boeira. São Paulo: Perspectiva, 1970.

LIBICKI, Martin C. **Cyberdeterrence and cyberwar**. Santa Monica: RAND Corporation, 2009.

LORENZ, Edward. **Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?** 139º Encontro da Associação Americana para o Avanço da Ciência. Washington: 1972. Disponível em: <http://eaps4.mit.edu/research/Lorenz/Butterfly_1972.pdf>. Acesso em: 13 jun. 2014.

LUGO, William. Violent video games recruit American youth. In: **Reclaiming Children & Youth**, volume 15, number 1, 2006. Disponível em:

<http://nutmeg.easternct.edu/~lugow/courses/videogames/America's%20Army.pdf>. Acesso em: 08 jul. 2014.

LUHMANN, Niklas. **Law as a Social System**. Tradução: KLAUS A. ZIEGERT. Oxford, Oxford University Press, 2004. 498 p.

LUHMANN, Niklas. **The Autopoiesis of Social Systems**. London, 1986, 172p.

LYNN III, William J. Defending a New Domain: The Pentagon's Cyberstrategy. **Foreign Affairs Magazine**. Washington, v. 89, n.5, p. 97-108, set./out. 2010.

MORIN, Edgar; ALMEIDA, Maria da Conceição de; CARVALHO, Edgard de Assis. **Educação e complexidade:** os sete saberes e outros ensaios. São Paulo: Cortez, 2002.

MACHADO, Jonathan D. **O que é firewall?** Disponível em: <http://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm>. Acesso em: 18 fev. 2015.

MAGALHÃES, Jose Luiz Quadros de. **Direito Constitucional**: curso de direitos fundamentais. São Paulo: Método, 2008.

MAGALHÃES, José Luiz Quadros. **Plurinacionalidade e cosmopolitismo**: a diversidade cultural das cidades e diversidade comportamental nas metrópoles. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=14564>. Acesso em: 20 jun. 2014.

MCDOUGAL, Myres S.; FELICIANO, Florentino P. International Coercion and World Public Order: The General Principles of the Law of War (1958). In: **The Yale Law Journal**, v.57, n.5. Disponível em: <http://www.army.mil/article/12072/army-experience-center-opens-in-philadelphia/>. Acesso em: 26 jan. 2015.

MCLEROY, Carrie. **Army Experience Center opens in Philadelphia**. Disponível em: <http://www.army.mil/article/12072/army-experience-center-opens-in-philadelphia/>. Acesso em: 09 jan. 2015.

MCLUHAN, Marshall. **Understanding Media**: the extensions of man. New York: McGraw-Hill, 1964.

MARTINS, Elaine. **O que é um worm?** Disponível em: <http://www.tecmundo.com.br/antivirus/206-o-que-e-um-worm-.htm>. Acesso em: 30 jan. 2015.

MATURANA, Humberto R.; VARELA, Francisco J. ***Autopoiesis* and Cognition**: the realization of the living. Nova York: Reidel, 1980.

MATURANA, Humberto. **Emoções e Linguagem na Educação e na Política**. Belo Horizonte: Ed. UFMG, 1998.

MATURANA, Humberto R. **La objetividad**: un argumento para obligar. Chile, Domen Ediciones, 1997.

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: 18 fev. 2015.

MEARSHEIMER, John J. **A Tragédia Política das Grandes Potências**. Lisboa: Gradiva, 2007.

NICOLAÏDIS, Kalypso; TONG, Jouyce L. **Diversity or Cacophony? The Continuing Debate over New Sources of International Law.** Oxford: Oxford University Press, 2014. Disponível em: <http://www.sant.ox.ac.uk/people/knicolaidis/nicolaidis% 20tong.pdf>. Acesso em: 29 jun. 2014.

NYE Jr, Joseph S. **Soft power**. Washington: Public Affairs, 2004.

NYE Jr, Joseph S. **The future of power**. Washington: Public Affairs, 2010.

NYE Jr, Joseph S. **The powers to lead**. New York: Oxford University Press, 2008.

OBAMA, Barack. **Presidential Proclamation**: National Cybersecurity Awareness Month. Washington: out. 2011. Disponível em: <http://www.whitehouse.gov/the-press-office/2011/10/03/presidential-proclamation-national-cybersecurity-awareness-month>. Acesso em: 09 out. 2011.

O'BRIEN, William V. **Just War Doctrine's Complementary Role in the International Law of War**. Disponível em: <file:///Users/renatabarros/Downloads/vol-67_VII_OBrien_Just_War_Doctrine-s_Complementary_Role.pdf>. Acesso em: 30 jan. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Carta da ONU. (1945).** Disponível em: <http://unicrio.org.br/img/CartadaONU_VersoInternet.pdf>. Acesso em: 27 jun. 2014.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Convenção das Nações Unidas sobre o Direito do Mar. (1982).** Disponível em: <http://www.un.org/depts/los/convention_agreements/texts/unclos/closindx.htm>. Acesso em: 17 fev. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração de Salvador (2010).** Disponível em: <https://blogdovladimir.files.wordpress.com/2010/04/declaracao-de-salvador-12-un-crime-congress.pdf>. Acesso em: 07 jan. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Estatuto da Corte Internacional de Justiça. (1945).** Disponível em: <http://unicrio.org.br/img/CartadaONU_ VersoInternet.pdf>. Acesso em: 27 jun. 2014.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Estudo Compreensivo sobre crimes cibernéticos (2013).** Disponível em: <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf >. Acesso em: 07 jan. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Protocolo Facultativo à Convenção sobre os direitos da criança relativo à participação de crianças em conflitos armados (2002).** Disponível em: <http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPACCRC.aspx>. Acesso em: 09 jan. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Relatório de Brundtland (1987)**. Disponível em: <http://www.un-documents.net/wced-ocf.htm>. Acesso em: 17 fev. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Resolução 53/70 sobre desenvolvimentos no campo da informação e telecomunicações no contexto de segurança internacional (1998)**. Disponível em: <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70>. Acesso em: 26 jan. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Resolution 60/288 on The United Nations Global Counter-Terrorism Strategy (2006)**. Disponível em: <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/288>. Acesso em: 18 fev. 2015.

ORGANIZAÇÃO DE COOPERAÇÃO DE XANGAI (OCX). **Acordo entre os governos dos Estados-membros da OCX na cooperação em matéria de garantir a segurança de informações internacionais (2008)**. Disponível em: <https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf>. Acesso em: 24 jan. 2015.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). **Carta da Organização dos Estados Americanos**: (Reformada pelo Protocolo de Buenos Aires em 1967, pelo Protocolo de Cartagena das Índias em 1985, pelo Protocolo de Washington em 1992, e pelo Protocolo de Manágua em 1993 e Protocolo de Washington em de 1997). 1997. Disponível em: <http://www.oas.org/juridico/portuguese/carta.htm>. Acesso em: 01 fev. 2015.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). **A Estratégia Interamericana de Combate à Ameaça de Segurança Cibernética (2004)**. Disponível em: <https://ccdcoe.org/sites/default/files/documents/OAS-040608-InterAmericanCyberSecurityStrategy.pdf>. Acesso em: 28 fev. 2015.

ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). **Regulamento Sanitário Internacional (2005).** Disponível em:

<http://portal.anvisa.gov.br/wps/wcm/connect/fe029a0047457f438b08df3fbc4c6735/Regulamento+Sanitario+Internacional+versao+para+impressao+090810.pdf?MOD=AJPERES>. Acesso em: 18 fev. 2015.

QUINTÃO SOARES, Mário Lúcio. **Direitos Fundamentais e Direito Comunitário**: por uma metódica de direitos fundamentais aplicada às normas comunitárias. Belo Horizonte: Del Rey, 2000.

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

ROSE, Joel. **The Army Experience Center**: Mission accomplished? Disponível em: < http://www.marketplace.org/topics/business/army-experience-center-mission-accomplished>. Acesso em: 09 jan. 2015.

STEIN, Janice. Social and Electronic Networks in the War on Terror. In: LATHAM, Robert. **Bombs and Bandwidth**: the Emerging Relationship between IT and Security, New York: Free Press, 2003. Disponível em: <https://books.google.com.br/books?id=tE8_S9K3jVQC&pg=PA271&lpg=PA271&dq=Social+and+Electronic+Networks+in+the+War+on+Terror>. Acesso em: 23 jan. 2015.

UNIVERSIDADE DE OXFORD. **Oxford Dictionaries**. Disponível em: <http://www.oxforddictionaries.com/definition/english/cyberespionage>. Acesso em: 05 de jul. 2014.

PAKALNIŠKIS, Saulius. What factors explain why there is not a common and comprehensive global response to cyber threats? Holanda: Leiden University Press, 2011. Disponível em: <http://www.naavi.org/pati/pati_cybercrimes_dec03.htm>. Acesso em: 18 fev. 2015.

PARTHASARATHI, Pati. **Cyber crime**. Disponível em: <http://www.naavi.org/pati/pati_cybercrimes_dec03.htm>. Acesso em: 11 out. 2011.

PISA, Pedro. **O que é IP?**. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-ip.html>. Acesso em: 17 fev. 2015.

POPPER, Karl R. **A lógica da pesquisa científica**. Tradução Leonidas Regenberg e Octanny Silveira da Mota. São Paulo: Pensamento Cultrix, 1972.

PREBLE, Christopher. **The DNA of global power**. Washington: World Politics Review, 2011.

PRIGOGINE, Ilya. **As leis do caos**. Tradução Roberto Leal Ferreira. São Paulo: UNESP, 2002.

PRIGOGINE, Ilya. **O fim das certezas**. Tradução Roberto Leal Ferreira. São Paulo: UNESP, 1996.

ROLAND, Alex. **Technology and War**. Disponível em: <http://www.unc.edu/depts/diplomat/AD_Issues/amdipl_4/roland.html>. Acesso em: 26 de jan. 2015.

ROSENAU, James N. **Along the Domestic-Foreign Frontier**: exploring governance in a turbulent world. Cambridge: Cambridge University Press, 1997.

ROSENAU, James N. **Turbulence in World Politics**: a theory of change and continuity. Princeton: Princeton University Press, 1990.

ROOT, Hilton L. **Dynamics among Nations**: The Evolution of Legitimacy and Development in Modern States. Cambrige: MIT Press, 2013.

ROTHKOPF, David J. **Cyberpolitik: The Changing Nature of Power in the Information Age.** Disponível em: <http://www.foreignpolicy.com/articles/2010/02/22/the_new_rules_of_war>. Acesso em: 12 out. 2011.

SCHIBBERGES, Julian. **Governance and Cyberwar**: the role of the European Union. Disponível em: <http://essay.utwente.nl/62960/1/BA-Julian_Schibberges.pdf>. Acesso em: 21 fev. 2015.

SCHMITT, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warefare**. Cambridge: Cambridge University Press, 2013.

SHAW, Malcolm N. **Direito Internacional**. Tradução Marcelo Brandão Cipolla, Lenita Ananias do Nascimento, Antônio de Oliveira Sette-Câmara. São Paulo: Martins Martins Fontes, 2010.

SOLOMON, Brett; MITNICK, Drew. **The dangers of a militarized internet**. Disponível em: <https://www.accessnow.org/blog/2014/12/08/the-dangers-of-a-militarized-internet>. Acesso em: 23 de jan. de 2015.

SPADE, Paul Vincent. **Ockham's Nominalist Metaphysics**: Some Main Themes. In: The Cambridge Companion to Ockham. Ed. Paul Vincent Spade. New York: Cambridge University Press, 1999, p. 100-117.

TETLEY, William. **Mixed jurisdictions**: common law vs civil law (codified and uncodified). Disponível em: <http://www.cisg.law.pace.edu/cisg/biblio/tetley.html>. Acesso em: 18 fev. 2015.

TORQUE COMUNICAÇÃO E INTERNET. **Glossário de termos usados na Internet**. Disponível em: <http://www.torque.com.br/internet/glossario.htm/>. Acesso em: 09 jul. 2015.

TZU, Sun. **A Arte da Guerra**. Tradução do chinês para o francês pelo padre Amiot em 1772. Traduzido do francês por Sueli Barros Cassal. Porto Alegre: L&PM, 2006.

UNIÃO EROPEIA. **Tratado de Lisboa**. União Europeia, 2007.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES (UIT). **Constituição e a Convenção da União Internacional de Telecomunicações, concluídas em Genebra, em 22 de dezembro de 1992, e seu instrumento de Emenda aprovado em Quioto, em 14 de outubro de 1994**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D2962.htm>. Acesso em: 01 de fev. de 2015.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES (UIT). **ITU Global Cybersecurity Agenda (2007)**. Disponível em: <http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf>. Acesso em: 18 de fev. de 2015.

U.S. DEPARTMENT OF DEFENSE. **Cybersecurity**. Washington: 2011. Disponível em: <http://www.defense.gov/home/features/2010/0410_cybersec/>. Acesso em: 09 de out. de 2011.

VARELLA, Marcelo Dias. **Internacionalização do Direito**: Direito Internacional, globalização e complexidade. Brasília: UniCEUB, 2013. Disponível em: <http://www.marcelodvarella.org/marcelodvarella.org/Teoria_do_Direito_Internacional_files/Internacionalizacao_do_direito_PDF_final%20%281%29.pdf>. Acesso em: 27 jun. 2014.

VASCONCELLOS, Maria José Esteves de. **Pensamento sistêmico**: o novo paradigma da ciência. Campinas: Papirus, 2002.

VITALI, Stefania; GLATTFELDER, James B.; BATTISTON, Stefano. **The network of global corporate control**. Revista New Scientist de Londres, 2011. Disponível em: <file:///C:/Users/Felipe%20Furtado/Desktop/1107.5728.pdf>. Acesso em: 19 jun. 2014.

WALDROP, M. Mitchell. **Complexity**: the emerging science at the edge of order and chaos. New York: Simon & Schuster Paperbacks, 1991.

WALLERSTEIN, Immanuel. **O Universalismo Europeu**. São Paulo: Boitempo, 2007.

WALLERSTEIN, Immanuel. **World-Systems Analysis**: an introduction. Durham: Duke University Press, 2004.

WAXMAN, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future. **The Yale Journal of International Law**. Disponível em: <http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf>. Acesso em: 19 jan. 2015.

WEAWER, Warren. **Science and complexity**. American Scientist Magazine. North Carolina: Sigma Xi, The Scientific Research Society, 1948.

WENDT, Emerson. Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos. **Revista Brasileira de Inteligência** / Agência Brasileira de Inteligência. n.6 (abr. 2011). Brasília: ABIN, 2011.

WIENER, Norbert. **Cibernética**. Tradução Prof. Gita K. Ghinzberg. São Paulo: Polígono o e Universidade de São Paulo, 1970.

WIENER, Norbert. **Cibernética e sociedade**: o uso de seres humanos. Tradução José Paulo Paes. São Paulo: Cultrix, 1954.

ZIOLKOWSKI, Katharina. **Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy**. Tallinn: NATO CCD COE Publicações, 2013. Disponível em: <https://ccdcoe.org/publications/books/Peacetime-Regime.pdf>. Acesso em: 31 jan. 2014.

ZENKO, Micah. Collateral damage: the dangerous precedentes of America's Drone Wars. **World Politics Review**, New York: Cambridge University Press, 2012.