CENTRO UNIVERSITÁRIO DE BRASILIA
FACULDADE DE CIÊNCIAS JURÍDICAS E SOCIAIS- FAJS
CURSO: RELAÇÕES INTERNACIONAIS

BÁRBARA FERREIRA NAZÁRIO

Cybersecurity, Cyberspace e Relações Internacionais

BRASÍLIA – DF

CENTRO UNIVERSITÁRIO DE BRASILIA
FACULDADE DE CIÊNCIAS JURÍDICAS E SOCIAIS – FAJS
CURSO: RELAÇÕES INTERNACIONAIS

BÁRBARA FERREIRA NAZÁRIO

Cybersecurity, Cyberspace e Relações Internacionais

Artigo científico apresentada como requisito parcial para a obtenção do título de Bacharel em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Luciano Muñoz

Brasília
2018

BÁRBARA FERREIRA NAZÁRIO

Cybersecurity, Cyberspace e Relações Internacionais

Artigo científico apresentada como requisito parcial para a obtenção do título de Bacharel em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Luciano Muñoz

Brasília, ... de 2018

Banca Examinadora

_____

Prof.

Orientador

_____

Prof.

Examinador

RESUMO

O presente artigo se propôs a analisar como o tema de cybersecurity se destacou entre a comunidade internacional, com ênfase na área de defesa. Para isso, utilizou-se livros e artigos científicos, além de dados e documentos de organizações internacionais especializadas em cybersecurity. Estes dados ajudam a entender como a tecnologia e a informação implicaram em mudanças de comportamento na sociedade, que reflete no âmbito internacional, especialmente em relação a segurança internacional. O artigo apresenta conceitos importantes que permeiam o âmbito de cybersecurity, como também as possibilidades de criar regulações para o cyberspace entre os Estados, o andamento de negociações e como estudiosos e tomadores de decisões interpretam diferentes leis que podem ser aplicadas neste determinado assunto. As invasões cibernéticas a Estônia, em 2007 foram usadas como exemplo de cyberattack a um país e quais são as consequências de tal ataque. Por fim, a teoria realista das relações internacionais foi utilizada para explicar as ações dos Estados e dos indivíduos, sendo que ainda existe espaço para inserir a novidade do cyberspace e suas características nas teorias de relações internacionais.

ABSTRACT

The present article aims to analyze how the cybersecurity topic stood out among the international community, especially in the defense field. With that intent, books and scientific articles, as well as data and documents from international organizations specialized in cybersecurity. The data helps to understand how technology and information resulted in changes in society's behavior, influencing the international community, especially international security. The article presents important concepts that permeate the cybersecurity scope, as well as the possibilities in creating regulations between States, the progress the negotiations and how scholars and decision makers interpret different laws that can be applied to this subject. The cyberattacks towards Estonia, in 2007 were used as an example of how a country could be attacked and the consequences of such attack. At last, the realist theory of international relations was used to explain how individuals as States act, while still there is space to add the novelty that is cyberspace and its characteristics in international relations theories.

SUMÁRIO

INTRODUÇÃO

O cyberspace levou a comunidade mundial a conhecer uma nova era, uma era de informação, de forma instantânea e sem fronteiras. A comunicação, o comércio, economia, todos se adaptaram à tecnologia, que facilita as ações do dia-a-dia. Apesar das qualidades da internet, existem outros aspectos que preocupam os Estados, principalmente aqueles relacionados à segurança nacional. Observa-se a importância do assunto de cybersecurity no âmbito internacional, sendo objeto de discussão entre estudiosos e tomadores de decisão, tanto na esfera nacional quanto na esfera internacional.

O presente trabalho pretende explicar as razões pelas quais cybersecurity se tornou um assunto de high politics na comunidade internacional. Dividido em três partes, este artigo apresenta conceitos utilizados para explicar as características que são importantes para cybersecurity e como o Direito Internacional lida com as novidades de cyberspace e tenta regular as ações dos indivíduos e dos Estados neste ambiente.

Em seguida, são analisados os ataques cibernéticos contra a Estônia, em 2007; e, por último, utiliza-se da teoria realista das relações internacionais para interpretar o sistema internacional, evidenciando os comportamentos dos Estados e dos indivíduos em relação ao cyberspace e cybersecurity.

CONCEITOS DE CYBERSECURITY E O DIREITO INTERNACIONAL

A humanidade mudou drasticamente a forma de se comunicar, de criar e de compartilhar conhecimento graças à Internet. Utilizada pela primeira vez em 1969, na Universidade da Califórnia, a Internet foi criada para transmissão de dados entre computadores da instituição. O governo americano e empresas privadas tiveram grande interesse nesta ferramenta e no que ela poderia proporcionar. Com investimentos e pesquisas, a “world wide web” se tornou o que conhecemos hoje.

Esta ferramenta proporcionou ao mundo um ambiente único e ilimitado onde informações podem ser compartilhadas para quem tiver acesso à um computador. O avanço da tecnologia fez com que o acesso a este ambiente, que antes estava restrito a ambientes educacionais e governamentais, fosse ainda mais fácil de ser acessado e com computadores, tablets, smartphones e a rede wi-fi.

A invenção da Internet foi capaz de modificar os modos tradicionais da vida em sociedade. O comércio, a política e a cultura tomaram novas formas e os sujeitos demandaram novas necessidades, modificando as menores interações e fazendo que a sociedade se torne dependente da Internet. Isso faz com que esta rede aglomere todo tipo de conteúdo, de informações básicas a importantes sites governamentais e programas que regulam a bases militares a usinas hidrelétricas.

1. Conceitos de Cybersecurity

O ambiente descrito acima como único e sem fronteiras é denominado cyberspace. Os autores Singer e Friedman explicam o que seria o cyberspace:

> Cyberspace is first and foremost an information environment. It is made up of digitalized data that is created, stored, and most importantly, shared. This means that it is not merely a physical place and thus defies measurement in any kind of physical dimension.
> [...] But cyberspace isn’t purely virtual. It compromises the computers that store data plus the systems and infrastructure that allow it to flow. This includes the Internet of networked computer, closed intranets, cellular technologies fiber-optic cables, and space- based communications. (SINGER; FRIEDMAN, 2014, p. 13, 14).

O cyberspace portanto é um ambiente em que se armazena informação e é através dele que ela é compartilhada. Não é limitado como o conceito de território tradicional. A partir do conceito dado pelos autores, pode-se inferir que apesar do cyberspace ser ilimitado em seu tamanho, ele não está isento de responsabilidade ou

até mesmo de “fronteiras”. “Cyberspace poder ser global, mas não é apátrida ou um global commons, termos que são usados frequentemente pelo governo e a mídia” (SINGER; FRIEDMAN, 2014, p.14). A organização civil União Internacional para a Conservação da Natureza descreve global commons como recursos naturais comuns a um nível planetário, identificado pelos Estados como livres de quaisquer jurisdições nacionais. Para que a Internet e o cyberspace funcionem é necessário pessoas para acessá-lo e maquinários como computadores e estes fatores são aplicados aos conceitos de Estado e propriedade.

O conceito de cyberspace pode ser incluído no conceito de meio técnico-científico-informacional. Segundo Milton Santos (2013), o meio técnico-científico-informacional é um meio geográfico onde o território inclui obrigatoriamente ciência, tecnologia e informação. A tecnologia e a ciência se tornam fundamentais para o espaço. O mundo se torna dependente da tecnologia e da ciência e possibilitam a criação deste novo espaço. As transformações sociais ocorrem através das transformações tecnológicas.

A informação está sempre presente e é necessária para a realização das atividades neste novo meio. A informação ganha uma relevância maior neste ambiente. O nível de desenvolvimento dos países passa a contar também com a quantidade de tecnologia que cada país possui. Apesar da globalização que leva esse meio para todo o mundo, ele não acontece de maneira uniforme. Alguns lugares têm facilidade ou dificuldade de assimilar este novo meio.

A sociedade se vê entrelaçada à tecnologia, à ciência e à informação. Elas se tornam interdependentes. Isto leva a outro elemento característico do cyberspace: sua importância por conter diversos serviços intrínsecos a sociedade, ressaltando o conceito de dependência dos homens a tecnologia e a ciência. A ideia principal por trás da criação da Internet era o compartilhamento de documentos e dados. Com sua evolução, o comércio se tornou uma grande parte da plataforma com uma enorme quantidade de empresas e lojas fazendo negócios pela web e consequentemente gerando trilhões de dólares em vendas. Outras atividades essenciais estão agregadas ao cyberspace através de softwares especializados como energia, transporte, agricultura e saúde. Estas não têm seu acesso ao público geral, mas através de seus sistemas podem ser acessadas ou hackeadas.

São esses fatores que fazem do cyberspace um lugar importante e um alvo. É nesse ambiente que um novo tipo de conflito nasce. Estudiosos e políticos começaram

a entender a possibilidade de quaisquer outras atividades que se desviam do seu objetivo original. Criminosos viram na Internet um jeito fácil de ganhar dinheiro através de vírus que roubam dados bancários, documentos, falsos sites de compra e outros tipos de farsas. Seguindo esse pensamento, nada impediria alguém de tentar roubar informações e dados de instituições governamentais ou intuições privadas.

Choucri escreve em seu livro sobre a relação entre as relações internacionais e o cyberspace. O autor relembra que o cyberspace era uma matéria de *low politics* e como o tema foi crescendo e tomando mais espaço na agenda internacional se juntando a outros assuntos de preocupação para os Estados:

> Nationalism, political participation, political contentions, conflict, violence, and war are among the common concerns of High politics. But low politics do not always remain below de surface. If the cumulative effects of normal activities shift the established dynamics of interaction, then the seemingly routine can move to the forefront of political attention. When this happens, it can propel the submerge features into the political limelight. (CHOUCRI, 2012, p. 3).

O autor ainda descreve características que fazem parte do modelo tradicional das relações internacionais e foram modificadas pelo cyberspace. A temporalidade, que corresponde a instantaneidade do cyberspace; corporalidade, que se refere aos barreiras físicas das fronteiras e localidade física dos indivíduos; permeação que descreve os limites jurídicos; fluidez, as rápidas mudanças e reconfigurações que acontecem neste ambiente; participação, o efeito do cyberspace na sociedade civil e a liberdade de expressão; atribuição, o anonimato dos atores e de links e *accountability,* que se relaciona a reponsabilidade das ações e os seus mecanismos.

É a natureza vulnerável do cyberspace, as alterações dos fatores e a imprevisibilidade que leva o assunto ao centro das discussões. Sendo que tantos serviços essenciais para o funcionamento de um Estado e empresas estão presentes no cyberspace, que é de fácil acesso a tantas pessoas no mundo, é essencial saber proteger os recursos e informações vitais. Daí nasce a importância de guardar e prever tais atentados a bases de informações. Essa se tornou a prioridade de muitos governos que decidiram convocar estudiosos sobre o assunto para voltar seus esforços para diminuir ameaças.

O National Initiative for Cyber Security Careers and Studies é um ramo do Departamento de Segurança dos Estados Unidos que se especializa a ensinar e treinar profissionais no setor. A instituição define cybersecurity como:

> The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. (National Initiative for Cyber Security Careers and Studies).

A definição estendida de cybersecurity é a que segue a baixo:

> “Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (National Initiative for Cyber Security Careers and Studies).

P. W. Singer e Allan Friedman explicam que a segurança surge da necessidade de se proteger de um inimigo, isto é, somente quando algum indivíduo pode ganhar algo a partir do funcionamento incorreto de um programa ou o uso de informações obtidas de forma ilegal. Conforme os autores, tradicionalmente, os objetivos de cybersecurity são: confidencialidade, integridade e disponibilidade.

Confidencialidade diz respeito à informação e como mantê-la restrita. Privacidade não é somente um objetivo social ou político. No mundo digital, informação tem valor (SINGER; FRIEDMAN, 2014, p. 35). É importante resguardá-la, não importando se diz respeito a segredo de Estado ou informações privadas de cidadãos e empresas. Deve ocorrer através de tecnologia e normas. Integridade corresponde ao sistema e se ele realmente cumpre com a sua função e que os dados não foram alterados por terceiros, sem autorização. A integridade é essencial para saber se o sistema é confiável e se nada foi violado. Hackers mais experientes sabem enganar o sistema que está sendo invadido e encobrem suas ações ao transmitir dados falsos de que o sistema funciona normalmente. Desta maneira, é complexo como pode-se confiar no sistema para certificar que este cumpre suas funções se é este mesmo sistema que pode ser alterado e distribuir informações falsas.

Disponibilidade aborda a funcionalidade do sistema e se este funciona como esperado. Refere-se ao fato de o programa não realizar seu trabalho, não por um erro natural, mas por intervenção de terceiros como a violação da função de um programa, o impedindo seu objetivo ou o sequestro dele. Singer e Friedman adicionam a este trio de segurança de informação um quarto objetivo: resiliência. Esta fala sobre o sistema ainda cumprir as suas funções mesmo sendo transgredido. As ameaças à

segurança devem ser esperadas e os sistemas devem ser preparados para estes, protegendo-se e se mantendo funcionais com sua aplicação final.

Ao se considerar as ameaças existentes no cyberspace é necessário entender que ameaça não é o mesmo que vulnerabilidade. As ameaças surgem quando existe uma vulnerabilidade. Com uma brecha no sistema, este pode ser invadido. O objetivo é essencial de se considerar ao analisar as vulnerabilidades. Dependendo do objetivo, a vulnerabilidade e como se defender irá variar. O livro de P. W. Singer and Allan Friedman (2014) especifica três tipos de objetivos: roubo de dados, uso impróprio de credencias e sequestros de recursos. A ameaça pode vir de alguém que possui permissão para utilizar o sistema como o vazamento de informações da NSA feitas pelo funcionário do órgão, Edward Snowden. Nesse caso, a ameaça tinha um entendimento mais profundo das vulnerabilidades.

Outro conceito importante em cybersecurity é cyberattack. A definição de cyberattack não será a mesma ao redor do mundo como na China, na Rússia e nos Estados Unidos. Esta é uma questão que impede os países de cooperarem, criarem regulamentações e organizações internacionais com o foco no assunto. Para o governo chinês, criar rumores contra o governo em redes sociais é considerado um cyberattack. O mesmo não acontecerá nos EUA.

A característica mais importante que distingue cyberattack de qualquer outro tipo de ataque é que este não usa forças tradicionais como bombas, mísseis e artilharia, seu método de ataque é digital, portanto não pode ser impedido por força militar, diplomacia, força política e não pode ser parado por barreiras geográficas. O tempo em que o ataque acontece é quase instantâneo, podendo ocorrer em segundos. Isso permite que os ataques aconteçam em diversos alvos ao mesmo tempo. Diferente de um ataque físico comum, que procura destruir ou danificar o alvo, o cyberattack atinge primeiro as informações. Mesmo que o ataque resulte em estragos físicos, primeiramente será necessário alcançar os dados digitais.

O National Research Council, reunido em 2009 pelo governo dos Estados Unidos define cyberattacks como *"...deliberate actions to alter, disrupt, deceive, degrade, or destroy computter systems or networks or the information and / or programs resident in or transiting these systems or networks."* (NATIONAL RESEACH COUNCIL, 2009). Pode-se concluir que a diferença de cyberattacks para outros tipos de ataques é sua natureza digital.

Os cyberattacks atacam diretamente os três objetivos a serem alcançados em cybersecurity: confidencialidade, integridade e disponibilidade. Os ataques a confidencialidade são direcionados a entrada do criminoso no sistema, o roubo de dados e monitoramento das atividades. Esse tipo de ataque pode afetar empresas que tenham as informações de seus clientes roubados ou o roubo de dados de uma base militar e de suas estratégias. A gravidade do ataque irá determinar sua importância. Os ataques a propriedade intelectual vem sendo um problema entre China e Estados Unidos.

Os ataques à integridade miram na alteração de dados ao invés de rouba-los. Esses ataques se tornam complexos pois existe uma dependência do sistema para avisar que o próprio foi invadido, o que nessa situação, não acontece, assim os usuários são alimentados informações falsas. As invasões podem resultar em alterações em sites oficiais do governo, com motivos políticos, criar permissões falsas para criminosos entrarem em locais com segurança e impedir o funcionamento de sistemas de outros países causando problemas para a população e gerando instabilidade no governo. Ataques a disponibilidade impedem os usuários de acessarem o sistema e se não for parado pode causar danos graves dependendo do sistema que foi atacado.

A identificação dos hackers é um grande desafio para cybersecurity, se não o maior. Não só identificação, mas também atribuir e responsabilizar os indivíduos por seus crimes. É comum que se identifique os grupos que são especializados em invadir sistemas de computadores de outros países, mas não é possível provar quem contrata esses grupos.

Para manter sua identidade anônima, o hacker utiliza de malwares (softwares programados para roubar dados e invadir dispositivos) para infectar computadores e controlá-los formando uma botnet (rede de computadores que executam a mesma tarefa repetidas vezes). Os donos dos computadores não sabem que sua máquina foi infectada. Desta forma, o hacker pode conectar milhões de computadores em diversos países e assim, dificultar a sua identificação. Ao se tentar investigar o ataque, é possível saber de que localidade ele foi iniciado, porém é mais complexo saber se o computador está sendo controlado remotamente, e consequentemente, quem é a pessoa por trás do ataque, sua nacionalidade, a qual grupo pertence.

Investigar os responsáveis por cyberattacks causam, no meio internacional, um sério debate sobre privacidade, o que pode causar problemas entre as relações entre

países como por exemplo China e Estados Unidos. É de entendimento comum que o governo chinês controla o uso da internet de seus cidadãos, o que leva a suspeita de que ataques cibernéticos que provem do território chinês estejam conectados ao governo. Porém, os chineses se defendem com a prerrogativa que grupos de hackers usam da grande suspeita que a comunidade internacional tem sobre a China para desviarem quaisquer desconfianças que ocorram. Outro fator que os chineses usam como defesa é o grande número de computadores desprotegidos no país.

Sabe-se, porém, que governos utilizam de grupos de hackers, chamados de hackers patrióticos e estudantes para financiar e mobilizar ataques a outros países. Este recrutamento recebe o nome de crowd-source, o ato de obter recursos e informações de pessoas através da internet. Assim, o Estado se exime da culpa do ataque e ao mesmo tempo se beneficia dele. Segundo Ronald Deibert, citado por Friedman e Singer (2014, p. 83), “Em tal ambiente, se complica a tarefa de atribuir culpa ao estado e formar uma resposta apropriada. Isso pode, potencialmente desestabiliza a ordem global”.

Dado o exposto, provar culpa é uma tarefa difícil. Todos esses fatores levam a um problema de atribuição. A resposta deixada para o Estado que foi atacado tem como soluções expor o grupo responsável pelo ataque como uma justificativa para um possível contra-ataque ou divulgar para a comunidade internacional os responsáveis e esperar que isso cause um mal-estar internacional, dando fim aos ataques e prováveis planos futuros.

2. Normas cibernéticas no Direito Internacional

Com tantos desafios encontrados em cybersecurity, além da grande dependência da humanidade da tecnologia, existe a questão de porque os Estados não criam normas para regular o cyberspace. A novidade do fenômeno abre espaço para debates sobre o tema, mas não há acordos que sejam extremamente significantes na lei internacional. Enquanto isso, os Estados desenvolvem tecnologias e melhoram suas defesas e a sua capacidade de ataque. Isso faz com que as discussões sobre o tema não desenvolvam e limita criação de leis e normas e a cooperação entre os Estados.

Segundo Schmitt e Vihul (2016), a lei internacional acontece em três formas: tratados, costumes e princípios gerais da lei. Decisões judiciais e o trabalho de

acadêmicos renomados são fontes secundárias. A ausência de leis especializadas e focadas no cyberspace faz com que os trabalhos de acadêmicos sejam instrumentos indispensáveis para formar leis internacionais.

Os costumes são leis que não são escritas e que se constrói com as ações dos Estados durante anos. São baseadas na prática dos Estados. Mesmo não sendo escrita, os costumes vinculam os estados. É necessário que vários Estados pratiquem os costumes, e que exista diversidade de países que o utilizam para fortificar essas regras. Muitas práticas ficam somente em plano regional, o que pode acontecer com leis cibernéticas.

Os Estados podem descumprir os costumes quando a lei de um tratado está sendo executada. Schimitt e Vihul exemplificam a situação quando um país “viola” a soberania de outro ao entrar na infraestrutura cibernética de outro país, com a finalidade de conduzir operações contra o terrorismo. Ou quando um país está sofrendo um ataque cibernético e precisa da ajuda de outro Estado com maiores capacidades cibernéticas.

O costume pode ser esquecido caso caia em desuso pelos Estados ou caso estes considerem que o costume pode colocar a segurança dos Estados em risco. A novidade de mundo cibernético faz com que os costumes não sejam definidos, criando vulnerabilidades nos costumes relacionados as atividades cibernéticas. Os Estados podem transformar os costumes em tratados, que se fortalecerão com o tempo.

A dificuldade de costumes no âmbito cibernético está no fato que é difícil analisar as atividades dos Estado no cyberspace, um obstáculo para singularizar práticas em comum e transforma-la em costumes. As práticas não são feitas abertamente, portanto não há regras explicitas. O interesse nacional e a segurança nacional irão tomar características políticas e estratégicas, ao invés de características legais no âmbito internacional.

Na questão de regular as atividades cibernéticas através de acordos, existem alguns tratados importantes como a Convenção sobre o Cibercrime, também conhecido como Convenção de Budapeste, Organização de Cooperação para Xangai ou Shanghai Cooperation Organization’s International Information Security Agreement; a Convenção da União Internacional de Telecomunicações (UIT) e o Setor de Normalização das Telecomunicações (UIT-T). O tratado de cooperação mais significativo sobre atividades cibernéticas até o momento é o Convenção sobre o Cibercrime, formado no dia 23 de novembro de 2001, em Budapeste, como um

Tratado parte do Conselho da Europa. Muitos países não aderiram ao tratado pela discordância das definições de violação de propriedade intelectual, mecanismos envolvendo a invasão a outros países e cibercrime. (KSHETRI, 2014). Outro fator importante que envolve a sociedade civil é o monitoramento governamental do cyberspace, e no que pode interferir na liberdade de expressão dos indivíduos. China, Rússia e Estados Unidos fazem parte do grupo de países que não adeririam a Convenção.

No Preâmbulo da Convenção sobre o Cibercrime (2001, p. 1) afirma:

> Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável.

A Convenção sobre o Cibercrime tem como força a consulta entre os países, a chamada de Regras de Procedimento, estipuladas no Artigo 46º:

> **Artigo 46º - Consulta entre as Partes**
>
> 1. As Parte consultar-se-ão periodicamente, se necessário, a fim de facilitar:
> a) A utilização e a execução efetiva da presente Convenção, incluindo a identificação de qualquer problema na matéria, bem como os efeitos de qualquer declaração ou reserva feita em conformidade com a presente Convenção;
> b) A troca de informações sobre os desenvolvimentos jurídicos, políticos ou técnicos importantes verificados no domínio da cibercriminalidade e a recolha de provas sob forma eletrônica;
> c) A análise de eventuais complementos ou aditamentos à Convenção. (Convenção sobre o Cibercrime. 2001)

Como observado pelas partes citadas da Convenção, para que o tratado seja eficiente os países membros da Convenção devem estar comprometidas em expor e disponibilizar avanços tecnológicos aos outros Estados, o que pode ser vantajoso ao lidar com grupos independentes de cyber terrorismo ou outros grupos criminosos. Porém, é importante lembrar que dificilmente os Estados irão compartilhar tecnologias significativas para a defesa de seu território e informações intrínsecas do seu país e cidadãos.

Os Estados Unidos dão preferência a mecanismos informais de cooperação como arranjos ad hoc, o que mostra ser eficaz. Os países se comprometem a compartilhar informações em assuntos específicos como ações contra quadrilhas de crime organizado e pornografia infantil. A cooperação informal se mostra mais flexível que tratados formais o que pode atrair mais Estados pela adaptabilidade da situação. Porém, críticos afirmam que os arranjos informais não mudam de forma definitiva o comportamento dos países e políticas domésticas. Outro lado negativo é que os países com grande poder de barganha usam os mecanismos informais ao seu favor. Os países que não possuem grande força econômica e militar podem utilizar do cyberspace para agredir países maiores e mais fortes.

As participações dos Estados em cyberattacks a outros Estados também é um fator que atrapalha na tentativa de cooperação. Como já mencionado, as provas de que um país atacou outro no cyberspace são circunstanciais. Um exemplo é o vírus Stuxnet que atingiu o programa nuclear iraniano. O Stuxnet é um vírus, criado para atingir centrífugas de enriquecimento de urânio. Em 2010, o programa nuclear iraniano sofreu com falhas em suas centrífugas e computadores. Meses depois, a Bielorrússia descobriu o Stuxnet em arquivos nos computadores iranianos. (WIRED, 2014)

Os Estados Unidos e Israel são suspeitos de terem lançado o ataque, porém não há provas concretas disso, apesar de que ambos os países têm grande interesse no programa nuclear iraniano. A falta de punição para aqueles que cometem esses crimes proporciona aos Estados um ambiente permissivo para ataques sem reprimendas e punições, ao contrário de ataques no mundo físico.

Uma grande questão divide a comunidade internacional e dificulta a cooperação é: leis não especificas a atividades cibernéticas podem ser aplicadas em atividades cibernéticas? Rússia e China discordam de maior parte dos países ao dizer que não. O Grupo de Peritos Governamentais da ONU (Group of Governmental Experts) chegaram à conclusão que o Direito Internacional e principalmente a Carta da ONU são aplicáveis as atividades cibernéticas para manter a paz e a estabilidade internacional, assim como a soberania e a responsabilidade dos Estados que permite que o ambiente de tecnologias de informação e comunicação seja pacífico e colaborativo. O Direito Internacional Humanitário e sua aplicabilidade ficou de fora do documento oficial do Grupo de Peritos Governamentais, um fracasso para o GGE.

O Grupo de Perito Internacionais (International Group of Experts) foi criado por especialistas para interpretar a aplicação de leis não relacionadas a atividades

cibernéticas, sendo *jus ad bellum* e Direito Humanitário Internacional o maior desafio. Assim, o Tallin Manual foi criado, com as interpretações dos peritos, mesmo elas sendo contraditórias e a aplicação do contexto que originou o instrumento a ser aplicado ao cyberspace.

Os peritos não souberam identificar quando uma atividade cibernética poderia ser qualificada como uso da força. Em relação ao Artigo 51 da Carta da ONU, que rege o direito de legítima defesa dos Estados, não se chegaram a conclusão da aplicação do artigo contra atores que não sejam o Estado. Ainda sobre o Artigo 51 e a legítima defesa, a questão era quando um ataque armado é grave o bastante para se considerar retaliação. Para alguns, ataques que prejudicam estruturas não físicas como a economia de um país devem ser considerados, outros discordam. (SCHMITT E VIHUL. 2016, p. 32)

Em relação a aplicação do Direito Internacional Humanitário em um possível tratado para regular atividades cibernéticas, existem dúvidas sobre do termo ataque e se ele se aplica a além do sentido de causar danos físicos. O artigo 52 do Protocolo Adicional I da Convenção de Genebra proibi os ataques diretos a objetos de civis. Interpretando objeto como informação, ataques a dados de civis seria proibido. Se dados não cabem no conceito de objetos, só seria crime se o ataque causasse danos físicos.

É importante que os Estados se manifestem e expressem a sua opinião sobre o uso do DIH para consolida-lo em tratados, principalmente aqueles que tem influência em organizações internacionais. A interpretação judicial e o trabalho de estudiosos, como demonstrado pelo Tallin Mannual (2013) ajuda na construção dos tratados, que é naturalmente lenta. Mesmo que um acordo seja feito, ainda existe a questão das reservas, que podem desviar o tratado de sua intenção inicial.

Estados dificilmente irão se vincular a tratado sobre um assunto tão novo que ainda está em desenvolvimento, especialmente quando não entendem sobre as vantagens e desvantagens das atividades cibernéticas em operações militares e armamentos. Os Estados temem que as restrições de armas irão tirar-lhes vantagens no campo de batalha. O interesse nacional irá se sobressair sobre o Direito Internacional.

Os princípios gerais do direito são regras comuns pelos sistemas legais por todo o mundo e se baseiam em justiça, promovendo equidade. Por serem aceitados mundialmente, são mais fáceis de serem aceitos e aplicados a atividades cibernéticas.

É pelos princípios gerais que o Tallin Mannual agregou a regra que afirma que operações cibernéticas não devem violar a soberania de outros Estados.

O cyberspace não possui regras, tratados e costumes explícitos que tornem o ambiente menos instável. Por meio da interpretação do Direito Internacional e o trabalho de estudiosos é um dos caminhos para a criação de normas sobre atividades cibernéticas. O assunto sempre será controverso, especialmente pelo espaço para interpretação de diversos Estados que são influenciados por seus interesses e políticas. Por se tratar de um assunto novo e que está se transformando e se desenvolve a todo instante, é possível dizer que o Direito Internacional aplicado nessa esfera será limitado.

ESTUDO DE CASO: ESTÔNIA

O caso de ataques cibernéticos a Estônia se destaca, por ser um dos únicos ataques cibernéticos que deixou a economia, o governo, a mídia e a população da Estônia transtornadas. Os ataques ocorreram entra 27 de abril a 18 de maio de 2007. Este ataque é um exemplo do medo de muitos estudiosos e autoridades sobre os poderes que hackers possuem de incapacitar todo um país ou mais. A partir da grande dependência da tecnologia, que cresceu rapidamente após 11 anos do ocorrido, a ameaça também cresce, fazendo que as políticas internas se voltem à cybersecurity.

A Estônia está localizada no noroeste da Europa, e tem a Rússia e Letônia como vizinhos. A Estônia foi conquistada pela Alemanha no século XI e dominado pela Suécia no século XV. Também foi dominada pela Dinamarca e a Rússia. Em 1918, conseguiu sua independência do Império Russo com o fim da Primeira Guerra Mundial. A sua autonomia durou 20 anos e terminou quando a Rússia dominou novamente o país em 1940 e o agregou ao União Soviética. O colapso da URSS permitiu que o a Estônia voltasse a ser independente em 1991. Atualmente é um dos membros da ONU e OTAN (Organização do Tratado do Atlântico Norte). Existe ainda animosidade entre Rússia e Estônia, que considera a anexação do país a URSS ilegal. A Rússia alega que a Estônia infringe os direitos humanos pelo tratamento dos cidadãos que falam russo. O conflito entre os dois países toma uma vertente étnica.

A minoria russa na Estônia constitui 24,8% da população (CIA, 2018). A imigração dos russos começou após a Primeira Guerra Mundial com a intenção de aumentar a população russa no país. A tensão entre Rússia e Estônia culminou em

uma série de protestos. O governo de Tallinn decidiu mover o Soldado de Bronze do centro da capital, erguida para comemorar o fim da Segunda Guerra Mundial. Para os russos, a estátua do soldado russo tem um grande significado, símbolo de orgulho e de vitória sobre os nazistas. Porém, para os estonianos, era um símbolo de repressão, da invasão soviética e da anexação forçada a URSS. No dia 26 de abril, a estátua foi retirada e os protestos começaram na capital. Aqueles que eram pró-Kremlin foram as ruas para manifestar. Uma pessoa morreu, 156 ficaram feridas e 1.000 pessoas foram detidas. O governo russo impediu o comércio de produtos da Estônia e Rússia declarou o ato como política de vingança contra os russos que vivem no país. (BBC, 2017).

No dia seguinte aos protestos, a Estônia sofreu com diversos ataques cibernéticos. Sites do governo, de bancos, meios de comunicação sofreram com “bombardeios” de pedidos de informação que incapacita o funcionamento normal dos sites. Caixas eletrônicos, online banking e e-mails entre os membros do parlamento pararam de funcionar periodicamente. Um único banco relatou ter pedido um milhão de dólares devido ao acontecido. Membros da mídia não conseguiam enviar notícias para serem publicadas. Fóruns em russo publicavam atualizações sobre o andamento das invasões e recrutavam a participação de outros hackers. A Estônia, que tinha sua infraestrutura baseada na Internet (e-governo), sofreu bastante com os ataques que inviabilizou o funcionamento de bancos, mídia e a comunicação entre os órgãos do governo.

A Estônia acusou a Rússia de estar por trás dos ataques. Segundo um especialista da OTAN, uma ação grande e sincronizada como só seria possível se fosse previamente orquestrado. Nem todos os hackers possuem este tipo avançado de habilidade para causar tamanha desordem. O Kremlin possui grande conhecimento sobre essa área e dado o nível de organização dos ataques, é esperado que a Rússia se torne suspeita de patrocinar hackers para realizar os ataques. A Rússia se beneficiaria dos ataques pois o país poderia atacar a Estônia sem arcar com o possível conflito com os países da OTAN. Além disso, a Estônia é importante para a Rússia pois está localizada em uma área estratégica para o trânsito de gás e óleo natural. As ações cibernéticas seriam uma boa opção para atacar seu vizinho sem a problemática de um ataque tradicional. O Kremlin não condenou os ataques. Tanto a Estônia, quanto a União Europeia e a OTAN tentaram rastrear os responsáveis pelos ataques,

mas não conseguiram achar o culpado e nem se a Rússia estaria por trás das ações contra a Estônia.

O ataque a Estônia pode ser considerado cyber terrorismo, que é a utilização de uma rede de computadores para atingir infraestruturas importantes de um país ou para intimidar a sociedade e o governo. Depois dos acontecimentos, a Estônia se tornou o país número um em experts de tecnologia da informação. Criou-se o Cyber Defense Unit que é formado por cidadãos voluntários especializados em informática e direito que se dedicam a melhorar sua tecnologia e proteger o seu país. A unidade especializada treina para possíveis ataques, garantem a segurança na Internet para os cidadãos e cooperam com o plano privado para compartilhar informações. Um ano após os ataques, a OTAN acelerou o processo da criação do NATO Cooperative Cyber Defence Centre of Excellence, proposto pela Estônia em 2004.

O caso da Estônia foi o primeiro ataque cibernético com grandes reflexos sobre todo um país, expondo a nova realidade de um mundo conectado e dependente da tecnologia de informação. Foi, para muitos países, um alerta para aumentar a atenção para cybersecurity, mostrando que ataques cibernéticos podem sim acontecer. Cyberattacks possibilitam o ataque ao inimigo sem que exista traços, podendo assim evitar as consequências internacionais. É necessário que os Estados e a lei internacional se adaptem para abranger esta nova realidade.

CYBERSECURITY E A TEORIA REALISTA

Esta parte do artigo tem como finalidade analisar a conjuntura teórica do realismo, salientando como a nova realidade do cyberspace se relaciona com o realismo. É dever das Relações Internacionais analisar o sistema internacional, os seus atores e suas interações, sendo elas econômicas, políticas e sociais. A teoria realista utiliza ideias de importantes autores para justificar as razões pela qual os Estados se comportam.

Nogueira e Messari (2005) contam como Tucídides contribuiu para estabelecer pressupostos importantes para a teoria realista. O autor afirma que os Estados iniciam e aderem a guerras pelo medo de não sobreviver. Existe pouco espaço para moralidade na convivência entre os Estados. Maquiavel colabora para o realismo ao afirmar que o Estado busca a sobrevivência como ator e é necessário poder para isso.

O uso da balança de poder, assim como as alianças com os outros Estados é essencial para lidar com o desafio de segurança.

Hobbes ajuda a reforçar a ideia do estado de anarquia no sistema internacional. A anarquia se deve ao fato de não existir um Leviatã no plano internacional. Não há um soberano que tenha o monopólio do uso da força, criando uma espécie de estado de natureza nas relações internacionais. Conclui-se então que a teoria realista se baseia no indivíduo, na natureza humana, vista de uma forma negativa.

A era da informação atual apresenta uma forma de poder diferente da tradicional. Ao se pensar em segurança de um Estado, é comum e natural pensar em exércitos com uma grande quantidade de homens e fortes com alta força bélica para destruir as forças inimigas. Assim, os armamentos garantem o poder da proteção do Estado e o poder de ameaçar os seus inimigos. O cyberspace, porém, oferece novas possibilidades. A disseminação dos computadores e outros aparelhos eletrônicos que se conectam a Internet por todo o mundo, ocasiona na facilidade de acesso ao cyberspace, aumentando o número de pessoas que se especializam no uso de máquinas, sem passar, necessariamente por instituições formais de educação.

É comum, na atualidade, a modernização das infraestruturas essenciais de um Estado para atender a sua comunidade de uma forma mais eficiente e que possa chegar ao maior número de pessoas possíveis. O aumento da dependência das nações em tecnologia origina novas vulnerabilidades para o Estado, sendo que o ataque as infraestruturas essências como distribuição de água, online banking, transporte público e armamentos pode desestabilizar todo um país. Aquele que tiver habilidades para atacar um Estado com esse objetivo pode levar toda uma nação ao caos.

Então, o poder, por essa razão, não se restringe aos políticos, exércitos, ou líderes de Estado. A obtenção de informações cruciais para todo a manutenção de um Estado, incluindo a área militar pode dar ao indivíduo ou um grupo o poder de danifica-lo. O cyberspace aumenta a probabilidade de acesso os sistemas de serviço públicos, que também irá ampliar o número de indivíduos ou grupos que tem capacidade de invadir esses sistemas, além de poder fazê-lo anonimamente, sem mesmo precisar sair de sua casa. Observa-se então a entrada de novos atores com novos métodos de atacar Estados.

Hans Morgenthau (2003) criou seis princípios para definir o realismo. O primeiro princípio afirma que a natureza humana é o que governa a política e a sociedade,

sendo que a natureza humana é imutável. O segundo princípio define os interesses a partir do poder, sendo este o objetivo dos Estados. O terceiro princípio estipula o uso dos princípios morais na ação política, desde que não ameacem os interesses e a segurança do Estado. O quinto princípio afirma que as aspirações morais são particulares e não devem ser “exportados” para todo o mundo. O sexto princípio afirma que a política é uma esfera autônoma e estuda fenômenos diferentes dos fenômenos sociais.

Dentro dos seis princípios de Morgenthau, pode-se concluir que o terceiro princípio é aplicável a mais um novo formato de poder disponibilizado pelas redes de computadores, salientando que a informação não é restrita somente ao Estado. Outro princípio de Morgenthau que se destaca é o quinto princípio que se refere as aspirações morais. Como mencionado por Nogueira e Messari (2005), Morgenthau se referia ao Estados Unidos da América ao escrever que as aspirações são particulares de cada país. Os EUA já “exportava” os ideais ocidentais como soft-power. A globalização permitiu que culturas, religiões e produções intelectuais atravessassem fronteiras. O cyberspace faz este mesmo papel, porém de uma forma mais eficaz e instantânea. Mesmo que os morais não sejam “exportados” por um país específico, eles irão naturalmente, através do cyberspace, se disseminar pelo mundo.

Para os realistas, o Estado é o único ator das relações internacionais. O papel do Estado é organizar a nação internamente, sendo ele o único detentor do uso legítimo da força. Nas relações entre outras nações, seu dever é de manter a segurança e garantir o interesse nacional no ambiente anárquico que é o sistema internacional. O Estado é guiado pelo medo de ser aniquilado por outros países e pelo prestígio que busca.

Apesar da importância e do papel central do Estado, dois autores importantes para a teoria realista, Kenneth Waltz e Hans Morgenthau, não escreveram extensamente sobre o Estado em si, e sim sobre o seu papel, internamente e externamente. Para Morgenthau, o Estado se destaca por ter o monopólio do uso legítimo da força e por possuir leis. Assim, é de responsabilidade do Estado manter a paz dentro do seu território e extinguir ações que possam desestabilizar a ordem, se necessário com o uso da força.

Morgenthau (2003) afirma ainda que os nacionais de um país não irão contra o interesse nacional pois os cidadãos são ensinados que a nação é maior que qualquer assunto que possa causar conflitos internos como partidos, religião e economia. A

lealdade a nação impede os cidadãos de ameaçar a coesão interna do Estado. Entende-se que a comunidade vê o interesse nacional como um bem para todos os cidadãos e que o inimigo no ambiente internacional é maior que divergências internas.

O autor descreve a identidade do indivíduo dentro da nação, como um cidadão leal e que sua identidade está ligada a cultura da nação, língua, costumes, história. Por essa razão, o indivíduo é fiel ao seu Estado, criando relações com seus patriotas que possuem similaridades. Mesmo com diferenças religiosas ou políticas, o cidadão não irá colocar essas divergências acima do Estado. Existe o sentimento nacional da população. Em relação aos estrangeiros, o indivíduo não tem compatibilidade por não viverem no mesmo país e terem diferentes características difundidas pela sua nação.

A globalização promoveu a dispersão de diversas culturas e religiões pelo mundo. Com a presença do cyberspace, o indivíduo tem muitas conexões diferentes, para além de suas fronteiras. Assim como o cidadão se identifica com seus patriotas, no cyberspace ele irá se identificar com estrangeiros. Ao se considerar a dependência dos seres humanos aos seus aparelhos de comunicação, principalmente com a função de conversar, se informar e emitir opiniões o estrangeiro perde a imagem de estranho ou de inimigo e se transforma em um companheiro ao compararem suas experiências e identificarem interesses comuns como política, religião e economia. Isso faz com que se tenha uma maior compaixão ao estrangeiro, o que influencia a opinião pública em relação a atividades militares em terras internacionais. Nessa situação, o indivíduo irá se identificar com o estrangeiro, mas não irá afetar seu sentimento nacional.

Porém, pode-se observar a atuação de grupos terroristas como o Estado Islâmico que usam da Internet para propagar seus ideais e seus objetivos de conquista. A atuação do ISIS na Internet tem como alvo jovens islâmicos que estão desconectados da religião ou até mesmo pessoas que não são associadas ao islã, mas que são consideradas “antissociais” e se sentem marginalizados. Não são atraídos somente pela questão religiosa do conflito, mas pela violência. Com vídeos de alto valor de produção, jovens são atraídos pela satisfação imediata e uma cultura que promove a redenção pela violência.

Kenneth Waltz (1979) apresentou a teoria estrutural as Relações Internacionais. Waltz cria então três imagens das relações internacionais. A primeira imagem tem o indivíduo como nível de análise. A natureza humana é a principal causa das guerras. As atitudes dos homens são egoístas, agressivas e estúpidas. A natureza

humana é imutável. A segunda imagem coloca o Estado no centro da análise, sendo os Estados os responsáveis pelas guerras, em busca de sua própria segurança ou em busca de seus interesses. A terceira imagem analisa o sistema internacional como um todo. Como o sistema internacional é anárquico, os Estados procuram garantir sua própria segurança.

As três imagens podem ser aplicadas, até um certo ponto, a estrutura do cyberspace. Considerando a natureza humana, é de se esperar em um ambiente em que não há fronteiras e a possibilidade de agir anonimamente, que os indivíduos utilizem a Internet para buscar seus interesses. Muitos crimes são cometidos pelo Internet: roubo de dados, fraudes, uso de software falsos, plágio, perfis falsos e enganosos, venda de drogas e outras substâncias proibidas, pedofilia.

O cyberspace parece viver uma dualidade. Não existem regras que regulem todo o cyberspace, permitindo que várias pessoas possam acessar qualquer tipo de conteúdo ou criar qualquer tipo de conteúdo. Porém, como mencionado por Singer e Friedman (2014), os indivíduos que acessam uma rede de computadores e cometem crimes terão que responder a justiça do Estado no qual o indivíduo vive ou promoveu a ação criminosa. As características globais e ilimitadas do cyberspace permitem que esses crimes aconteçam rapidamente e em vários locais ao mesmo tempo, provando importante a cooperação entre os Estados para controlar grupos ou indivíduos que descumprem leis. Muitas vezes é difícil rastrear os culpados pois o cyberspace dificulta a identificação de seus usuários. Consequentemente, os Estados acabam perdendo, de certa forma, sua autoridade neste ambiente, por ser mais fácil cometer crimes sem ter que responder por eles.

Caso os Estados tentem controlar o cyberspace, pode ser percebido como uma quebra dos direitos humanos da população, como a liberdade de expressão e a privacidade. Existe o medo de que os governos censurem as pessoas e que invadam os dados sigilosos para seu próprio interesse.

Assim como afirmado na segunda imagem de Waltz, os Estados irão seguir seus próprios interesses e buscar formas de se proteger. Os Estados são importantes na criação de novas tecnologias relacionadas ao cyberspace. Com a realidade dos cyberattacks, os Estados tentam se defender e superar os outros Estados. Além de que os Estados possuem recursos maiores como dinheiro e experts para investir em tecnologia.

A cooperação para a leis internacionais especializadas nesse âmbito é lenta. Os Estados têm receio de assinar tratados que possam compromete-los no futuro. Observa-se que neste caso, os Estados dão preferência aos seus próprios interesses, principalmente em um assunto tão novo e instável como cybersecurity.

Outro problema comum para a cooperação são as atividades secretas dos Estados usando o cyberspace. É sabido que os Estados usam da tecnologia para espionar e atacar outras nações como ocorreu com os Estados Unidos em 2013, acusado de espionar Rússia, Brasil, Alemanha, China e Paquistão. Rússia também foi acusada de atacar a Estônia em 2007. No caso americano, os Estados Unidos foram denunciados pelo próprio cidadão e funcionário do governo americano. O caso russo foi uma acusação da Estônia e da OTAN, sendo que grupos opositores russos seriam os verdadeiros culpados, sem qualquer ligação com o Kremlin. É importante, afirmar que nesses casos nenhum dos dois países sofreram quaisquer punições por não respeitar a soberania de outras nações.

Os ataques a Estônia mostram como os Estados se comportam tal tecnologia a disposição, demonstrando para seu oponente o poder, o intimidando. Ao mesmo tempo, a Rússia se viu impossibilitada de intimidar a Estônia por vias tradicionais de segurança, através da força militar, além de evitar perda material e vidas. Os cyberattacks tornam-se uma arma de convencimento e intimidação sem necessidade de mobilizar exércitos e sem números de mortos.

O cyberspace e suas características que vão contra ao entendimento e as atuais estruturas que permeiam a sociedade e os governos, que lidam com forças cinéticas e palpáveis. Muitas áreas já modificaram suas infraestruturas e se adaptaram para utilizar a tecnologia s seu favor, como a economia, o comércio, a educação e até mesmo os Estados. Apesar de o cyberspace não alterar totalmente a estrutura mundial atual certamente traz novos desafios, principalmente para a segurança internacional e para o Direito Internacional. Os autores Johan Eriksson e Giampiero Giacomello (2006) presumem que o realismo não vê o cyberspace como uma grande mudança na ordem mundial, pois não afeta a anarquia internacional, que continuará a mesma. É importante relembrar que mesmo com a permanência da estrutura mundial atual, é necessário que estudiosos considerem as novas possibilidades e novos atores internacionais, incluindo novos métodos de atuação que o cyberspace cria que são opostas as estruturas que permeiam a atual realidade.

CONCLUSÃO

O primeiro tópico deste artigo esclarece o cyberspace como um ambiente único e sem fronteiras, que armazena informações e as compartilha. Este conceito se encaixa no conceito meio técnico-cientifico-informacional de Milton Santos. Os indivíduos se tornam dependentes da tecnologia, da informação e da ciência, se entrelaçando ao território. Assim, a sociedade necessita da ciência, da informação e da tecnologia para operar normalmente.

Com tantas informações, é de se esperar que o cyberspace se torne alvo da ganância de indivíduos que buscam se beneficiar. Os Estados e empresas precisam se defender dessas ameaças. Muitas vezes torna-se difícil a atribuição deste tipo de crime. Por causa dessa dificuldade, os Estados utilizam desta ferramenta para atacar outros países, sem ter que responder por seus atos.

A cooperação neste campo torna-se difícil pois muitos países possuem opiniões e políticas diferentes sobre privacidade e a aplicação de outras leis, como o Direto Internacional Humano, no âmbito do cyberspace. Em relação a cooperação, os países dão preferência a arranjos ad hoc.

A segunda parte do artigo exemplifica como os Estados podem usar o cyberspace para ameaçar e atacar outros países, sem precisar responder por estes atos. O ataque a Estônia provou que a ameaça tecnológica é real e precisa ser debatida no meio internacional, o que é difícil pois a novidade apresentada pelo cyberspace deixa os países inseguros e sem previsibilidade, pela rapidez em que as tecnologias se desenvolvem.

A última parte do artigo utiliza a teoria realista das relações internacionais para explicar as ações dos Estados no sistema internacional e no cyberspace. Analisando as obras de Waltz e Morgenthau é possível afirmar que o cyberspace não muda de modo profundo a estrutura mundial atual, porém dificulta a atuação dos Estados, diminuindo sua autoridade a nível nacional, em relação a seus próprios cidadãos e facilita a atuação de outros sujeitos no campo internacional. O debate sobre cybersecurity torna-se também necessária para garantir a segurança dos Estados.

Ainda não existe uma grande atuação dos estudiosos em relações internacionais para integrar este novo ambiente, tão diferente do ambiente clássico que foi estudado, as teorias das relações internacionais. O futuro é incerto pois a

rapidez em que as mudanças tecnológicas acontecem dificulta previsões. É certo afirmar que o cyberspace e cybersecurity se tornaram partes importantes das vidas da sociedade mundial e deve ser acompanhada com atenção.

REFERÊNCIAS

BALDWIN, David A. The Concept of Security. **Review of International Studies**, Vol. 23, No. 1 (jan., 1997), pp. 5-26. Cambridge University Press Disponível em: <http://www.jstor.org/stable/20097464> Acesso em: 05 de novembro de 2017.

BERRINGER, Tatiana. O conceito de Estado para os estudos realistas das relações internacionais: uma análise sobre a obra A política entre as nações de Hans Morgenthau. **PLURAL,** Revista do Programa de Pós-Graduação em Sociologia da USP, São Paulo, v.24.2, p.16-37, 2017. Disponível em: <www.revistas.usp.br/plural/article/download/142992/137868/>. Acesso em: 15 de agosto de 2018.

CHOUCRI, Nazli. **Cyberpolitics in international relations**. The MIT Press, Inglaterra, 2012. Disponível em: <https://flavioufabc.files.wordpress.com/2017/02/cyberpolitics-and-international-relations.pdf>. Acesso em: 04 de abril de 2018.

COUNCIL OF EUROPE. **Convention on Cybercrime**, ETS No. 185, 2001. Disponível em: <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf>. Acesso em: 23 de março de 2018.

ERIKSSON, Johan; GIACOMELLO, Giampiero. The Information Revolution, Security, and International Relations: (IR)relevant Theory? **International Political Science Review (2006), Vol 27, No. 3, 221–244.** Disponível em: <https://pdfs.semanticscholar.org/9082/96559bfa6a29926e0777c353427b8342f1b0.pdf>. Acesso em: 05 de novembro de 2017

ESTONIA profile – Overview. **BBC**, 2016. Disponível em: <https://www.bbc.com/news/world-europe-17220811>. Acesso em: 10 de setembro de 2018.

ESTONIAN history and culture. **Visit Estonia**, 2017. Disponível em: <https://www.visitestonia.com/en/why-estonia/estonian-history-and-culture>. Acesso em: 10 de setembro de 2018.

FINN, Peter. **Statue's Removal Sparks Violent Protests in Estonia**. The Washington Post, 2007. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/27/AR2007042702434.html>. Acesso em: 10 de setembro de 2018.

FRIEDMAN, Allan; SINGER, Peter W. **Cybersecurity and cyberwar: what everyone needs to know.** United States of America by Oxford University Press. Disponível em: <https://news.asis.io/sites/default/files/Cybersecurity_and_Cyberwar.pdf>. Acesso em: 05 de novembro de 2017.

FRUHLINGER, Josh. **What is Stuxnet, who created it and how does it work?** CSO online, 2017. Disponível em: <https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html>. Acesso em: 20 de setembro de 2018.

GAFFNEY, O., NAKICENOVIC, N., ROCKSTRÖM, J. and ZIMM, C. **Global Commons in the Anthropocene: World Development on a Stable and Resilient Planet.** WP-16-019. Austria: IIASA Working Paper. 2016.

GELVIN, James L. What draws 'lone wolves' to the Islamic State? The Conversation, 2017. Disponível em: < https://theconversation.com/what-draws-lone-wolves-to-the-islamic-state-86746>. Acesso em: 10 de setembro de 2018.

HARDING, Luke. **Protest by Kremlin as police quell riots in Estonia**. The Guardian, 2007. Disponível em: <https://www.theguardian.com/world/2007/apr/29/russia.lukeharding>. Acesso em: 10 de setembro de 2018.

HERZOG, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." **Journal of Strategic Security 4**, no. 2 (2011): 49-60. Disponível em: <http://scholarcommons.usf.edu/jss/vol4/iss2/4>. Acesso em: 20 de outubro de 2017.

INTERNATIONAL GROUP OF EXPERTS. **Tallin Mannual on The International Law applicable to cyber warfare.** Cambridge University Press, 2013.

KSHETRI, Nir. **Cybersecurity and International Relations: The U.S. Engagement with China and Russia.** The University of North Carolina at Greensboro. Disponível em: <http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf>. Acesso em: 03 de setembro de 2017.

LEMONNIER, Jonathan. **What is Malware? How Malware Works & How to Remove it**. AVG Technologies, 2015. Disponível em: <https://www.avg.com/en/signal/what-is-malware>. Acesso em: 20 de setembro de 2018.

MAIAS, Lucas. O conceito de meio técnico-científico-informacional em Milton Santos e a não-visão da luta de classes. **Caminhos De Geografia,** Uberlândia, v. 13, n. 41, p. 29-41, mar. 2012. Disponível em: <http://www.ig.ufu.br/revista/caminhos.html>. Acesso em: 19 de julho de 2017.

MALWARE 101: What is a botnet? **Norton US**, 2016. Disponível em: <https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html>. Acesso em: 20 de setembro de 2018.

MATSUBARA, Mihoko; PLONK, Audrey; VISHIK, Claire. Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms. **International Cyber Norms: Legal, Policy & Industry Perspectiver.** NATO CCD COE Publications, Tallinn, 2016. Disponível em: <https://ccdcoe.org/multimedia/tallinn-papernature-international-lawcyber-norms.html>. Acesso em: 10 de julho de 2018.

MCGUINNESS, Damien. **How a cyber attack transformed Estonia.** BBC, 2017. Disponível em: <https://www.bbc.com/news/39655415>. Acesso em: 10 de setembro de 2018.

MORGENTHAU, Hans J. **A Política entre as Nações: A luta pelo poder e pela paz.** Brasília, Editora Universidade de Brasília, 2003.

NOGUEIRA, João Pontes; MESSARI, Nizar. **Teoria das relações internacionais: correntes e debates**. Rio de Janeiro: Elsevier, 2005.

ONU. Nações Unidas no Brasil. **A Carta das Nações Unidas**. 2017. Disponível em: <https://nacoesunidas.org/carta/ >. Acesso em: 7 de julho de 2018.

REARDON, Robert; CHOUCRI, Nazli. **The Role of Cyberspace in International Relations: A View of the Literature.** Department of Political Science, MIT. Disponível em:<https://ecir.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf>. Acesso em: 04 de novembro de 2017

ROGERS, Mike. **How ISIS uses the internet to recruit new members (hint: It involves kittens)**. Daily News, 2017. Disponível em: <http://www.nydailynews.com/news/national/isis-internet-recruit-members-hint-kittens-article-1.3473890>. Acesso em: 10 de setembro de 2018.

SANTOS. Milton. **Técnica espaço tempo: Globalização e meio técnico-científico informacional.** Edusp, 2013.

SCHMITT, Michael N.; VIHUL, Liis. The Nature of International Law Cyber Norms. **International Cyber Norms: Legal, Policy & Industry Perspectives,** Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn, 2016. Acesso em: < https://ccdcoe.org/multimedia/tallinn-paper-nature-international-law cyber-norms.html>. Acesso em: 10 de julho de 2018.

STERLING, Bruce. **Estonian cyber security.** Wired, 2018. Disponível em: < https://www.wired.com/beyond-the-beyond/2018/01/estonian-cyber-security/>. Acesso em: 10 de setembro de 2018.

WALTZ, Kenneth. **O homem, o Estado e a Guerra: uma análise teórica**. Martins Fontes, São Paulo, 2004.

WORLD Factbook. **Central Intelligence Agency**. Disponível em: <https://www.cia.gov/library/publications/the-world-factbook/geos/en.html>. Acesso em: 10 de setembro de 2018