UNIVERSIDADE FEDERAL DE GOIÁS
REGIONAL GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

LUÃ GONÇALVES VITORINO

DIREITO INTERNACIONAL E CIBERGUERRA: ATAQUES CIBERNÉTICOS ENTRE NAÇÕES, MANUAL DE TALLINN, POR QUE É MAIS FÁCIL REGULAR UMA CIBERGUERRA DO QUE REGULAR UMA CIBERSEGURANÇA?

CIDADE DE GOIÁS-GO
2021

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): LUÃ GONÇALVES VITORINO

Título do trabalho: DIREITO INTERNACIONAL E CIBERGUERRA: ATAQUES CIBERNÉTICOS ENTRE NAÇÕES, MANUAL DE TALLINN, POR QUE É MAIS FÁCIL REGULAR UMA CIBERGUERRA DO QUE REGULAR UMA CIBERSEGURANÇA?

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador)

Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Fernanda De Paula Ferreira Moi**, **Professor do Magistério Superior**, em 21/06/2021, às 10:54, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **LUÃ GONÇALVES VITORINO**, **Discente**, em 21/06/2021, às 12:19, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2149433** e o código CRC **5CB4997D**.

Referência: Processo nº 23070.025874/2021-84 SEI nº 2149433

LUÃ GONÇALVES VITORINO

DIREITO INTERNACIONAL E CIBERGUERRA: ATAQUES CIBERNÉTICOS ENTRE NAÇÕES, MANUAL DE TALLINN, POR QUE É MAIS FÁCIL REGULAR UMA CIBERGUERRA DO QUE REGULAR UMA CIBERSEGURANÇA?

Monografia apresentada ao Curso de Direito da Universidade Federal de Goiás – Regional Goiás - UAECSA, como requisito parcial para aprovação na disciplina de Monografia Jurídica II.

Orientadora: Prof.ª Dr. Fernanda de Paula Ferreira Moi

CIDADE DE GOIÁS-GO
2021

VITORINO, Luã Gonçalves

Direito Internacional e Ciberguerra: ataques cibernéticos entre nações, manual de tallinn, por que é mais fácil regular uma ciberguerra do que regular uma cibersegurança? / Luã Gonçalves VITORINO. – 2021.
49 f.

Orientador: Profa. Dra. Fernanda de Paula Ferreira Moi. Trabalho de Conclusão de Curso (Graduação) – Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Sociais Aplicadas, Direito, Cidade de Goiás, 2021.

1. Ciberguerra . 2. ciberespaço. 3. cibersegurança. 4. ciberataque. 5. Manual de Tallinn. I. MOI, Fernanda de Paula Ferreira, orient. II. Título.

CDU 341

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Ao(s) 11 de junho de 2021, às 13:00, iniciou-se a sessão pública de defesa do Trabalho de Conclusão de Curso (TCC) intitulado "DIREITO INTERNACIONAL E CIBERGUERRA: ATAQUES CIBERNÉTICOS ENTRE NAÇÕES, MANUAL DE TALLINN, POR QUE É MAIS FÁCIL REGULAR UMA CIBERGUERRA DO QUE REGULAR UMA CIBERSEGURANÇA?", de autoria de LUÃ GONÇALVES VITORINO, do curso de Direito, do(a) Unidade Acadêmica Especial de Ciências Sociais Aplicadas do Câmpus Goiás da UFG. Os trabalhos foram instalados pelo(a) Profa. Dra. Fernanda de Paula Ferreira Moi, da Unidade Acadêmica Especial de Ciências Sociais Aplicadas (UAECSA) com a participação dos demais membros da Banca Examinadora: Profa. Dra Bruna Pinotti Garcia Oliveira, da Unidade Acadêmica Especial de Ciências Sociais Aplicadas (UAECSA) e Prof. Dr Heitor Pagliaro, da Unidade Acadêmica Especial de Ciências Sociais Aplicadas (UAECSA). Após a apresentação, a banca examinadora realizou a arguição do(a) estudante. Posteriormente, de forma reservada, a Banca Examinadora se posicionou pela **APROVAÇÃO** do trabalho apresentado.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.

Documento assinado eletronicamente por **Bruna Pinotti Garcia Oliveira**, **Professora do Magistério Superior**, em 21/06/2021, às 10:54, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Fernanda De Paula Ferreira Moi**, **Professor do Magistério Superior**, em 21/06/2021, às 10:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Heitor De Carvalho Pagliaro**, **Professor do Magistério Superior**, em 21/06/2021, às 11:56, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2149405** e o código CRC **D1697AD1**.

Referência: Processo nº 23070.025874/2021-84 SEI nº 2149405

Dedico essa pesquisa a minha família pela oportunidade de estudar.

AGRADECIMENTOS

Aos meus pais, Marlene e Wanderlei, pelo esforço de eu ter uma oportunidade de um futuro melhor.

À minha irmã, seu esposo e minha sobrinha que sempre me apoiaram.

Aos meus tios, Cristiano e Luciano, pelas oportunidades de estudos e exemplo.

À minha orientadora, Fernanda de Paula Ferreira Moi, por aceitar e me guiar durante essa pesquisa.

Aos meus cachorros, Kurt e Lisbeth, que não me deixaram ficar louco durante o processo de pesquisa e quarentena.

À Universidade Federal de Goiás, especialmente à Regional Goiás, seu corpo docente, servidores e funcionários terceirizados.

A mim mesmo por não ter desistido no meio do caminho nesse cemitério de sonhos chamado Brasil.

“Talvez não seja sobre evitar o erro. Talvez seja definir um ponto de parada para encontrar uma falha no código, resolvê-la e continuar até atingirmos a próxima falha.”

(Mr. Robot)

"Uma verdadeira cibersegurança é preparar-se para o que vem por aí, não para o que veio por último."

(Neil Rerup)

RESUMO

Esta monografia tem por objetivo detectar como a ciberguerra vem crescendo e tornando-se cada vez mais presente no dia a dia, ocupando uma lacuna deixada pelo Direito Internacional Público, ao não passo que não temos uma cibersegurança internacional e ainda esbarramos em questões de soberania e meios de identificar responsáveis por ataques cibernéticos. Sendo assim, a pesquisa analisa as limitações de soberania e responsabilização enfrentadas pelo Direito e como isso leva a um descontrole no ciberespaço, tomando um rumo para a ciberguerra, que já conta com uma possível regulamentação já pronta, o Manual de Tallinn. Partindo dos métodos dedutivo e estudo de casos, analisou-se a evolução histórica de soberania, conceitos de ciberguerra, ciberespaço e cibersegurança, bem como elementos para caracterizar responsabilização internacional e suas dificuldades. Por meio de revisão bibliográfica de doutrinas, manuais e artigos relacionados ao tema, estudo do Manual de Tallinn e a análise de casos concretos de ciberguerra, buscamos promover um estudo que relacione as causas das dificuldades de uma segurança cibernética internacional. Apesar de encontramos um bom exemplo na cooperação em cibersegurança ao longo da pesquisa, ainda parecemos mais próximos de regular uma ciberguerra do que termos uma cibersegurança internacionalmente coordenada.

Palavras-chave: Ciberguerra; cibersegurança; ciberespaço; ciberataque; Manual de Tallinn.

ABSTRACT

This monograph aims to detect how cyberwar has been growing and becoming more and more present in daily life, occupying a gap left by Public International Law, while we do not have international cybersecurity and we still face issues of sovereignty and ways of identifying those responsible for cyber-attacks. Thus, the research analyzes the limitations of sovereignty and accountability faced by the Law and how it leads to a lack of control in cyberspace, taking a turn towards cyberwar, which already has a possible regulation already ready, the Tallinn Manual. Starting from deductive and case studies methods, the historical evolution of sovereignty, concepts of cyberwar, cyberspace and cybersecurity were analyzed, as well elements to characterize international accountability and its difficulties. Through bibliographic review of doctrines, manuals and articles related to the theme, study of the Tallinn Manual and analysis of concrete cases of cyberwar, we seek to promote a study that lists the causes of the difficulties of international cybersecurity. Although we found a good example in cybersecurity cooperation throughout the research, we still seem closer to regulating a cyberwar than having internationally coordinated cybersecurity.

Keywords: cyberwar; cybersecurity; cyberspace; cyber-attack; Tallinn Manual.

SUMÁRIO

INTRODUÇÃO

A partir do século XXI, a tecnologia deu um salto extraordinário. Formas de se relacionar, troca de informações, novas culturas, produtos etc., tudo na palma da mão, mas acompanhando a tecnologia, práticas estatais de defesa e ataque também se desenvolveram, surgindo um novo conceito de guerra, a ciberguerra. Inserida no contexto do ciberespaço, a guerra cibernética está em ascendência, enquanto isso, ainda não temos respostas do Direito sobre a regulação do ciberespaço ou uma cibersegurança coordenada internacionalmente.

Sendo assim, a ciberguerra já está em andamento e já têm suas consequências. Enquanto o ciberespaço está longe de ser minimamente regulado de forma internacional (e até internamente) com algum tratado, já temos um projeto que trata da regulação das consequências da ciberguerra, que é o Manual de Tallinn, um projeto da Organização do Tratado do Atlântico Norte (OTAN) e publicação Universidade de Cambridge. Nesse sentido, o Direito Internacional (assim como o Direito Interno) parece não conseguir acompanhar a evolução do ciberespaço e dar algum norte jurídico em casos de ataques cibernéticos entre nações, estas, que permanecem silentes em relação ao assunto. Sem uma cibersegurança internacional com padrões e mecanismos de identificação e responsabilização, Estados podem seguir livremente atacando, monitorando e influenciando outras soberanias sem consequências. Essas atitudes não geram prejuízos apenas no âmbito estatal, mas um ato de ciberguerra pode causar danos às infraestruturas críticas de um país, gerando grandes consequências para seus cidadãos também.

Desta linha de pensamento, surgiu a indagação de quais razões levam a uma maior facilidade de normatização de uma guerra cibernética do que construir regras de cibersegurança. Seguindo essa linha, a pesquisa pretende analisar os motivos que, no âmbito do Direito Internacional Público, atualmente, caminhamos para regular uma ciberguerra, enquanto uma cibersegurança internacional e diretrizes para o ciberespaço são deixadas de lado. Especificamente, buscamos analisar as dificuldades jurídicas na atribuição de responsabilidade por ciberataques entre Estados; como questões de soberania influenciam na não regulamentação do ciberespaço; analisar como a ciberguerra já tem um grande projeto de regulação e identificar porque uma ciberguerra já está ocorrendo.

Como Green afirma em *Cyber Warfare*: a multidisciplinar analysis "as dificuldades de atribuição tornam as armas cibernéticas atraentes para muitos países e sugerem que veremos o uso crescente de tais armas por Estados-Nações" (2015, p.62, tradução nossa), o crescente uso dessas armas cibernéticas trazem grande relevância na discussão sobre cibersegurança. O ciberespaço "desencadeou uma série de ajustes econômicos, sociais e políticos das arenas locais

às internacionais. Além disso, a segurança foi trazida de volta ao primeiro plano como uma das principais preocupações que afetam o caminho em quais Estados interagem." (KREMER e MÜLLER, 2014, p.04. tradução nossa**)**. A preocupação com a ciberguerra e suas consequências tem levado a pesquisas e elaboração de obras como *Encyclopedia of Cyber Warfare* (2017) e *Cyberspace, Cybersecurity, and Cybercrime* (2018) e *Public International Law of Cyberspace* (2017). Mas não apenas a ciberguerra traz preocupação, o Manual de Tallinn que tenta trazer regras sobre uma guerra no ambiente informático levanta temor, destaque para Dieter Fleck, em sua pesquisa "*Searching for International Rules Applicable to Cyber Warfare*: a Critical First Assessment of the New Tallinn Manual" (2013, p.349, tradução nossa), onde analisa a obsessão pela guerra e afirma que o Manual "Não aborda atividades para melhorar a segurança cibernética em um sentido mais amplo", na mesma direção Dan Efrony e Yuval Shany dizem que "A maioria das regras do Manual se concentra, no entanto, na interação entre as operações cibernéticas e o uso da força." (2018, p.584, tradução nossa).

Na busca para compreender e analisar tal conjuntura, seguimos os métodos dedutivo e de estudo de casos, analisando a evolução histórica da soberania, os conceitos de ciberespaço, ciberguerra e cibersegurança, bem como as dificuldades que o ciberespaço apresenta para atribuir-se responsabilidade para reparação de eventuais danos de um ciberataque; como e porque deu-se a construção do Manual de Tallinn e como a ciberguerra já está em andamento. Por meio da metodologia de revisão bibliográfica de doutrinas, manuais e artigos relacionados ao tema, estudo do Manual de Tallinn e a análise de casos concretos de atos de ciberguerra, buscando promover um estudo que relacione as causas das dificuldades de uma segurança cibernética internacional.

As questões apresentadas foram divididas em três capítulos dentro da pesquisa, e têm a seguinte estrutura. No primeiro capítulo, apresentamos a evolução histórica da soberania e como ela relaciona-se com o ciberespaço e como aquela dificulta a regulação deste. Dentro do mesmo capítulo procuramos conceituar ciberespaço e cibersegurança, dando relevância à importância de uma cibersegurança e principais obstáculos para a mesma. Por fim, demonstramos os elementos para atribuir responsabilidade por um ciberataque e as dificuldades em se estabelecer nexo entre um ciberataque e dano.

No segundo capítulo, trazemos o contexto histórico que culminou na produção do Manual de Tallinn e o seu processo de elaboração. Seguindo a análise do Manual, verificamos como ele é estruturado para apresentação de suas regras e explicações das mesmas. Fechando o capítulo, expomos como foi a recepção ao Manual por parte dos Estados, bem como pontos nele que geram críticas.

O capítulo terceiro, versou sobre a espantosa quantidade de ataques cibernéticos diários, com base em dados fornecidos por empresas de cibersegurança que monitoram o fluxo de ataques e quais os seus alvos e pontos de partida. Também é apresentado dois casos concretos emblemáticos de ciberguerra, os ataques à Estônia em 2007 e o Stuxnet em 2010, o primeiro, considerado o primeiro ciberataque coordenado contra uma nação inteira, e o segundo, o primeiro com um alvo específico. Ao terminar o capítulo um exemplo de cibersegurança coordenada entre múltiplos países foi apresentada, demonstrando que é possível tal normatização.

Sendo assim, o trabalho perpassa pelos capítulos tendo como base norteadora a lacuna deixada pelo Direito Internacional nas matérias de cibersegurança e ciberespaço e como a ciberguerra tem tomando esse espaço, com países, por enquanto, ficando impunes ao praticarem tais atos.

1 LIMITAÇÃO DO DIREITO INTERNACIONAL QUANTO AO DINAMISMO DO CIBERESPAÇO

1.1 SOBERANIA E O CIBERESPAÇO

Uma das maiores dificuldades em se regular o ciberespaço de forma internacional, talvez seja, a soberania, pois esse espaço virtual não representa um território, que é elemento essencial do Estado, e, consequentemente, não contém limites de fronteiras. Esta soberania está atrelada ao território "O território é o espaço onde se exerce a soberania estatal. Ele determina os limites do exercício do poder do Estado." (VARELLA, 2019, p.255).

A ideia de soberania e suas teorias surgem no século XVI, com o nascimento do Estado Moderno. O primeiro teórico a trabalhar a ideia foi Jean Bodin em sua obra "*Les Six Livres de la République*"[1], onde a descreve como "soberania é o poder absoluto e perpétuo de uma República, palavra que se usa tanto em relação aos particulares quanto em relação aos que manipulam todos os negócios de estado de uma República" (DALLARI, 2015, p.84), aqui, República é o equivalente ao que conhecemos por Estado nos dias atuais. Bodin explica que poder absoluto é aquele que não pode ser limitada por quem está no poder ou criação de leis, e perpétuo diz respeito a ter prazo indeterminado para ser exercida.

> Embora não tenha mencionado a inalienabilidade como característica da soberania, o que outros autores fariam depois, escreve Bodin que, seja qual for o poder e a autoridade que o soberano concede a outrem, ele não concede tanto que não retenha sempre mais. Dessa forma, a soberania coloca o seu titular, permanentemente, acima do direito interno e o deixa livre para acolher ou não o direito internacional, só desaparecendo o poder soberano quando se extinguir o próprio Estado. (DALLARI, 2015, p.84)

Em "O Contrato Social", Rousseau, acrescenta as características de inalienabilidade e indivisibilidade à soberania. "Ela é inalienável por ser o exercício da vontade geral, não podendo esta se alienar nem mesmo ser representada por quem quer que seja. E é indivisível porque a vontade só é geral se houver a participação do todo". Ao contrário de Bodin, Rousseau traz a concepção de limites desse poder soberano.

> Diz, então, que o pacto social dá ao corpo político um poder absoluto sobre todos os seus membros, e esse poder é aquele que, dirigido pela vontade geral, leva o nome de soberania. O poder soberano, completamente absoluto, sagrado e inviolável, não ultrapassa nem pode transgredir os limites das convenções gerais. A regra básica da limitação é que o soberano não pode sobrecarregar os cidadãos de coisas inúteis à

[1] "Os Seis Livros da República"

> comunidade e tampouco pode exigi-las, devendo, finalmente, fazer exigências iguais a todos os súditos. (DALLARI, 2015, p.85)

Aos poucos o conceito de soberania foi desenvolvendo-se, contrapondo-se à monarquia absolutista, "No combate da burguesia contra a monarquia absoluta, que teve seu ponto alto na Revolução Francesa, a ideia da soberania popular iria exercer grande influência, caminhando no sentido de soberania nacional, concebendo-se a nação como o próprio povo numa ordem." (DALLARI, 2015, p. 85). A soberania passa a ser elemento essencial do Estado e de grande interesse do mesmo, na ordem interna e na expansão territorial, Streck e Morais destacam que:

> No século XIX, a soberania emerge como expressão do poder político no interesse das conquistas territoriais das grandes potências, tendo, ao final deste período, como titular o Estado. Estando sempre ligada a uma noção de poder, aparece como uma qualidade do poder estatal ou como expressão da unidade de uma ordem como referido por Hans Kelsen. Em termos políticos, refere a plena eficácia do poder, não se preocupando com a questão da legitimidade, devendo ser absoluto. Em termos jurídicos, identifica-se com o poder de decidir sobre a eficácia do direito, dizer qual a regra aplicável em cada caso. (2003, p.156)

O Estado tornando-se o detentor da soberania, esta passa a ser juridicamente trabalhada "E já no século XX, aperfeiçoada a doutrina jurídica do Estado, a soberania passa a ser indicada como uma de suas notas características, colocando-se entre os temas fundamentais do direito público, desenvolvendo-se uma completa teoria jurídica da soberania." (DALLARI, 2015, p. 85). Tais teorias trabalham o conceito de soberania, divergentes em alguns termos, mas com um ponto convergente entre elas que é o atrelamento de soberania à ideia de poder estatal, como aponta Dallari:

> O primeiro aspecto importante a considerar é o que se refere ao conceito de soberania. Entre os autores há quem se refira a ela como um poder do Estado, enquanto outros preferem concebê-la como qualidade do poder do Estado, sendo diferente a posição de Kelsen, que, segundo sua concepção normativista, entende a soberania como expressão da unidade de uma ordem. Para Heller e Reale ela é uma qualidade essencial do Estado, enquanto Jellinek prefere qualificá-la como nota essencial do poder do Estado.
> (...) Procedendo a uma síntese de todas as teorias formuladas, o que se verifica é que a noção de soberania está sempre ligada a uma concepção de poder, pois mesmo quando concebida como o centro unificador de uma ordem está implícita a ideia de poder de unificação. (2015, p.85 e 86)

O conceito moderno de soberania apresenta duas dimensões, uma interna e uma externa, Bonavides a explica como:

> A soberania, que exprime o mais alto poder do Estado, a qualidade de poder supremo (*suprema potestas*), apresenta duas faces distintas: a interna e a externa. A soberania

> interna significa o *imperium* que o Estado tem sobre o território e a população, bem como a superioridade do poder político frente aos demais poderes sociais, que lhe ficam sujeitos, de forma mediata ou imediata. A soberania externa é a manifestação independente do poder do Estado perante outros Estados. (2011, p.119)

A partir da metade do século XX até os dias atuais, a chamada globalização traz acelerada interdependência econômica entre Estados e facilidade de trocas culturais entre os povos, e ao mesmo tempo novos desafios para a soberania. A globalização mitigou a soberania estatal, nascendo uma espécie de soberania econômica paralela, como observa Acquaviva:

> O fenômeno da globalização da economia mundial se expressa na abertura dos mercados, no livre comércio, na eliminação de barreiras fiscais em favor deste, no fluxo internacional de capitais, no fortalecimento das empresas multinacionais, na internacionalização da tecnologia e, mesmo, no notável incremento do turismo internacional. Como observa Rodrigo Borja, nesta nova ordem econômica internacional o capital criou sua própria "soberania". Com efeito, o capital, especialmente o especulativo, move-se com espantosa rapidez e total liberdade, escolhendo os Estados que adotará como fonte de renda. Conforme suas conveniências, em questão de segundos salta as fronteiras dos Estados, emigrando em busca de maior lucro. Quando um Estado deixa de oferecer condições vantajosas para este capital, é imediatamente sancionado com a *desinversão*, formando-se o pânico nas suas bolsas. Impossível evitar, então, a perda do controle de sua economia e criar alternativas independentes da especulação internacional. Assim, forçoso reconhecer que o poder *político* dos Estados vem a ser superado pela planificação econômica das grandes empresas multinacionais, que dispõem da economia mundial em favor de seus interesses, sem considerar as conveniências sociais. (2010, p.57)

Nesse sentido, Lewandowski, aponta como consequência da globalização a homogeneidade dos problemas que afetam o mundo e a limitação frente a agentes econômicos globais.

> Embora corresponda fundamentalmente a uma nova etapa na evolução do capitalismo, ensejada pelo progresso das comunicações e da informática, a globalização também resulta - e é causa ao mesmo tempo - da uniformização dos padrões culturais e dos problemas que hoje afetam o planeta como um todo.
> (...) De fato, pela primeira vez desde que se consolidou como *summa potestas* no plano interno e internacional, em especial a partir da Paz de Westphalia, o Estado não consegue mais controlar de forma satisfatória a repercussão doméstica das variáveis econômicas geradas externamente. Em outras palavras, o poder de autodeterminação das comunidades políticas organizadas em Estados passou a ser cerceado pelo poder dos agentes econômicos transnacionais, com o que ficou abalada a própria legitimidade dos governantes. (2004, p.253 e 254)

Lewandowski, ainda observa um novo modelo de "soberania compartilhada" aos moldes da União Europeia, onde um grupo de países juntam-se para melhor gerir questões políticas, econômicas e jurisdicionais.

> Vê-se, pois, que os integrantes da União não sofrem nenhuma perda de poder. Na verdade, o contrário é que ocorre, uma vez que sua capacidade de atuação, ao invés de diminuir, passa a ser potencializada pela ação comum. Compartilhar a soberania significa conferir-lhe operacionalidade, ou seja, possibilidade de intervir de forma objetiva e consequente na realidade fática. O exercício de competências de forma compartilhada no seio de instituições comuns, diz Victor Louis, não acarreta prejuízo para a soberania de seus integrantes, conferindo-lhes, ao revés, "a possibilidade de exercer responsabilidade que, no plano nacional, se haviam tornado puramente formais para Estados independentes".
> Essa técnica, é interessante notar, apresenta um aspecto paradoxal, qual seja, embora aparentemente os Estados renunciem a parcelas de sua soberania, na realidade conjugam forças para melhor preservá-la. Agem, segundo uma comparação um tanto quanto irreverente, "da mesma maneira que um cartel abre mão de sua liberdade de vender tudo o que pode para participar de uma fatia mais gorda dos lucros monopolísticos do grupo". (2004, p.292)

Esse modelo enfrenta alguns entraves, pois, para essa soberania compartilhada a nível global e formação de uma organização internacional, esse compartilhamento seria de forma voluntária, teríamos que ter consenso entre um grande número de países e, ainda, uma entidade internacional exerceria soberania do ciberespaço sobre os Estados-Nações, o que até o momento não é factível, pois, as organizações internacionais surgem da manifestação de vontade dos Estados e por eles são compostas, não lhes sendo atribuídas soberania como afirma Portela “a soberania é atributo exclusivo dos Estados. Nesse sentido, a circunstância de os entes estatais estabelecerem organizações internacionais não conferem a estas o caráter de entidades soberanas” (2017, p.158).

Sendo o ciberespaço produto da globalização, e ainda, um espaço não físico nascido na era do capital transacional, regular uma soberania sobre ele é uma tarefa complexa que ainda não temos. Temos uma vertente que traz o ciberespaço como um bem público global, a exemplo do alto mar, onde não há reinvindicação de soberania.

> Estados não podem afirmar soberania sobre o ciberespaço. Eles só podem regular a maneira como as pessoas (ou coisas) sujeitas à sua autoridade acessam o ciberespaço global. Não existe um “ciberespaço nacional” sobre o qual eles exercem controle supremo; em vez disso, há um ciberespaço global compartilhado e eles aplicam sua soberania sobre os atores e dispositivos físicos em seu território para restringir, de forma imperfeita e limitada, conexões a certos sites ou aplicativos. As autoridades territoriais simplesmente não estão no controle de quem acessa o ciberespaço fora de seu território ou os serviços ou aplicativos que atores externos fornecem sobre ele. Eles só podem identificar e bloquear coisas após o fato. Essas limitações não dão aos Estados soberania sobre o ciberespaço mais do que a soberania de um país no licenciamento de navios e aprovação de sua entrada e saída de seus portos, isso não dá a eles a soberania sobre o oceano, muito menos a propriedade de satélites e instalações lançamento conferem-lhe soberania sobre o espaço sideral. (MUELLER, 2019, p.12, tradução nossa)

Mas diferentemente do alto mar, o ciberespaço, necessariamente, precisa de uma infraestrutura localizada em algum território para existir, para Talpai e Branco:

> Apesar de engenhosa a solução de tratar o ciberespaço como um bem público global, o 'locus' digital se distingue dos bens que de fato se enquadram nessa categoria por depender de infraestrutura que, necessariamente, existe em determinada localização geográfica e pertence a alguma entidade, que realiza sua operação e manutenção.
> Parece-nos mais razoável compreender o ciberespaço não como um bem público global, mas como um ambiente artificial – criado pelo ser humano e passível de modificação por ele – que perpassa várias soberanias ao mesmo tempo e precisa de um tratamento diferenciado para salvaguardar a soberania dos Estados que entram em contato com esse ambiente digital. (2020, p.55)

Nesse sentido, a responsabilização de ciberataques, seja qual for a vertente de ciberespaço ou soberania, fica condicionada à descoberta da localização da infraestrutura utilizada, esta sim, física e passível de soberania. Tratando-se do âmbito privado essa soberania, de certo modo, ainda pode ser exercida sobre uma empresa transnacional, como por exemplo, quando temos o uso de uma plataforma para prática de crimes ou atos que não condizem com a cultura daquele país. A sede dessa empresa pode estar em outro país, mas para operar em outros, equipamentos *in loco* são necessários, uma certa infraestrutura, e essa infraestrutura está passível ao exercício da soberania.

A problemática encontra-se quando um ataque provém de uma infraestrutura totalmente localizada em outro Estado ou, de forma mais complexa, com partes de infraestrutura em vários Estados, ou seja, em território soberano de outro(s) Estados, e tal ataque tem traços de ser um suposto ataque de um Estado contra outro. Paradoxalmente, a mesma lógica da infraestrutura encontrar-se em um local permitir certa soberania, também é aplicável do ciberespaço não ser passível de soberania, como destaca Talpai e Branco:

> Analisou-se a hipótese de compreender o ciberespaço como bem público global, mas descartou-se essa possiblidade pois todas as ações realizadas no espaço virtual *'são tomadas por indivíduos ou entidades sujeitos à jurisdição de um ou mais Estados'*. Também por isso os Estados não podem reivindicar soberania sobre o ciberespaço, dado que a infraestrutura que permite a sua existência está, via de regra, localizada no território soberano de outros Estados. (2020, p.56)

Com todas essas questões, um tratado que procurasse regular essas questões de soberania poderia evitar muitos conflitos, mas nos parece uma realidade distante que o Direito ainda não conseguiu encontrar soluções.

1.2 CIBERESPAÇO

O Manual de Tallinn conceitua ciberespaço como "O ambiente formado por componentes físicos e não físicos, caracterizado pelo uso de computadores e do espectro

eletromagnético, para armazenar, modificar e trocar dados usando redes de computadores" (SCHMITT, 2013, p.258, tradução nossa). Dodge e Kitchin trazem que "O termo ciberespaço significa literalmente 'espaço navegável' e é derivado da palavra grega kyber (para navegar)" (2001, p.01, tradução nossa), os mesmos autores trazem uma conceituação mais abrangente de ciberespaço:

> Atualmente, o ciberespaço não consiste em um espaço homogêneo; é uma miríade de ciberespaços em rápida expansão, cada um fornecendo uma forma diferente de interação e comunicação digital. De um modo geral, estes espaços podem ser categorizados naqueles existentes nas tecnologias da Internet, aqueles na realidade virtual e nas telecomunicações convencionais como o telefone e o fax, embora devido à rápida convergência de tecnologias novos espaços híbridos estão emergindo." (2001, p.01, tradução nossa).

Mas o ciberespaço engloba muito mais que uma rede de computadores, nos dias atuais, esse espaço online influência inúmeras áreas do conhecimento e a vida. A antropologia já o estuda como afeta a cultura, deslocamentos urbanos e até mesmo o turismo, segundo Camargo, Santos e Guterres:

> Nesse novo espaço antropológico, o do saber, as pessoas estariam mais propensas e dispostas a construir conhecimentos coletivos, conectando-se a outros cérebros, de forma errante, em busca de seus próprios entendimentos, recorrendo a artifícios que, segundo Lévy, suportariam esse espaço do saber, como os dispostos no ciberespaço, onde pessoas poderiam expressar os seus próprios entendimentos, questionamentos, percepções, sentimentos e desejos diante de um todo e, mesmo, de um ou vários coletivos formados neste mesmo espaço. (2012, P.582)

Como pode-se notar, o ciberespaço vai muito além da simples internet que usamos no dia a dia, é um ambiente muito mais complexo e dinâmico do que pensamos. Até mesmo como uma categoria geográfica já é estudado, como destaca Silva

> Para que seja possível compreender o papel do ciberespaço nas pesquisas geográficas, é necessário que se utilize o mesmo enquanto uma categoria geográfica distinta das demais. Não o sendo um objeto autônomo, dotado de uma particularidade epistêmica que necessite uma nova disciplina científica para avaliá-lo, nem um mero meio novo em que problemáticas geográficas espaciais, territoriais, regionais, locais ou mesmo ambientais se desenrolam, o ciberespaço, no atual quadro de desenvolvimento tecnológico da humanidade, é uma categoria geográfica tal qual outros elementos das mais diversas ordens: território, região, paisagem, lugar, etc. (SILVA, 2013, p.28)

Nesse contexto, o ciberespaço ao longo de sua existência, tem evoluindo em espantosa rapidez e talvez já seja um organismo vivo, sem ter um Estado, uma instituição ou várias que o possam controlar, apenas utiliza-lo da melhor maneira, o que não prevalece, notadamente diante

de uma explosão de ataques cibernéticos entre esses Estados e instituições, e consequente ciberguerra. Essa complexidade juntamente com a inércia dos países em discutir uma cibersegurança global, leva a uma direção de regulamentação de pequenas porções do ciberespaço no campo nacional de cada país para crimes cometidos por indivíduos, enquanto isso, o Manual de Tallinn adianta-se a uma cibersegurança e traz regras para uma iminente ciberguerra, utilizando conceitos já existentes no Direito Internacional aplicando-os ao contexto cibernético.

1.3 CIBERGUERRA

Apesar de Manual de Tallinn trazer regras para uma possível ciberguerra e até conflitos armados nesse contexto, ele não traz um conceito de ciberguerra, apenas de ciberataque "Um ciberataque é uma operação cibernética, seja ofensiva ou defensiva, que seja razoavelmente esperado que cause ferimentos ou morte a pessoas ou danos ou destruição de objetos." (2013, p.106, tradução nossa), como podemos perceber, essa definição é parecida com a de um ataque fora do contexto cibernético e não esclarece o que de fato é ciberguerra.

A definição de ciberguerra gera conflitos entre estudiosos do assunto, na concepção de Parks e Duggan "A ciberguerra é o subconjunto da guerra de informações que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual contida em uma coleção de computadores e redes." (2011, p.122, tradução nossa). Para Liff ciberguerra é:

> (...) um estado de conflito entre dois ou mais atores políticos caracterizado pelo uso deliberado hostil e indutor de custos de CNA[2] contra a infraestrutura civil ou militar crítica de um adversário com intenção coercitiva, a fim de extrair concessões políticas, como uma medida de força bruta contra militares ou redes civis, a fim de reduzir a capacidade do adversário de se defender ou retaliar na mesma moeda ou com força convencional, ou contra alvos civis e / ou militares, a fim de enquadrar outro ator para fins estratégicos. (2012, p.406-408, tradução nossa)

Clarke e Knake postulam que ciberguerra pode ser definida como "ações de um Estado-Nação para penetrar nos computadores ou redes de outra nação para o propósito de causar danos ou perturbações"(2010, p.14, tradução nossa). Esses danos e perturbações vão desde o âmbito social até segredos industriais. Para Stiennon

> A ciberguerra é uma extensão da política por meio de ações realizadas no ciberespaço por atores estatais (ou por atores não estatais com orientação ou apoio estatal significativo) que constituem uma séria ameaça à segurança de outro estado, ou uma

[2] Computer Network Attacks (CNA), Ataques de Redes de Computadores.

> ação da mesma natureza tomada em resposta a uma séria ameaça à segurança de um estado (real ou percebida). (2015, p.8, tradução nossa)

Com mais profundidade e abrangência, a Dr. Julie E. Mehan, em seu livro *Cyberwar, Cyberterror, Cybercrime and Cyberactivism: An in-depth guide to the role of security standards in the cybersecurity environment* (Ciberguerra, Ciberterror, Cibercrime e Ciberativismo: um guia aprofundado para o papel dos padrões no ambiente de segurança cibernética), traz o conceito de ciberguerra por classes, que vão de um a quatro, de acordo com seus níveis de alcance e dano. Segundo ela, essas classificações são:

> Como tal, a ciberguerra de Classe I preocupa-se com a proteção de informações pessoais - ou privacidade pessoal. Embora os resultados ainda possam ser devastadores, a ciberguerra de Classe I é considerada o grau mais baixo.
> Ciberguerra de Classe II, o próximo passo, preocupa-se com a indústria e espionagem econômica, que pode ser dirigida contra nações, corporações, universidades ou outras estruturas organizacionais. Esta forma de ciberguerra está definitivamente em ascensão.
> A ciberguerra de Classe III é oficialmente sobre guerra global e terrorismo, que inclui o ciberterrorismo, mas que também pode incluir ataques contra outras partes da infraestrutura crítica. Seja com o propósito de destruir um computador pessoal ou uma rede de outra entidade, ou a negação de um serviço e se o ofensor é um hacker malicioso, um criminoso extorsionário, um verdadeiro terrorista (que provavelmente se considera um mártir de qualquer causa), ou um governo estrangeiro, o resultado final cai na mesma categoria.
> Por fim, a ciberguerra de Classe IV é o uso de todas as técnicas das Classes I até a III em combinação com atividades militares em um esforço para obter vantagem em um campo de batalha ou um multiplicador de força. (2014, p.39, tradução nossa)

Como podemos perceber, a ciberguerra não está relacionada apenas à algum ataque que leve a um conflito armado, ou que necessariamente, irá ferir a incolumidade física das pessoas. Há diversas formas de ataques e alvos que, mesmo não causando um dano físico, podem causar profundos danos econômicos, políticos e sociais, como salienta Mehan "A ciberguerra, portanto, infere tanto o conflito relacionado à informação a nível nacional, militar, bem como atividades de conflito de baixa intensidade pretendidas para infligir níveis limitados de dano." (2014, p.39, tradução nossa).

Uma das maiores preocupações relacionadas à ciberguerra é o ataque às infraestruturas primordiais de uma Nação, como, por exemplo, redes elétricas, transportes, gás, água, telecomunicações. São as infraestruturas que se forem prejudicadas podem trazer algum dano à segurança, economia e saúde pública nacionais, além de possíveis vantagens políticas e econômicas. Em tópico mais adiante analisaremos casos concretos de tais ataques e suas consequências.

1.4 CIBERSEGURANÇA

Leiner *et al.* conceituam a cibersegurança como sendo "a atividade ou processo, habilidade ou capacidade, ou estado pelo qual os sistemas de informação e comunicação e as informações neles contidas são protegidos e/ou defendidos contra danos, não autorizado uso ou modificação ou exploração." (apud KREMLING e PARKER, p.64, 2017, tradução nossa). Cibersegurança lida com a permanente proteção, melhoramento e desenvolvimento de padrões, protocolos e softwares contra possíveis ciberataques e rastreamento dos mesmos. Mas, além de ataques externos, cibersegurança, também, engloba detecção e correção de falhas internas dos sistemas.

A tecnologia da informação é parte essencial do desenvolvimento econômico, social e até cultural do mundo. O controle e funcionamento de infraestruturas críticas em praticamente todos os setores são automatizadas, estabelecer padrões internacionais de cibersegurança é de suma importância para a manutenção do bom funcionamento interno de um país e diminuição de tensões internacionais, preservando a paz.

1.4.1 **Por que ter uma cibersegurança internacional?**

Um tratado abordando uma cibersegurança global faz-se necessário para proteger civis, coibir espionagem entre Estados e de empresas contra Estados, ataques de ciberterrorismo, bem como a melhoria dos meios para apuração de responsabilidade por ciberataques. Mas o ciberespaço e cibersegurança não estão restritas às fronteiras, aqueles ultrapassam essas fronteiras, tornando-se em uma questão de geopolítica internacional.

Para Kremling e Parker:

> há uma codependência do governo e do setor privado em que muitos ativos privados são prejudiciais ao público, e sua segurança é de grande importância para o governo. Por exemplo, muitas infraestruturas críticas são propriedade privada, mas o governo ajuda a protegê-las. As informações proprietárias, como pesquisas da empresa, segredos comerciais, hardware e software, são em sua maioria propriedade de empresas privadas, mas o governo tem interesse em proteger essas informações. (2017, p.344, tradução nossa)

Nesse sentido, estabelecer regras internacionais de cibersegurança poderia gerar mais proteção tanto no âmbito público quanto no privado. Se uma empresa multinacional de um país ter uma filial em outro e desenvolver pesquisas e avanços, mas os benefícios desses avanços atingirem apenas o país de origem haverá um desiquilíbrio tecnológico.

Além da proteção de informações nacionais, públicas e privadas, um tratado internacional de padrões de cibersegurança também traria maior efetividade e redução de custos ao combate de crimes cometidos por entes não estatais, como expõem Kremer e Müller:

> A conveniência de um tratado ou alguma forma de cooperação institucionalizada é mais frequentemente escalonada em termos dos benefícios que tal mecanismo ofereceria em termos de redução dos custos de abordagens unilaterais e técnicas para aumentar a segurança da rede, e também na redução dos riscos ou falhas do sistema que podem estar associados a ações técnicas unilaterais por parte dos Estados para proteger redes de comunicação eletrônica ou ativos conectados a eles.
> Um acordo internacional com ampla participação poderia preservar a abertura dos usos e conexões da Internet, em oposição às etapas múltiplas e contínuas dos Estados para promover seus interesses nacionais na ausência de quaisquer normas ou compromissos internacionais. A ação cooperativa dos Estados também é desejável, pois pode potencialmente limitar as ações de atores não estatais ou criminosos cibernéticos. (2014, p.235, tradução nossa)

Seguindo este escopo, uma cibersegurança a nível internacional traria benefícios mútuos aos Estados, como mais segurança jurídica, e mais proteção para suas populações dentro do ciberespaço e mitigação de ataques e consequências deles fora do espaço cibernético, Kremer e Müller destacam que "Além da interconexão e interdependência das redes, as redes de comunicação eletrônica são infraestruturas críticas internas para todos os países, e assim a proteção desses recursos também fornece a base para objetivos compartilhados" (2014, p.237, tradução nossa). O ciberespaço é um lugar interconectado mundialmente e como consequência os meios de segurança também os são, como aponta Bajaj:

> O domínio unilateral do ciberespaço não pode ser alcançado por nenhum país. Nenhum governo pode combater o crime cibernético ou proteger seu ciberespaço isoladamente. A segurança cibernética não é um problema de tecnologia que pode ser "resolvido"; é um risco a ser administrado por uma combinação de tecnologia defensiva, análise astuta e guerra de informação e diplomacia tradicional. (apud KREMER e MÜLLER, 2014, p.237, tradução nossa)

1.4.2 **Principais entraves para uma cibersegurança internacional.**

Apesar de ser uma necessidade, estabelecer padrões, regras e um tratado internacional de cibersegurança não é uma tarefa simples. Além da questão já abordada sobre soberania[3], surgem dificuldades em âmbitos nacionais e internacionais para implementação de tais regras, como, adequações legislativas, especialização e melhoria do judiciário em questões cibernéticas, direito de privacidade, liberdade de expressão, acesso à informação e questões econômicas e de mercado.

[3] Conferir tópico 1.1

O Legislativo, além de analisar o eventual tratado, teria que elaborar leis seguindo-o, e ainda com mecanismos que essas leis sejam cumpridas. Isto poderia gerar um impacto econômico e cultural em empresas, redes sociais e nos Executivos Federal, Estadual e Municipal. Investimentos em infraestrutura e profissionais de cibersegurança, de equipamentos mais seguros até policiais especialistas em informática, seriam necessários para a consecução e aprimoramento da proteção cibernética.

A adequação do Judiciário passaria por juízes especializados em direito digital e crimes cibernéticos. As investigações e procedimentos tornar-se-iam mais céleres, pois, no ciberespaço os acontecimentos são rápidos e o meio de levantamento de provas e troca de provas entre países é lento, mas flexibilizar esses procedimentos sem uma coordenação entre os Poderes e padrões internacionais pode ameaçar o devido processo legal. Kostopoulos (2017) destaca algumas áreas que precisariam de desenvolvimento, diminuição da burocracia nacional e internacional, melhoria na autenticação de provas cibernéticas, mitigação da perda de evidências, acesso a evidências que se encontram em outros países, legislação abrangente e compreensível, investigadores de crimes cibernéticos e especialistas em cibersegurança em massa.

Implementar leis e investigações dessa maneira demandaria um sistema de vigilância que ficaria em uma linha tênue entre cibersegurança eficiente e desrespeito ao direito à privacidade, liberdade de expressão e acesso à informação. Por enquanto, o que temos é uma aplicação por extensão dos direitos consolidados fora do espaço cibernético no ambiente on-line, como destaca Oliveira:

> A abordagem abrangente baseada em direitos humanos, que estende a lógica de raciocínio dos direitos humanos exercidos off-line aos direitos humanos exercidos on-line pode não ser suficiente, mas é necessária. Afinal, se está distante de um cenário de normatização da pauta dos direitos humanos eletrônicos e, na ausência de um tratado internacional específico sobre os mesmos, apenas o uso de analogias com tratados já postos, como os da Carta Internacional dos Direitos Humanos ou o Pacto de São José da Costa Rica, permite a imposição de regras de conduta aos Estados com relação ao ambiente on-line em sua jurisdição, na medida do possível. (2020, p.253)

O movimento que vemos é a construção de leis domésticas, enquanto não temos uma coordenação internacional. Essa elaboração interna de leis, possivelmente, serão objeto de conflitos em possível tratado posterior, dificultando um consenso sobre cibersegurança e ampliando a margem de reservas por parte dos Países, dificultando a real intenção do tratado. Como exemplo, a legislação brasileira por meio da Lei Geral de Proteção de Dados (LGPD) de

2018, tem, entre outros, como fundamento proteger a privacidade, liberdade de expressão e acesso à informação.

Como destaca Kittichaisaree:

> As legislações nacionais variam significativamente, mesmo nos elementos mais básicos do regime de proteção de dados pessoais. A legislação nacional de cada Estado sobre proteção de dados é baseada no direito de um indivíduo à privacidade, mas o significado da privacidade e as origens do direito de um indivíduo à privacidade podem variar e, consequentemente, as políticas e leis que regem o direito à privacidade muitas vezes diferem de um Estado para outro.
> [...]
> Uma vez que grande parte do processamento de dados é realizado por entidades privadas, um Estado deve regulamentar esse processamento de modo a garantir que os direitos dos indivíduos sejam protegidos de acordo com obrigações ou padrões internacionais vinculativos para o Estado. (2017, p.57 e 66, tradução nossa)

A construção da cibersegurança segue o caminho tradicional de muitas áreas reguladas internacionalmente, primeiros as nações tem uma organização legislativa e jurídica interna, tal área passa a ser globalizada e surge a necessidade de regulamentação de padrões internacionais. Mas o ciberespaço já nasceu da globalização, parece lógico que a regulamentação deveria partir de padrões, tratados e regras internacionais consensualmente discutidas, como postula Kittichaisaree "Os Estados devem respeitar as obrigações internacionais de direitos humanos vinculando-os e, assim, abordar a questão da governança do ciberespaço dentro tais parâmetros." (2017, p. 349, tradução nossa)

Outro aspecto que torna a discussão complexa é o formato de mercado global que temos hoje em dia. A eventual regularização do espaço cibernético traria impactos na política de privacidade e forma de atuação de empresas já estabelecidas pelo globo. Uma rede social passaria por uma adequação para atuar da forma que atua hoje, sediada em um país, mas oferecendo seus serviços em vários, assim, estando sob soberanias diferentes. A cibersegurança trazendo um impacto financeiro em diversas áreas, estas, provavelmente, demonstrariam uma resistência a algum tratado e uma influência sobre as regras do mesmo.

1.5 ATRIBUIÇÃO DA RESPONSABILIDADE INTERNACIONAL

A atribuição da responsabilidade por um ato ilícito internacional fora do ciberespaço já é complicada, este ambiente trouxe maior complexidade ao tema, para o Manual de Tallinn "Um Estado tem responsabilidade internacional por uma operação cibernética atribuível a ele e que constitui uma violação de uma obrigação." (2013, p.29). Mazzuoli define responsabilidade como:

> A responsabilidade internacional do Estado é o instituto jurídico que visa responsabilizar determinado Estado pela prática de um ato atentatório (ilícito) ao Direito Internacional perpetrado contra os direitos ou a dignidade de outro Estado, prevendo certa reparação a este último pelos prejuízos e gravames que injustamente sofreu. (2015, p.615)

A ideia de responsabilidade internacional visa à reparação dos danos e não o âmbito penal, esta é individual e é tratada pelo Tribunal Penal Internacional. Para a atribuição de responsabilidade internacional devemos observar alguns elementos: a) o ato ilícito internacional, “Tal violação pode ser relativa a um tratado, um costume internacional ou qualquer outra fonte do direito das gentes.” (MAZZUOLI, 2015, p.621); b) nexo causal, que liga o ato ilícito ao dano, "significa que o ato ou omissão é atribuível ao Estado" (Accioly apud MAZZUOLI, 2015, p.622) e; c) dano, prejuízo sofrido pelo Estado recebedor do ato ilícito, “Tal prejuízo (resultado antijurídico do fato) pode ser material ou imaterial (moral), e pode ter decorrido de um ato ilícito cometido por um Estado (ou organização internacional) ou por um particular em nome do Estado.” (MAZZUOLI, 2015, p.623).

Dos elementos que caracterizam a responsabilidade internacional, o mais complexo é o nexo causal. A quantidade de ataques e dificuldade em rastreá-los com eficiência pode trazer atribuições equivocadas e gerar tensões políticas indesejadas. Kittichaisaree diz que:

> Para o propósito de atribuição de responsabilidade no ciberespaço, deve-se identificar a fonte de origem da comunicação, percorrendo a rota pela qual a comunicação venho, a pessoa/ entidade por trás dela, e se essa pessoa/entidade é dirigida ou controlada por outra pessoa/entidade ou um Estado. (2017, p. 37, tradução nossa)

Estabelecer essa fonte de origem ainda é um exercício complicado e cheio de falhas, algumas dimensões como velocidade em traçar a fonte de ataque, mesmo traçando a fonte do ataque, revelar com exatidão a identidade do criminoso ou Estado atacante por de trás da máquina fonte é mais complicado, e o atual aparato estatal não tem a especialização necessária para uma eficiente investigação, como destaca Kremling e Parker “A investigação de crimes cibernéticos é muito complexa, exigindo especialistas em segurança cibernética. A tradicional aplicação da lei não inclui tais habilidades especializadas.” (2017, p.359, tradução nossa). Fernandes ainda aponta que:

> Por último, o delicado e crucial problema de traçar a origem de um ciberataque. Desde logo, uma dificuldade surge aqui pelo fato de os ciberataques serem frequentemente conduzidos por meio de outros computadores e/ou sistemas informáticos, de modo a esconder a sua procura e esconder a sua real autoria. Depois, há a dificuldade e risco, já anteriormente mencionados, de que os programas que ajudam a traçar a autoria do ataque poderem não identificar corretamente a autoria do ataque. Esse risco de

> atribuição errada pode levar a que o ataque seja percebido como tendo vindo de um Estado, quando este não é o verdadeiro Estado de origem do mesmo. (2012, p.22)

Sklerov sugere que "Estados que recusam a atuar em conformidade com o seu dever internacional de prevenir que o seu território seja usado para cometer ciberataques, escolheram o risco de serem considerados indiretamente responsáveis, por acidente" (2009, p.94, tradução nossa) e mesmo que um Estado seja a ponte de um Estado atacando o outro, mas tenha medidas se segurança e coopere na investigação com o Estado alvo, essa responsabilidade seria afastada.

A Comissão de Direito Internacional das Nações Unidas apresentou em 2001 um projeto sobre responsabilidade dos Estados, mas até os dias atuais ainda é apenas um projeto. Alguns artigos apresentam a possibilidade de um Estado responder por atos mesmo que uma pessoa ou entidade, desde que estas atuem com atribuições de Poder Público. O artigo 11 do projeto traz uma regra que que corrobora com o pensamento de Sklerov, um ato que mesmo não sendo oficialmente praticado em nome do Estado ou pessoas e entidades sob sua tutela, mas que seja sabidamente reconhecido internacional como prática e conduta desse Estado, pode trazer a responsabilidade, ou seja, no contexto de ciberespaço, a conduta de não cumprir padrões de cibersegurança e ser alvo vulnerável para ser usado para atacar outros é escolher o risco de ser responsabilizado.

Tanto por questões tecnológicas quanto legais, a atribuição de responsabilidade por um ciberataque influência a ciberguerra. Concluir a fonte de um ataque de forma errônea pode desencadear tensões entre Estados com nenhuma relação direta nos ciberataques em questão. Apesar da urgência de uma regulamentação internacional do ciberespaço e da cibersegurança, não parece ser uma prioridade, como aponta Graham:

> Ainda mais revelador, vários participantes globais têm demonstrado consistentemente uma falta de desejo em lidar com ataques cibernéticos por meio de uma aplicação eficaz da lei. Na verdade, vemos o inverso. A cortina de fumaça de um Estado que atribui ataques cibernéticos exclusivamente a particulares dentro de um Estado pode frequentemente servir como uma cobertura conveniente para Estados que podem estar direcionando ou intencionalmente tolerando tais ataques. (2010, p.93, tradução nossa)

Por fim, após estabelecer o nexo causal entre ataque e dano, para cometer um ato ilícito o mesmo deve ser regulamentado pelo direito internacional como tal ato, e muitas práticas cibernéticas ainda carecem de tal formalismo, Dionísio destaca "Os Estados não incorrem em responsabilidade internacional se praticarem atos que sejam permitidos ou não regulamentados pelo Direito Internacional, assim a título de exemplo um Estado que pratique atos de ciberespionagem não incorrerá em responsabilidade internacional." (2018, p.83). A falta de

uma regra internacional normatizando atos ilícitos cibernéticos por parte dos Estados impossibilita a responsabilização por eventual dano.

2 MANUAIS DE TALLINN: REGULAMENTAÇÃO DA CIBERGUERRA JÁ PRONTA

2.1 ORIGEM E PROCESSO DE ELABORAÇÃO

O ponto de partida para a elaboração do Manual de Tallinn se deu após uma série de ciberataques contra a Estônia em 2007. O país, já em 2007, tinha mais de 90% dos serviços públicos e privados computadorizados, por três semanas esses serviços foram alvos de ataques de vários pontos ao redor do mundo, mas grande parte da fonte de ataques era originário da Rússia, que nega envolvimento nos ataques. Esses eventos levaram a Estônia propor em 2008 a criação de um centro de excelência em ciberdefesa no âmbito da Organização do Tratado do Atlântico Norte (OTAN), assim surge o Centro de Excelência em Ciberdefesa Cooperativa[4], que tem status de organização militar internacional.

Ao todo, cerca de vinte experts em direito internacional foram convidados para fazer parte do centro de excelência e identificar quais legislações internacionais existentes se aplicariam em uma ciberguerra. A partir de 2009 o grupo estava formado e se dá início às pesquisas e produção do Manual, na capital Estoniana, Tallinn, que dá o nome ao Manual. Depois de três anos de elaboração, em 2013, a primeira versão do Manual foi publicada pela *Cambridge University Press*[5], trazendo o título "Manual Tallinn sobre a Lei Internacional Aplicável à Ciberguerra", o Manual se descreve como:

> Produto de um projeto de três anos de vinte renomados estudiosos e profissionais do direito internacional, o Manual de Tallinn identifica o direito internacional aplicável à guerra cibernética e estabelece noventa e cinco "regras sólidas" [6]que regem esses conflitos. Aborda tópicos como soberania, responsabilidade do Estado, o *jus ad bellum*, Direito Internacional Humanitário e Direito da Neutralidade. Um extenso comentário acompanha cada regra, que estabelece a base de cada regra no tratado e na lei consuetudinária, explica como o Grupo de Especialistas interpretou as normas aplicáveis no contexto cibernético e descreve quaisquer divergências dentro do grupo quanto à aplicação de cada regra. (SCHMITT, 2013, p.2, tradução nossa)

Essa primeira versão do manual lida com a situação de ciberataques poderem levar a um conflito armado, em geral, preocupa-se com o *jus ad bellum* e o *jus in bellum*. O primeiro trata-se de examinar quais critérios seriam justos para entrar em guerra ou invocar a legítima defesa para contra-atacar, os motivos de uma guerra. O segundo, é o direito na guerra propriamente

[4] No original, Cooperative Cyber Defence Centre of Excellence (CCDCOE).
[5] Editora da Universidade de Cambridge.
[6] No original é usado o termo 'black-letter rules', utilizado no inglês como leis e posições estabelecidas, equivalente à 'jurisprudência pacífica'.

dito ou Direito Humanitário, os limites na condução de uma guerra e mitigação de seus efeitos colaterais aos civis.

Em 2017, foi lançado um novo manual, intitulado “Manual de Tallinn 2.0 Sobre a Lei Internacional Aplicado à Operações Cibernéticas”, uma continuação do primeiro, estendendo para um contexto de tempos de paz a aplicação de leis e preceitos internacionais a operações cibernéticas de Estados. Não se trata de um manual de cibersegurança, apenas aumenta o número de regras, relacionando temas de direito internacional já existentes aplicadas no cenário do ciberespaço, como, operações em alto mar e operações aéreas. Embora haja uma expansão dos temas, boa parte do segundo manual é apenas a repetição do primeiro, apenas em um primeiro momento trata-se de operações internacionais de Estados fora de uma situação de conflito armado, ou seja, operações que podem violar normas internacionais que não ensejam o uso da força. A versão 2.0 do manual traz como descrição:

> O Manual de Tallinn 2.0 expande a altamente influente primeira edição, estendendo sua cobertura da lei internacional que rege a guerra cibernética para regimes jurídicos em tempos de paz. O produto de um projeto de acompanhamento de quatro anos por um novo grupo de 19 renomados especialistas em direito internacional, aborda temas como soberania, responsabilidade do Estado, direitos humanos e direito do ar, espaço e mar. O Manual de Tallinn 2.0 identifica 154 "regras sólidas" que regem as operações cibernéticas e fornece comentários extensos sobre cada regra. Embora o Manual de Tallinn 2.0 represente as opiniões dos especialistas em sua capacidade pessoal, o projeto se beneficiou da contribuição não oficial de muitos Estados e de mais de 50 revisores. (SCHMITT 2017, p.9, tradução nossa)

Ambos manuais revelam ter em sua espinha dorsal cunho militar das operações abordadas, seja em conjuntura de conflito armado ou não. Pouco é abordado sobre questões fora do contexto militar ou que já não tenham uma norma internacional aplicada fora do ciberespaço, como por exemplo, quando aborda ciberespionagem de forma mais genérica “Embora a ciberespionagem em tempos de paz por parte dos Estados não viole por si só o direito internacional, o método pelo qual é realizada pode violar” (SCHMITT, 2017, p.168, tradução nossa).

2.2 ESTRUTURA DO MANUAL

A primeira versão do Manual está estruturada em duas partes, a primeira “Lei Internacional de Cibersegurança”, tratando de Estados e ciberespaço e o uso da força, a segunda “A Lei de Ciberconflito Armado”, abordando lei de conflito armado em geral, condução das hostilidades, certas pessoas, objetos e atividades, ocupação e neutralidade. Cada parte subdivide-se em capítulos, estes em seções e em cada seção as regras. A segunda versão segue

a mesma estrutura, partes, capítulos, seções e regras, mas acrescenta duas novas partes, “Paz Internacional e Segurança e Ciberatividades” e “Regimes Especiais de Leis Internacionais e Ciberespaço”, as outras duas partes são uma reprodução do primeiro manual, onde “A Lei de Ciberconflito Armado” é mantida e “Lei Internacional de Cibersegurança” muda para “Lei Internacional Geral e Ciberespaço”, mudando apenas o título, as regras continuam com as mesmas descrições.

Apesar do nome da primeira parte do Manual trazer o nome “Lei Internacional de Cibersegurança”, não se trata de uma abordagem sobre cibersegurança internacional propriamente dita ou de padrões para cooperação entre Estados para proteção no ambiente do ciberespaço. Sobre o termo utilizado o Manual esclarece que:

> O termo "Lei Internacional de Cibersegurança" não é um termo técnico legalista. Em vez disso, o objeto e a finalidade de seu uso aqui é capturar os aspectos do direito internacional público que se relacionam com o uso hostil do ciberespaço, mas não são formalmente um aspecto do *jus in bello*. Portanto, o termo é apenas descritivo. Neste manual, ele se refere principalmente ao *jus ad bellum*. No entanto, também incorpora conceitos jurídicos como soberania, jurisdição e responsabilidade do Estado, na medida em que se relacionam com o funcionamento do *jus ad bellum* e do *jus in bello*. (SCHMITT, 2013, p.13, tradução nossa)

As regras foram formuladas a partir da discussão e consenso entre os especialistas convidados. Elas foram pensadas em cima de normas internacionais imperativas que são aplicadas fora do ciberespaço já aceitas pela maioria dos Estados, não inova nenhuma lei internacional nem sugere alguma política doméstica. A respeito das regras o Manual expõe:

> Não há disposições de tratado que lidem diretamente com a "ciberguerra". Da mesma forma, como as práticas cibernéticas dos Estados e as expressões publicamente disponíveis de opinio juris são esparsas, às vezes é difícil concluir definitivamente que existe qualquer norma de direito internacional costumeiro específica para o ciberespaço. Sendo assim, qualquer alegação de que cada afirmação do Manual representa uma reformulação incontestável do direito internacional seria um exagero. Essa incerteza não significa que as operações cibernéticas existam em um vazio normativo. O Grupo Internacional de Especialistas foi unânime em sua estimativa de que tanto o jus ad bellum quanto o jus in bello se aplicam às operações cibernéticas. Sua tarefa era determinar como essa lei se aplicava e identificar quaisquer aspectos cibernéticos dessa lei. As regras estabelecidas no Manual de Tallinn refletem, portanto, o consenso entre os Especialistas quanto à lei existente aplicável, ou seja, a lei que rege atualmente o conflito cibernético. Não estabelece lei futura, prática recomendada ou política preferencial.[7] (SCHMITT, 2013, p.5, tradução nossa)

Cada regra é seguida de comentários das razões daquela regra. Os comentários justificam como os especialistas chegaram em consenso sobre a regra, e que os mesmos a

[7] O Manual de Tallinn 2.0 traz a mesma descrição sobre as regras.

elaboraram de forma imparcial, a interpretação deles sobre a regra, a base legal que sustenta a rega, traz a terminologia de palavras utilizadas que possam ser ambíguas e possíveis situações praticas que a regra se aplicaria.

> O Comentário que acompanha cada regra destina-se a identificar sua base legal, explicar seu conteúdo normativo, abordar implicações práticas no contexto cibernético e estabelecer posições diferentes quanto ao escopo ou interpretação. Em particular, o Grupo Internacional de Especialistas procurou assiduamente capturar todas as posições razoáveis para inclusão no Comentário do Manual de Tallinn. Como nem a aplicação de um tratado nem a prática de Estados estão bem desenvolvidas neste campo, o grupo considerou de extrema importância articular todos os pontos de vista concorrentes de forma completa e justa para consideração pelos usuários do Manual. (2013, p.6, tradução nossa)

Portanto, o Manual tenta ser o mais didático possível, estruturando-se como um código de leis, mas no lugar de artigos temos regras e cada regra tem a sua exposição de motivos particular para diminuir a margem de interpretação para além da regra estipulada.

2.3 RECEPÇÃO E CRÍTICAS AO MANUAL

Os manuais não são instrumentos jurídicos vinculativos aos Estados, são de natureza acadêmica, ainda que, já se tenha especulações que serviria de norte para juristas e Nações na condução de situações elencadas pelos manuais.

> É essencial entender que o Manual de Tallinn não é um documento oficial, mas sim, apenas o produto de um grupo de especialistas independentes agindo apenas em sua capacidade pessoal. O manual não representa as opiniões do CCDCOE da OTAN, seus países patrocinadores ou da OTAN. Em particular, não pretende refletir a doutrina da OTAN. Nem reflete a posição de qualquer organização ou Estado representado por supervisores. Finalmente, a participação no Grupo Internacional de Especialistas por indivíduos com cargos oficiais em seus próprios países não deve ser interpretada indicando que o Manual representa os pontos de vista desses países. Em última análise, o Manual de Tallinn deve ser entendido como uma expressão unicamente das opiniões do Grupo Internacional de Peritos, todos agindo em sua capacidade privada. (SCHMITT, 2013, p.11, tradução nossa)

Mesmo que o projeto seja um primeiro passo para uma efetiva regulamentação de ciberoperações, o que se viu na prática até hoje foram posições divergentes sobre os manuais por algumas razões. Primeiro, pela questão de o grupo de experts serem de nacionalidades restritas aos países partes da OTAN no primeiro manual e no segundo, apesar de haver mais diversidade, ainda, continuava com apenas vinte profissionais, o que consequentemente, não engloba a posição da maioria dos países sobre o assunto.

> Uma questão preliminar levantada por uma série de críticos quanto à autoridade do Manual foi, se é um reflexo do direito internacional existente, ou apenas a articulação dos pontos de vista de grupo internacional de especialistas sobre como o Direito Internacional deve ser aplicado às operações cibernéticas (incluindo, às vezes, pontos de vista de consenso e dissensão). (Efrony e Shany, 2018, p.589, tradução nossa)

Em segundo lugar, o que se viu na prática em casos que poderiam encaixar-se nas regras dos manuais, foi uma situação de silêncio por parte dos países que foram vítimas de ataques, que preferiram não tornarem públicos a maioria dos ataques. Um estudo realizado em 2018 por Dan Efrony e Yuval Shany, analisou onze casos de ciberataques internacionais, foi identificado segundos os autores:

> Uma lacuna que identificamos entre a prática estatal e algumas regras chave de Tallinn é parcialmente explicada pela controvérsia em torno do conteúdo das regras que, às vezes, sugere dúvidas sobre as premissas normativas das quais elas se desenvolveram. Mais significativamente, no entanto, os estudos de caso sugerem que alguns Estados tendem a sair de seu caminho para evitar confiar pública e explicitamente em regras específicas do direito internacional (jus ad bellum e jus in bello) em conexão com operações cibernéticas, optando por uma política de silêncio e ambiguidade. Portanto, alguns estados vítimas não reconhecem que foram atacados; ao reconhecer que foram atacados, os estados não tendem a atribuir responsabilidades a outros estados; e ao atribuir responsabilidades, a maioria dos estados não invoca explicitamente o direito de se envolver em contramedidas, que as regras de Tallinn fornecem. (2018, p.587, tradução nossa)

Essa distância entre a realidade da prática dos Estados e as regras dos manuais levam a uma terceira crítica, que é o caráter apenas teórico dos estudos. Não houve pesquisa empírica sobre a atuação estatal internacional no ciberespaço para a elaboração dos documentos, o que levou a regras muito vagas, "outros críticos expressaram preocupação com a ampla dependência do grupo internacional de especialistas em princípios abertos e fatores contextuais, que criam uma incerteza significativa em sua aplicação" (EFRONY e SHANY, 2018, p.589, tradução nossa).

A grande preocupação com esses princípios abertos é a margem de interpretação que poderia dar aos Estados sobre quando um ciberataque dá o direito de contra-atacar com o uso a força. A regra onze do Manual trata do uso da força "Uma ciberoperação constitui uso da força quando sua escala e efeitos são comparáveis a operações não cibernéticas que chegam ao nível do uso da força" (SCHMITT, 2013, p.45, tradução nossa). Enquanto a regra treze traz "Um Estado que é alvo de uma ciberoperação que chega ao nível de um ataque armado pode exercer seu direito inerente de autodefesa. Se uma operação cibernética constitui um ataque armado depende de sua escala e efeitos." (SCHMITT, 2013, p.54, tradução nossa). Ao estabelecer essa

"escala e efeitos" são postos oito fatores principais[8] a se examinar se um ciberataque é ou pode levar ao uso da força ou a autodefesa, sendo eles: gravidade; dano imediato; direção do ataque; setor invadido; mensurabilidade de efeitos; caráter militar; envolvimento estatal e presunção de legalidade. Esse tipo de regras abertas somadas a falta de diversidade de opiniões na formulação dos manuais pode levar a ambiguidade de interpretação, a escala e efeitos da gravidade dos ciberataques de um Estado mais dependente de tecnologia em suas operações, ou Estados mais radicais pode ter um limiar mais curto ou mais longo de quando partir para o uso da força e conflito armado.

Outro ponto criticado nos manuais é a "diligência prévia" ou "devida diligência" tratada nas regras seis e sete, que prescrevem:

> Regra 6 - Um Estado deve exercer a devida diligência em não permitir que em seu território, ou sua infraestrutura cibernética sob seu controle governamental, seja usado para operações cibernéticas que afetam os direitos ou produzam consequências adversas graves para outros Estados.
> Regra 7 - O princípio da devida diligência exige que um Estado tome todas as medidas que são viáveis nas circunstâncias para pôr fim às operações cibernéticas que afetam os direitos ou produzam consequências adversas graves para outros Estados. (SCHMITT, 2017, p.30 e 43, tradução nossa)

O que é criticado neste ponto é que sem um tratado ou documento como o Manual de Tallinn falando sobre cibersegurança internacional e definindo padrões de como seria essa diligência prévia. A falta de nitidez de como seria a atribuição de responsabilidade desses Estados que sem tomar a devida diligência seriam a ponte de ciberataques de um país a um terceiro, poderia gerar consequências graves sem uma base de verificação se realmente essa diligência foi violada e como apontam Efrony e Shany:

> A habilidade para atribuir a responsabilidade de um Estado por falta de diligência exige que o Estado infrator seja confrontado com evidências que vinculem a operação em questão ao seu território e, mais ainda, que a estabeleçam, como uma questão legal e de fato, seu conhecimento real ou construtivo, e apoio ou aquiescência. (2018, p.645, tradução nossa)

Por fim, o modo como os manuais ficam distantes dos Direitos Humanos e focam na ciberguerra, mesmo o segundo manual que, teoricamente, trata de ciberoperações que não levariam a um conflito armado "o grupo internacional de especialistas atribuiu espaço limitado e conteúdo minimalista ao Direito Internacional do Direitos Humanos (DIDH) em ciberespaço,

[8] O Manual os coloca como um rol exemplificativo, aumentando mais ainda a margem de interpretação por parte dos Estados.

quando comparado ao tratamento dado às leis da guerra (*jus in bello e jus ad bellum*)" (EFRONY e SHANY, 2018, p.589, tradução nossa).

Os manuais precisam de uma revisão para que abarquem situações que não sejam apenas de cunho militar e que abordem cibersegurança a fundo. Atualmente, tal expansão do Manual está em andamento, um projeto para o "Manual de Tallinn 3.0" foi lançado. Ao que tudo indica, este projeto, ao contrário dos dois anteriores, será mais aberto a outros contextos e mais diversificado entre países. O Centro de Excelência em Ciberdefesa Cooperativa, por meio de seu site oficial está recebendo sugestões de alterações, revisões e novos tópicos para o novo manual[9], uma boa iniciativa para ouvir novos contextos de ciberespaço e suas necessidades, apesar da limitação da língua (apenas inglês) essa contribuição está aberta para qualquer um no globo fazer. Apesar de ser um documento não vinculativo, por enquanto, esses manuais têm grande prestígio entre os membros da OTAN, essa posição de receber opiniões de todos para a construção de um novo manual pode ser o início de uma discussão realmente séria sobre cibersegurança.

[9] É possível contribuir com o novo Manual de Tallinn 3.0 pelo endereço: https://ccdcoe.org/research/tallinn-manual/

3 GUERRA JÁ EM ANDAMENTO

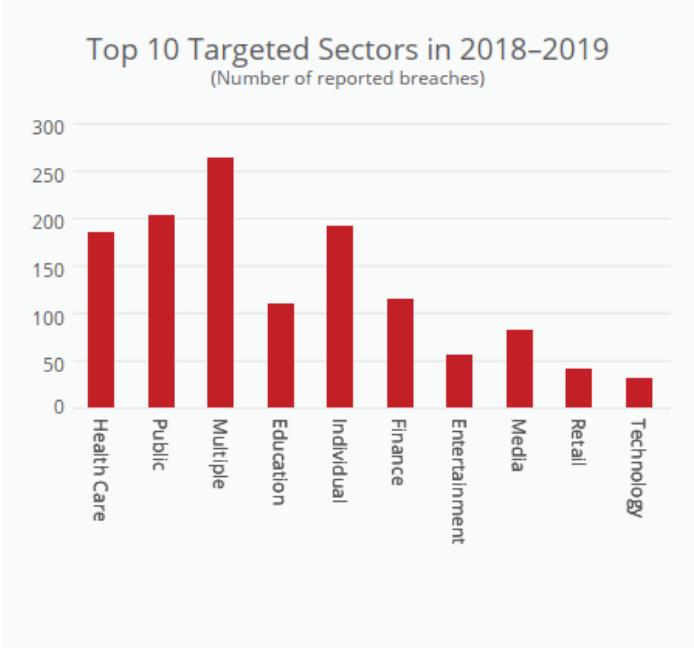
3.1 QUANTIDADE DE ATAQUES

Ainda em 2007 um relatório da empresa especializada em cibersegurança *McAfee* apontou que grande parte dos países já utilizavam a internet para espionagem, afirmando que "aproximadamente 120 países trabalhando nos seus comandos de ataques virtuais, os especialistas acreditam que, em um período de 10 a 20 anos, poderemos ver países lutando pela supremacia virtual" (2007, p.12). No mesmo relatório, especialistas da Organização do Tratado do Atlântico Norte (OTAN) revelam que grande parte dos governos ainda não tem ideia das ameaças e seus problemas e assumem posições que facilitam os ataques.

Do relatório de 2007 para cá, o volume de ataques online aumentou significativamente. A compilação desses ciberataques é feita por empresas de cibersegurança que têm parcerias com grandes empresas e governos, além de oferecer serviços de proteção individual. Para compilar os dados elas monitoram tentativas de ataques ou ataques reportados. Encontramos alguns relatórios anuais de ataques e mapas de ataques em tempo real, como das empresas de cibersegurança *McAfee*, *Check Point, Kaspersky e SonicWall*.

Entre 2018 e 2019, em seu relatório anual, a *McAfee* identificou mais de 200 milhões de ataques apenas a setores públicos.

Figura 1 - Setor Público (segundo da esquerda para direita)

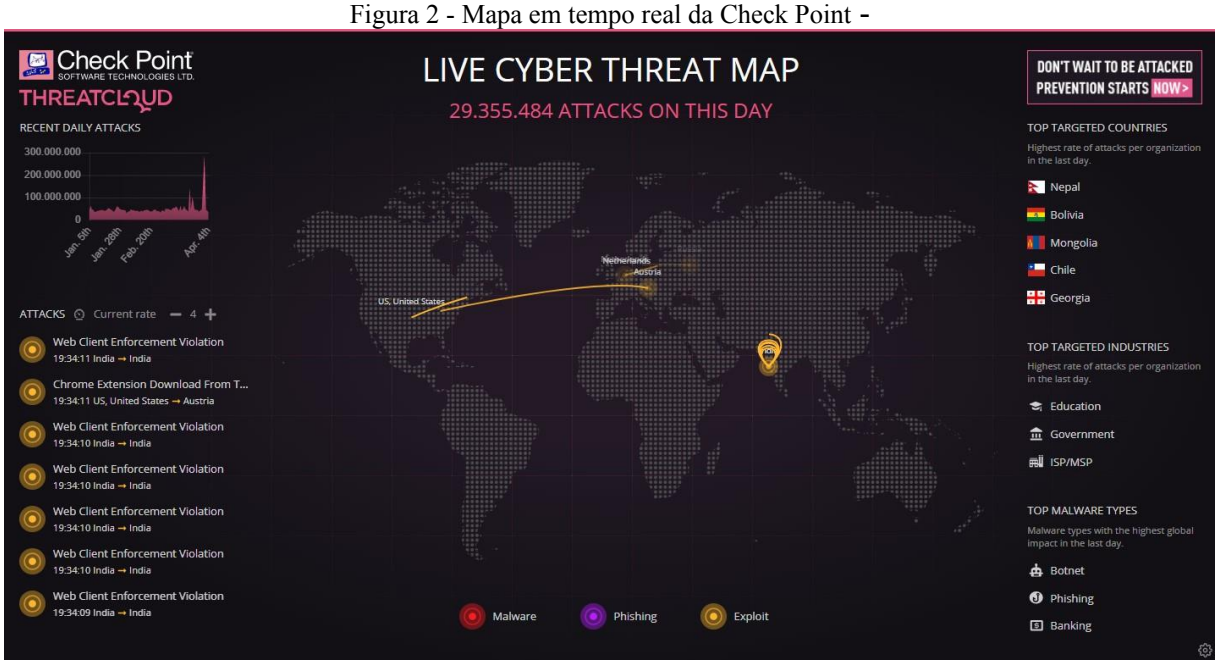


Fonte: Threats Report. p. 40. McAfee - Santa Clara, Califórnia, 2019.

A empresa *Check Point* mantém um site de monitoramento de ciberataques diários, compilando dados sobre origem, tipo de ataque e alvos. Apenas em dia foram detectados quase 30 milhões de ataques, com os setores de educação, governo e indústria sendo os principais alvos. De acordo com a empresa *Check Point*, em seu relatório anual de 2020, com a pandemia de corona vírus, houve um aumento e melhoria de ataques de espionagem entre nações, de acordo com o relatório:

> A pandemia COVID-19 remodelou dramaticamente a arena cibernética interestadual. Desafiou unidades de inteligência, redefiniu metas e criou novas oportunidades para os atores da ameaça. Em tempos em que a atividade de inteligência tradicional é limitada devido a bloqueios sustentados, distanciamento social e restrições de viagens internacionais, o uso de ofensivas. As ferramentas cibernéticas para realizar operações de coleta de informações e espionagem nacionais parecem ter se expandido. Na verdade, a nova inteligência cibernética se tornou a arma preferida de muitos países. (2020, p.7, tradução nossa).

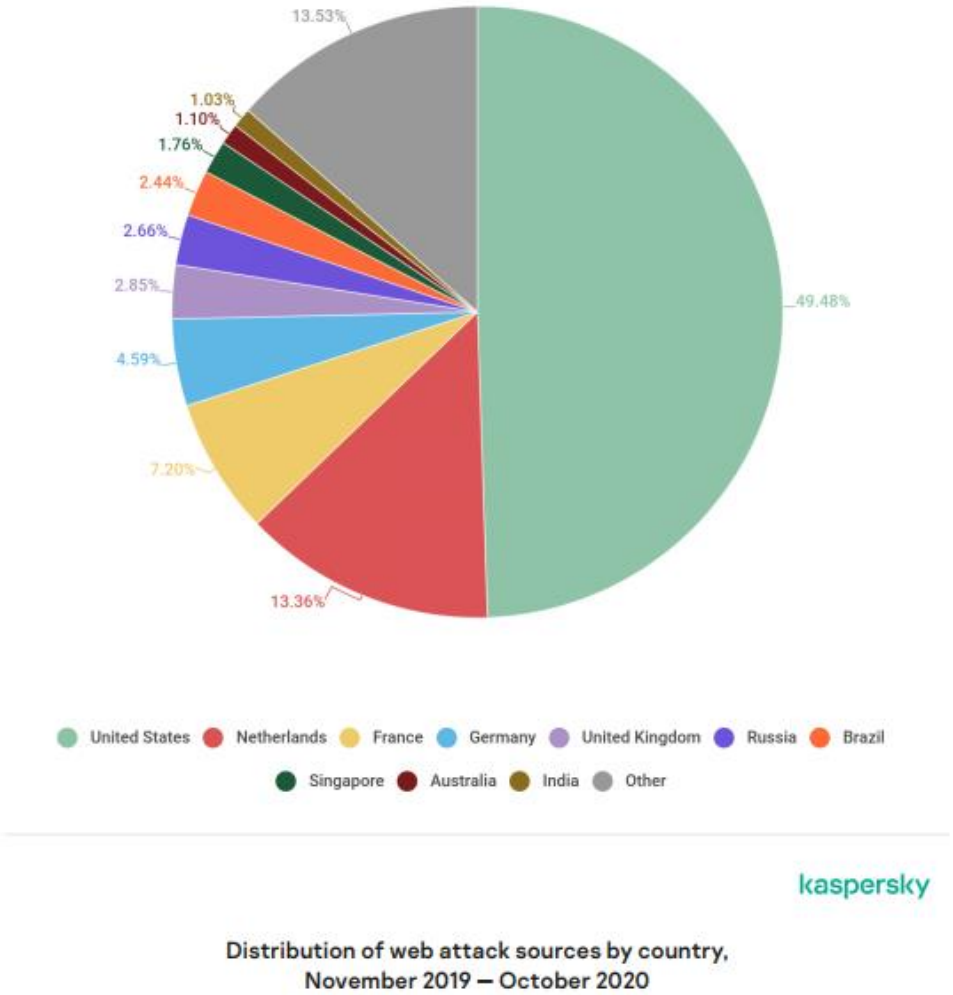
Figura 2 - Mapa em tempo real da Check Point -



Fonte: https://threatmap.checkpoint.com (imagem do dia 04 de abril de 2021, por volta de 23 horas).

Já a *Kaspersky* em seu relatório anual sobre cibersegurança de 2020, identificou que quase 87% da origem de ataques identificáveis provém de dez países: Estados Unidos, Holanda, França, Alemanha, Reino Unido, Rússia, Brasil, Singapura, Austrália e Índia. Sendo que, quase 50% do total de ataques tem origem dos Estados Unidos, país de maior investimento no setor. Já a China, expoente no setor cibernético, não aparece em nenhum dado devido à falta de transparência e dificuldade de acesso a dados do país.

Figura 3 - Origem de ataques por países



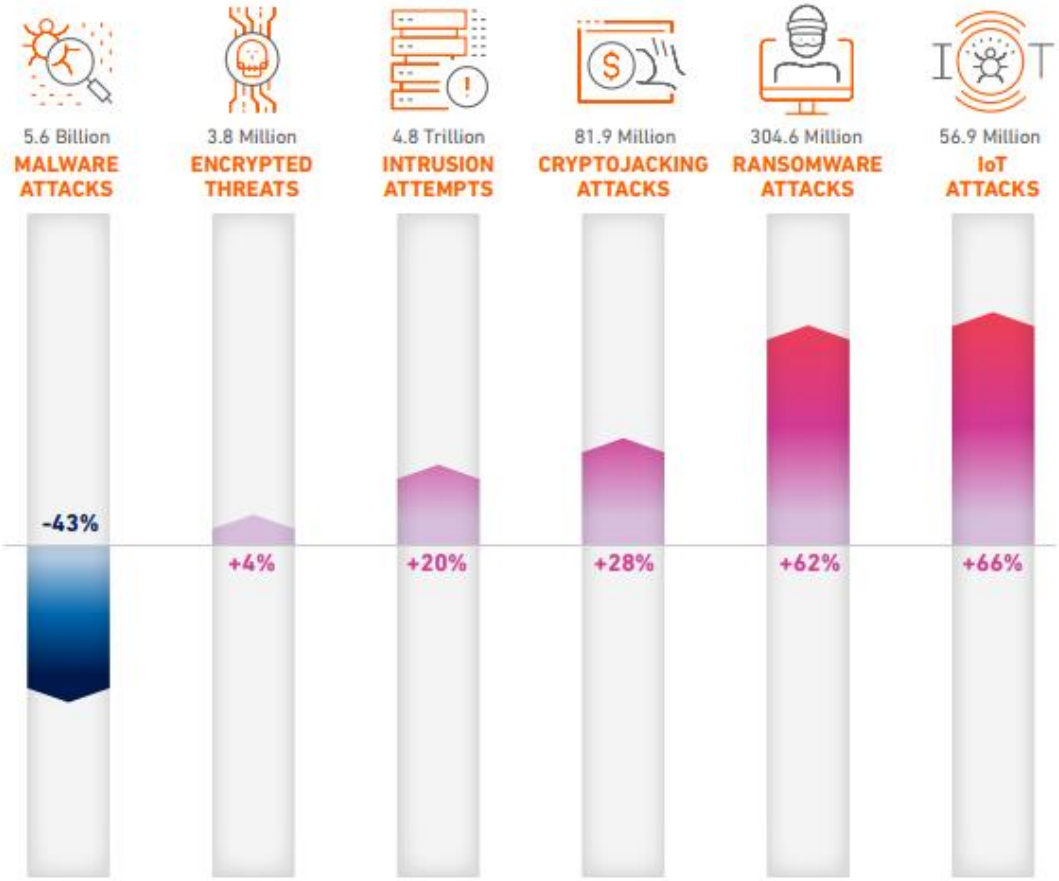
Fonte: relatório de estatísticas de ciberataques. p.20. Kaspersky, 2020.

A *SonicWall* compilou a quantidade de ataques por espécie de ataque, foi dividido entre *malware*, ameaças criptografadas, tentativas de invasão de sistemas, mineração de criptomoedas, ataque de resgate e internet das coisas. Foi computado a estimativa de ataques de 2020 e comparado com 2019. Apenas os ataques por *malware* que houve queda, mesmo com 43% de queda em 2020 em relação a 2019, 5,6 bilhões de ataques somente com esse tipo de ameaça foram registrados. Somando todos os ataques registrados chegamos a quase 5,4 trilhões de ataques apenas em 2020.

Dentre todos esses ataques, definir o que pode ou não ser um ciberataque entre nações é um processo delicado. Em todos os relatórios citados demonstra-se o aumento de ataques a governos e suas instituições com indicativos que certas regiões são ponto de partida dos ataques com mais frequência. Nesse sentido, além de estabelecer uma cadeia de investigação, processamento e julgamento dessa quantidade de ataques, encontramos uma grande incógnita

com essa quantidade de ataques e a forma como funciona o ciberespaço, que é como atribuir responsabilidade pelo ciberataque.

Figura 4 - Tendências de ciberataques globais do último ano.



Fonte: Relatório Sonic Wall de ciber ameaças. p.5, 2021.

3.2 CASOS EMBLEMÁTICOS

3.2.1 **Estônia 2007**

Considerado como o primeiro caso de ciberataques em massa a uma país, os ataques cibernéticos à Estônia, em 2007, tiveram como provável motivo uma estátua. O país era parte da União Soviética até a sua dissolução em 1991, a estátua é símbolo da vitória da antiga União Soviética contra o nazismo, intitulada como “Soldado de Bronze de Tallinn” e representa um soldado vestindo o uniforme do Exército Vermelho e ficava no centro da capital estoniana, Tallinn. O monumento localizava-se no centro da cidade, mas em abril de 2007, o governo estoniano decidiu muda-lo de local, causando revolta na comunidade russa residente no país e na própria Rússia.

Após tensões pelo episódio, protestos e até embate com a polícia, começa uma série de ataques cibernéticos a toda a Estônia, vindos de todas as partes do mundo. O país, já em 2007,

era uma das nações mais integradas à internet, desde eleições até compras de supermercado dependem de computadores e redes. Por cerca de três semanas o país sofreu com esses ataques tendo praticamente parado todos os serviços como transações bancárias, escolas online, sites estatais e até uma simples compra em supermercados foi prejudicada, pois, computadores não funcionavam corretamente para utilizarem os leitores de códigos de barras. Haataja destaca que:

> A Estônia era particularmente vulnerável à ameaça de ciberataques, dado o grau em que integrou soluções baseadas na internet na maioria dos aspectos da vida pública já em 2007. Tudo, desde o preenchimento de ações de seguridade social e impostos, ocorre inteiramente de forma digital, e a votação on-line também já era possível em eleições locais na época. Os ciberataques visaram vários sites da Estônia, incluindo os do Presidente, Primeiro Ministro, Parlamento, a maioria dos departamentos governamentais, partidos políticos, organizações de mídia, bancos e Provedores de Serviços de Internet (ISPs). Eles também visaram a infraestrutura de internet e os sistemas de informação da Estônia, como o serviço nacional de nomes de domínio (DNS) e os DNSs operados por vários ISPs. O principal efeito dos ataques foi perturbador. Eles interromperam o acesso a vários sites e os serviços que prestavam, afetaram o funcionamento dos canais de comunicação do governo e causaram ligeiras interrupções nas redes móveis e na linha de serviços de emergência. As interrupções afetaram seriamente a operação diária de várias organizações, incluindo bancos, departamentos governamentais e pequenas empresas. Os canais de comunicação online entre o governo e os estonianos também foram temporariamente prejudicados e, dado o grau em que serviços públicos importantes eram apenas acessíveis online, a falta de acesso a esses serviços teve um 'Efeito discernível' para muitas pessoas. Algumas estimativas quantificam o impacto econômico dos ataques entre 27 e 40 milhões de dólares dos Estados Unidos (EUA). (2017, p.3)

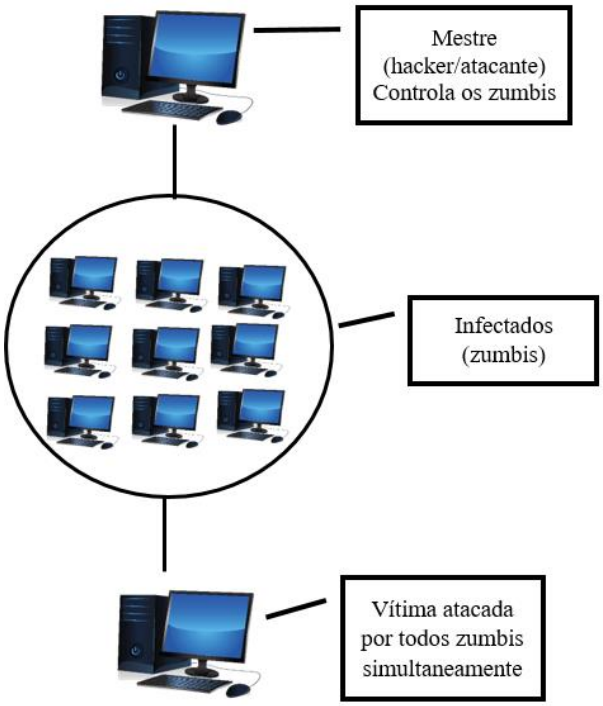
Os ataques foram realizados por meio de "ataque de negação de serviço"[10] também conhecido pelo nome "ataque distribuído de negação de serviço"[11]. O princípio básico desse tipo de ataque é ter computadores "mestres" que infectam vários outros computadores, transformando-os em "escravos" que realizam ataques automáticos à alvos determinados pelos mestres. Os ataques não são invasões aos sistemas ou infecção por vírus de computadores, mas, um acesso em massa a um servidor ou conjunto de servidores, sobrecarregando-os até se tornarem inacessíveis.

Após investigações, a Estônia, além de identificar ataques vindos de todos os lugares do mundo, conseguiu rastrear que muitos dos ataques estavam vindo de servidores russos. Somando com a conjuntura de tensão política pós remoção da estátua, foi atribuído à Rússia os ataques. Fóruns em língua russa foram encontrados com postagens incentivando os ataques e maneiras de participar dos ataques, o governo estoniano chegou a acionar os Estados partes da OTAN reivindicando a aplicação do artigo quinto do tratado do atlântico norte que traz que um

[10] No original *Denial of Service* (DoS)
[11] No original *Distributed Denial of Service* (DDoS)

ataque armado contra um dos membros configura um ataque a todos Estados parte, e consequentemente, podem reagir por legítima defesa de forma conjunta. Mas como o artigo expressa “ataque armado”, à época, ciberataques não tinham nenhum parâmetro de configurar um ataque armado, além de os elementos probatórios apresentados não eram conclusivos para atribuir os ataques inteiramente a Rússia, que nega envolvimento, o pedido estoniano não foi atendido.

Figura 5 - Representação de um ataque de negação de serviço.



Fonte: o autor.

Depois dos ataques nenhum responsável foi encontrado oficialmente, mas levou a uma mudança de postura em relação a cibersegurança, não apenas da Estônia. Vários países tendo em vista o potencial dos prejuízos de ciberataques começaram uma corrida na melhoria de defesa nesta área.

> No final, os dias da Estônia sofrendo um DDoS massivo resultaram na perda de 97 por cento de suas transações bancárias durante aquele tempo, a ameaça de perda de redes de energia e água, a desfiguração ou desligamento temporário de sites e servidores de e-mail de governos e partidos políticos estonianos e, finalmente, na percepção de que a Estônia de 2007 era extraordinariamente vulnerável a esse tipo de ataque. A maior questão remanescente em relação ao ataque DDoS na Estônia é se os países ligados à internet aprenderam todas as lições que ele oferece. (CONNELLY, 2017, p.104 e 105)

Os ataques também foram o principal motivo para a elaboração do Manual de Tallinn e alguns avanços em legislações internas sobre o ciberespaço, embora, ainda hoje, o desenvolvimento de uma forense digital que seja efetiva em investigar e atribuir responsabilidade por ataques cibernéticos não exista.

3.2.2 **Stuxnet 2010**

Considerado como o primeiro programa de ciberguerra com um alvo específico, o *stuxnet* surpreendeu por sua complexidade e objetividade. Descoberto em junho de 2010, apesar de suspeitas sobre os responsáveis, até hoje é de autoria desconhecida, mas com uma certeza por parte dos especialistas em cibersegurança que o estudaram, um Estado-Nação está por trás, pela complexidade, investimento e acumulo de conhecimento necessários para desenvolver um software tão específico e bem elaborado.

> Embora os autores do Stuxnet não foram oficialmente identificados, o tamanho e sofisticação do *worm* levaram os especialistas a acreditarem que poderia ter sido criado apenas com o patrocínio de um Estado-Nação, e embora nenhum assumiu, vazou para a imprensa por meio de autoridades nos Estados Unidos e em Israel indícios que fortemente sugerem que esses dois países fizeram a ato. (KUSHNER, 2013, p.50, tradução nossa)

Stuxnet é um *rootkit*, um conjunto de softwares em um só, normalmente utilizado com más intenções. É a junção das palavras *root* e *kit*, raiz e conjunto respectivamente. Em computação, o termo raiz significa ter acesso privilegiado ao sistema operacional explorando falhas e executando processos anômalos do programado, o que o *stuxnet* fez muito bem. O *rootkit* foi projetado para ter acesso a componentes restritos do sistema operacional *Windows*, ocultando processos e integrando-se ao sistema de forma como se fosse parte dele, assim, não sendo detectado até mesmo por antivírus.

Nesse sentido, ele foi programado para atacar especificamente a instalação nuclear de Natanz, usada para enriquecimento de urânio, no Irã, que mesmo não sendo conectadas à internet foram infectadas com sucesso. O *software* desenhado tinha a característica de auto multiplicação quando um pendrive ou dispositivo móvel era conectado a uma máquina infectada, sendo essa a provável forma que conseguiu alcançar o sistema das instalações iranianas.

> Os sistemas autônomos ou que se comunicam por redes privadas podem receber um grau de proteção adicional por meio de medidas de segurança física e processual, pois o acesso ao sistema é necessário para realizar um ataque. No entanto, após a introdução do malware Stuxnet que foi programado para atingir o desempenho de

> enriquecimento de urânio do Irã na instalação nuclear de Natanz e pretendia causar danos físicos reais, desde então foi relatado ter afetado sistemas em uma usina nuclear russa e sistemas na Indonésia, Índia, Azerbaijão, Paquistão e Estados Unidos. Os sistemas afetados nas instalações de Natanz foram "bloqueados" e não conectados à Internet, mas, como costuma acontecer, o ponto mais fraco de segurança falhou e uma pessoa carregou o malware para as instalações, supostamente em um dispositivo USB. (JONES e KOVACICH, 2016, p.44, tradução nossa)

Após infectar o Windows, o próximo passo e alvo do stuxnet era o Sistema de Supervisão e Aquisição de Dados[12] (SCADA), da empresa alemã Siemens. Esse sistema monitora, controla e reporta eventuais erros do Controlador Lógico Programável (CLP)[13], que é muito comum em indústrias e controla processos repetitivos, como o tempo de duração do subir e descer de uma cancela de pedágio. O CLP controla as centrífugas da usina nuclear no Irã, fazendo-as girar na velocidade correta de forma automatizada, o *stuxnet* altera essa velocidade de rotação alterando a programação e como se apossou do sistema SCADA essa alteração não é reportada, o *stuxnet* reconfigura todo o sistema e mantém nos monitores como se a situação estivesse normal.

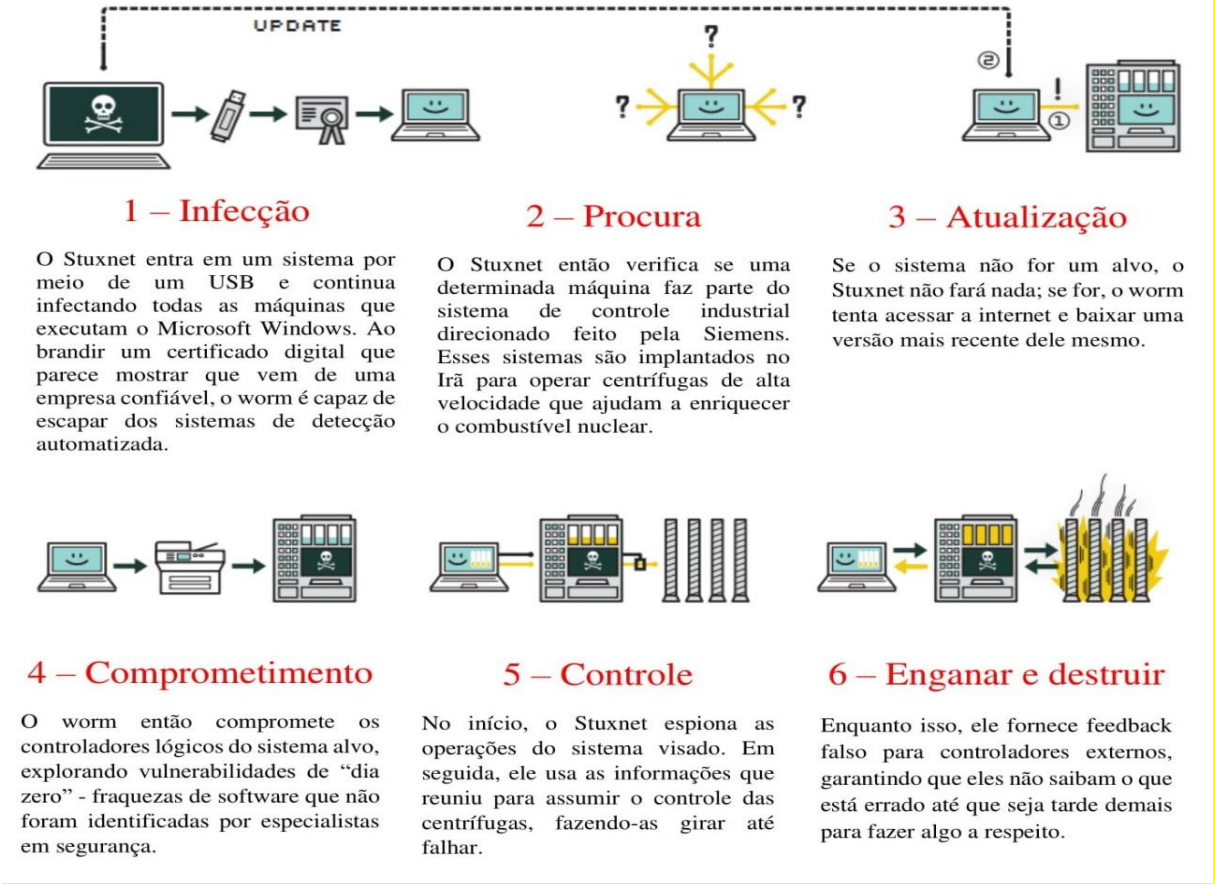
> Ao contrário da crença inicial, Stuxnet não era sobre espionagem industrial: não roubou, manipulou ou apagou informação. Em vez disso, o objetivo do Stuxnet era destruir fisicamente um alvo militar - não apenas metaforicamente, mas literalmente. Ele tinha como alvo apenas controladores de um fabricante específico (Siemens); ao encontrá-los (anexado a um caixa do Windows infectada via Ethernet, Profibus ou link de comunicação proprietário da Siemens chamado MPI), passou por um complexo processo de impressão digital para fazer certeza de que estava no alvo. Este processo incluiu a verificação de números de modelo, detalhes de configuração e até mesmo baixando o código do programa do controlador para verificar se foi o programa "certo". (LANGNER, 2011, p.49, tradução nossa)

O stuxnet entrava no sistema se passando por um processo legitimo e reprogramava as centrifugas para autodestruição fazendo-as girarem 40% mais rápido e sem reportar um alerta de erro. Felizmente, em junho de 2010, o vírus foi descoberto antes do desastre.

> Em junho de 2010, a Virusblokada, uma empresa de antivírus em Minsk, Bielorrússia, foi contratada por um cliente iraniano para investigar uma anomalia em um computador. Acreditava-se que a anomalia era uma falha, pois o computador estava se reinicializando continuamente. Sergey Ulasen, um analista da Virusblokada, acabou descobrindo o Stuxnet, e a empresa imediatamente notificou a comunidade internacional e começou a trabalhar para descobrir suas origens. Até agora, a Symantec Corporation, uma empresa americana de tecnologia, tem o relato mais detalhado do Stuxnet disponível ao público. Os relatórios indicaram que não apenas o Stuxnet destruiu 1.000 das 5.000 centrífugas na instalação nuclear do Irã, em Natanz, mas que também havia até 9.000 novas infecções diárias na usina nuclear de Bushehr, o que tornaria as centrífugas fora de controle e, em última instância, autodestrutivas. (KESHAVARZ, apud SPRINGER, 2017, p.282, tradução nossa)

[12] *Supervisory Control and Data Acquisition* (SCADA)
[13] *Programmable Logic Controller* (PLC)

Figura 6 - Representação dos passos do stuxnet.



Fonte: The real story of stuxnet, Revista IEEE Spectrum, vol. 50, p. 48-53, tradução nossa.

Além da construção sofisticada em cima dos exatos sistemas da usina nuclear iraniana, outo dado que corrobora com a hipótese que a arma foi criada especificamente para atacar o plano de enriquecimento de urânio em Natanz é a quantidade de infeções no país, desde o descobrimento do *stuxnet* e seu monitoramento, estima-se que mais de cem mil máquinas foram infectadas em todo mundo, destas, mais de sessenta mil estão localizadas no Irã.

Doravante a descoberta do *stuxnet*, uma questão preocupa especialistas em ciberdefesa, que é o acesso de criminosos a estrutura do *software*, pois, uma simples atualização de sistema não resolve o problema. A forma como foi construído e o que o stuxnet ataca implica em uma renovação do produto físico, o que gera muita preocupação, já que, os CPLs são usados em praticamente 100% das indústrias e infraestruturas críticas, como a rede elétrica e dutos de petróleo, como destaca Langner:

> As vulnerabilidades que eles exploram não podem ser corrigidas porque não são defeitos de software ou firmware, mas recursos legítimos do produto. Em outras palavras, essas vulnerabilidades estão aqui para ficar até que o fornecedor lance uma

> nova geração de produto e os proprietários de ativos substituam a base instalada por esses novos produtos antes do fim da vida útil programada, um cenário que levará muitos, muitos anos. Nesse período, os invasores podem usar as mesmas ogivas digitais novamente, já que usam uma nova falha e novas falhas são comparativamente fáceis de obter. As ogivas digitais, como tal, não podem ser desarmadas se conseguirem adentrar nos controladores. Os controladores industriais não têm software antivírus e as explorações do controlador que o stuxnet usa não podem ser "corrigidas". Elas são totalmente funcionais enquanto a geração atual do produto estiver em uso, o que pode levar mais 20 anos. (2011, p.50 e 51, tradução nossa)

3.3 DIRETIVA DE SEGURANÇA DE REDE E INFORMAÇÃO DA UNIÃO EUROPEIA (*NETWORK AND INFORMATION SECURITY DIRECTIVE*) – UMA LUZ NO FIM DO TÚNEL.

Se por um lado temos o Manual de Tallinn emergindo como um direcionamento do que é permitido ou não em uma eventual ciberguerra, por outro existem esforços para fortalecimento da cibersegurança e cooperação entre países para alcançar esse objetivo. Como exemplo, temos a Diretiva de Segurança de Rede e Informação da União Europeia, que estabelece uma cibersegurança coletiva visando a melhoria de "a) Capacidades de cibersegurança dos Estados Membros; b) a cooperação entre Estados-Membros; e c) Supervisão dos Estados Membros de setores críticos" (ZYGIEREWICZ, 2020, p.4, tradução nossa).

A diretiva entrou em vigor em 2016 e foi estruturada pensando em apresentar padrões para os países membros e dando prazo a esses para a implementação nos respectivos ordenamentos internos. Esse prazo foi de dois anos e posto no artigo 25 da diretiva.

> Os Estados-Membros adotam e publicam, até 9 de maio de 2018, as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva. Do facto informam imediatamente a Comissão. (Jornal Oficial da União Europeia, 2016, p.25)

Além do prazo para a implementação, ainda temos a previsão de os Estados-Membros identificarem os serviços essenciais que necessitam de maior proteção. E uma avaliação programada para 2021, com o fim de "revisar o funcionamento do diretiva, com um foco particular na cooperação estratégica e operacional, e o escopo em relação a OESs e DSPs[14]." (ZYGIEREWICZ, 2020, p.7, tradução nossa). A Diretiva é um marco em cooperação entre país na questão de cibersegurança, aumenta as capacidades defensivas de cada país, já que estipula a adoção nacional de segurança das redes seguindo a Diretiva, e também para administração de incidentes com equipes especializadas.

[14] Operators Providing Essential Services (Operadoras Que Fornecem Serviços Essenciais) e Digital Service Providers (Provedores de Serviços Digitais).

> 2. Para o efeito, a presente diretiva:
> a) Estabelece a obrigação de os Estados-Membros adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação;
> b) Cria um grupo de cooperação a fim de apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros e de desenvolver a confiança entre eles;
> c) Cria uma rede de equipas de resposta a incidentes de segurança informática (rede de CSIRT[15]) a fim de contribuir para o desenvolvimento da confiança entre os Estados-Membros e de promover uma cooperação operacional célere e eficaz;
> d) Estabelece requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais;
> e) Estabelece a obrigação de os Estados-Membros designarem as autoridades nacionais competentes, os pontos de contacto únicos e as CSIRT com atribuições relacionadas com a segurança das redes e dos sistemas de informação. (Jornal Oficial da União Europeia, 2016, p.11 e 12)

Como podemos perceber, a Diretiva não apenas impõe que os países da União Europeia criem legislações domésticas, mas, também, cria grupos especializados em cibersegurança, compartilhamento de informações e razoável tempo para a implementação e adaptação de cada nação às proposições da norma, além de prever avaliações periódicas da própria Diretiva. Mesmo que essa regulamentação se dê no contexto do bloco europeu, onde os países têm mais acesso à tecnologia, melhor infraestrutura e longa relação de cooperação, a Diretiva demonstra ser possível a colaboração para construir-se uma cibersegurança conjunta que proteja Estados e seus cidadãos, não ficando refém das dúvidas e danos de uma ciberguerra.

[15] Computer Security Incident Response Teams (Equipes de Resposta a Incidentes de Segurança de Computador).

CONSIDERAÇÕES FINAIS

A presente pesquisa expôs pontos que limitam a regulamentação de uma cibersegurança internacional, o que leva a uma desenfreada série de ciberataques entre Estados sem atribuição de responsabilidade. Buscou-se relatar o papel da soberania e suas dificuldades dentro do ciberespaço, bem como temos um manual de regulação de ciberguerra pronto.

Ao longo da história recente, notadamente no século XXI, a tecnologia da informação desenvolveu-se rapidamente a cada ano, a velocidade desse desenvolvimento não foi acompanhada pelo Direito, este que ainda carece de discussões aprofundadas e revisão de conceitos para se adequar ao ciberespaço e normatizá-lo. Nesse sentido, o ambiente cibernético, aparentemente, tornou-se uma "terra sem lei" onde mecanismos para a apuração de responsabilidades individuais e principalmente estatais ainda engatinham em seu desenvolvimento.

Sem uma regulamentação convincente, padrões de segurança e eficiente meios de investigação de reponsabilidade, o ciberespaço tem sido tomado por ciberoperações que atingem países como um todo. Esbarrando no conceito de soberania, um tratado internacional sobre cibersegurança parece estar longe ocorrer, ou simplesmente não é interesse de alguns países que isso aconteça. Percebe-se o movimento, com forte base na soberania, de tentativas de regulamentação de fatos ocorridos no ciberespaço apenas em âmbito nacional de cada nação, representando um contrassenso, já que o ambiente virtual se tornou algo mundial, não estando no controle de apenas um país exercendo soberania sobre o ciberespaço.

As dificuldades em estabelecer um nexo causal entre ciberataques e dano somado a enorme quantidade de ataques via ciberespaço, tornou propenso um ambiente de ciberguerra na arena internacional. Com isso, Estados dão ênfase a regulação de direitos individuais domesticamente, enquanto, seus atos ficam em uma lacuna normativa, onde a cibersegurança fica em um plano de cada um por si e não em um plano de proteção para todos. A forma como a globalização caminha contribui para esse cenário, ao passo que, empresas multinacionais detém grande parte das estruturas do ciberespaço, e este tem sido construído no interesse dessas empresas e não no interesse da coletividade. Os Estados de origem dessas instituições privadas precisam da cooperação e consumo de outros para terem lucros, mas o controle de como funciona as relações dentro do ciberespaço não é cooperativo, uma lógica falha, já que quem oferece os serviços dependem de quem os consomem, então, as regras de funcionamento também deveriam ser trabalhadas de forma conjunta.

Enquanto tal lógica não se adequa a realidade, armas cibernéticas como o *stuxnet* mostrado nesta pesquisa, serão cada vez mais comuns. Sem uma cibersegurança coordenada, ataques, como os contra a Estônia, podem ser mais intensificados. Discutir e estabelecer padrões de cibersegurança não se trata de aumentar o controle sobre os indivíduos, mas sim, estabelecer limites à atuação estatal e suas consequências, fortalecer todos de uma forma geral, aumentar a proteção aos direitos individuais dentro do ambiente virtual e com redução de custos para isso.

O contexto atual do ciberespaço assemelhasse com as discussões sobre o aquecimento global. Quando se alerta sobre o problema, a primeira onda de reações é dizer que não há problema. Aumentando as evidências, temos a admissão do problema, mas nega-se a participação humana nele. Por último, quando não há mais como negar o problema e a participação humana nele, trazemos a desculpa que fazer alguma coisa a respeito terá um custo alto para a economia e que alguns Estados terão maior prejuízo que outros. Esse pensamento leva a um posicionamento de resolver os problemas no curto prazo, e no lugar de falarmos em cibersegurança, surge o Manual de Tallinn com regras para uma ciberguerra. Mas assim como a redução do aquecimento global, estabelecer uma cibersegurança global seria um benefício para todos os Estados e seus indivíduos.

Apesar desse movimento de insegurança e propensão para uma guerra cibernética, o exemplo trazido pela Diretiva de Segurança de Rede e Informação da União Europeia, demonstra que uma cooperação bem ordenada torna possível progredir rumo a uma cibersegurança que projeta os cidadãos e ao mesmo tempo os interesses dos Estados.

REFERÊNCIAS

ACQUAVIVA, Marcus Cláudio. **Teoria Geral do Estado**. 3 ed. - Barueri, SP: Manole, 2010.

BONAVIDES, Paulo. **Ciência Política**. 18 ed. - São Paulo: Malheiros Editores, 2011.

BRANCO, P. G., & TALPAI, B. (2020). **A soberania e o ciberespaço: uma análise crítica do conceito de soberania e globalização**. JURIS - Revista Da Faculdade De Direito, 30(1), 43–62. Disponível em: https://doi.org/10.14295/juris.v30i1.11285. Acesso em: 16 mar. 2021.

BRASIL. Decreto n° 7.030 de 14 de dezembro de 2009. Promulga a Convenção de Viena sobre o Direito dos Tratados, concluída em 23 de maio de 1969, com reserva aos Artigos 25 e 66. **Diário Oficial da União**, Brasília, 15 dez. 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d7030.htm. Acessado em: 07 abr. 2021.

CAMARGO; SANTOS; GUTERRES, **Antropologia no ciberespaço: buscando compreender as experiências de deslocamento humano**. In: Revista Rosa dos Ventos, Programa de Mestrado em Turismo, Universidade de Caxias do Sul-RS, 2012.

CLARKE, A. R.; KANAKE, R. K., **Cyber War: the next threat to national security and what to do about it**. HarperCollins Publishers Ltd., London, 2010.

CYBER Security Report, **Check Point Software Security Report**. Check Point Research, 2021.

CYBER Attack Trends, **Check Point Cyber Attack trends: 2020 Mid-Year Report**. Check Point Research, 2020.

CYBER Threat Report, **Sonic Wall Cyber Threat Report 2021**, SonicWall Inc, 2021.

DALLARI, Dalmo de Abreu. **Elementos da teoria geral do Estado**. 32 ed. - São Paulo: Saraiva, 2013.

DIONÍSIO, Cátia S. Guerreiro. **A responsabilidade internacional dos Estados e operações cibernéticas**. Dissertação (mestrado) – Universidade de Lisboa, Faculdade de Direito, 2018.

DIRETIVA (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. **Jornal Oficial da União Europeia**, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=HU. Acesso: 30 de abril de 2021.

DODGE, M.; KITCHIN, R., **Mapping cyberspace**, Routledge, London, 2001.

FERNANDES, José Pedro Teixeira. **O direito internacional humanitário e a emergência da ciberguerra**. Revista de Direito Internacional, Brasília, jul/dez v.9, n.2, p.11-24, 2012.

GRAHAM, David E. **Cyber Threats and the Law of War**. Journal of National Security Law & Policy, Vol.4(1), p.87-102, August 13, 2010.

HAATAJA, Samuli. **The 2007 cyber-attacks against Estonia and international law on the use of force: an informational approach**. Law, Innovation and Technology, 2017.

INTERNATIONAL Law Commission, **Draft Articles on Responsibility of States for Internationally Wrongful Acts**, nov. de 2001. Disponível em: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Acesso em: 3 abr. 2021.

JONES, A; KOVACICH, G. L. **Global Information Warfare: the new digital battlefield**. Taylor & Francis Group: Boca Raton, 2016.

KASPERSKY, **Security Bulletin 2020: Statistics**, Kaspersky Lab, 2020.

KITTICHAISAREE, Kriangsak. **Public International Law of Cyberspace**. Springer, Switzerland, 2017.

KOSTOPOULOS, George K. **Cyberspace and cybersecurity**. 2ed.; Boca Raton, Florida: CRC Press, 2017.

KREMLING, J.; PARKER, A. M. S. **Cyberspace, cybersecurity, and Cybercrime**. 1 ed. Thousand Oaks: SAGE Publications, 2017.

KREMER, J. F.; MÜLLER, B. **Cyberspace and International Relations: theory, prospects and challenges**. Springer: Verlag Berlin Heidelberg, 2014.

KUSHNER, David. **The real story of stuxnet**. IEEE Spectrum, vol. 50, no. 3, p. 48-53, mar. 2013.

LANGNER, Ralph. **Stuxnet: Dissecting a Cyberwarfare Weapon**. The IEEE Security & Privacy, p.49-51, mai/jun, 2011.

LEWANDOWSKI, Enrique Ricardo. **Globalização, regionalização e soberania**. - São Paulo: Editora Juarez de Oliveira, 2004.

LIFF, Adam P. Cyberwar: **A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War**. Journal of Strategic Studies, Vol.35, n. 3, p.401-428, jun. 2012.

MAZZUOLI, Valerio de Oliveira. **Curso de Direito Internacional Público**. 9 ed. -São Paulo, Revista dos Tribunais, 2015.

MEHAN, Julie E., **Cyberwar, Cyberterror, Cybercrime and Cyberactivism: An in-depth guide to the role of security standards in the cybersecurity environment**. IT Governance Publishing, Cambridgeshire, 2014.

MUELLER, Milton L. **Against Sovereignty in Cyberspace**. International Studies Review, Vol.22, p.1-23, set. 2019. Disponível em: https://academic.oup.com/isr/advance-article-abstract/doi/10.1093/isr/viz044/5572338. Acessado em: 01 maio de 2021.

OLIVEIRA, Bruna Pinotti Garcia. **Evolução do direito informacional na internet: a histórica luta pelo direito de informação no direito internacional dos direitos humanos e sua continuidade na era da informatização**. Tese (Doutorado) – Programa de Pós-Graduação em Direito, Faculdade de Direito, Universidade de Brasília – UnB, Brasília, 2020.

PARKS, R.; DUGGAN, D. **Principles of Cyberwarfare**. Security & Privacy, IEEE, p.122-125, nov. 2011.

PORTELA, Paulo Henrique Gonçalves, **Direito Internacional Público e Privado, incluindo noções de direitos humanos e de direito comunitário**. 9 ed. – Salvador, JusPODIVM, 2017.

RELATÓRIO de criminologia virtual; **crime virtual: a próxima onda**. McAfee - Santa Clara, Califórnia, 2007.

REPORT, McAfee labs **Threats Report**, McAfee - Santa Clara, Califórnia,2019.

SILVA, Guilherme Carvalho da. **O ciberespaço como categoria geográfica**. Dissertação (Mestrado) Departamento de Geografia do Instituto de Ciências Humanas da Universidade de Brasília, Brasília: GEA/IH/UNB, 2013.

SCHIMITT, Michael N. **Tallinn Manual on the international law applicable to cyber warfare**. Cambridge University Press, 2013.

SCHIMITT, Michael N. **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**. Cambridge University Press, 2017.

SKLEROV, Matthew J. **Solving the dilema of states responses to cyberattacks: a justification for the use of active defenses Against states who neglect their duty to prevent**.

Dissertação (mestrado) The Judge Advocate General's School, United States Army, 201 Mil. L. Rev. 1, 2009.

SPRINGER, PAUL J. **Encyclopedia of Cyber Warfare**. ABC-CLIO, LLC: Santa Barbara, CA, 2017.

STIENNON, Richard. **A short history of cyber warfare**. In: GREEN, James A. (org.); Cyber Warfare: a multidisciplinary analysis. Routledge, Abingdon, 2015.

STRECK, L.L; MORAIS, J.L.B. **Ciência política e teoria geral do Estado**. 3 ed.- Porto Alegre: Livraria do Advogado, 2003.

OTAN – ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO. **Tratado do Atlântico Norte**. Washington D.C., 1949. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pt. Acesso em: 20 de abril de 2021.

VARELLA, Marcelo Dias, **Direito Internacional Público**. 8.ed. São Paulo: Saraiva Educação, 2019.

ZYGIEREWICZ, Anna. **Directive on security of network and information systems** (NIS Directive). European Parliamentary Research Service, 2020.