Grupo de Peritos Governamentais das Nações Unidas

As relações internacionais no uso de tecnologias da informação: Medidas cooperativas e políticas de segurança contra crimes cibernéticos

DIRETORES

Ana Carolina Rocha

Bryan Robson Azevedo

Miguel Scatolin Teixeira

DIRETORA-ASSISTENTE

Júlia Matos

Apresentação da mesa

Prezados delegados e delegadas, sejam bem vindos ao Grupo de Peritos Governamentais das Nações Unidas. Meu nome é Ana Carolina Rocha, tenho 17 anos e atualmente estou cursando o terceiro ano do técnico integrado em Edificações do CEFET-MG. Esta será minha 2° participação como diretora de um comitê do MOCS e acredito que este comitê irá proporcionar uma experiência incrível para todos.

Construir o comitê foi uma das experiências mais satisfatórias que tive em relação ao mundo das simulações. A temática diz sobre algo que sou apaixonada: a Internet e seus recursos. Além disso, por se tratar de um mecanismo que cada vez mais tem feito parte do cotidiano, é importante discutir sobre seus benefícios, limitações e perigos. Sendo assim, espero que todos vocês levem consigo os conhecimentos aqui contidos não só para a simulação em si, mas para toda vida. Gostaria de agradecer a todos que se empenham diariamente para fazer o evento acontecer da melhor forma possível e em especial ao Miguel, Bryan e Julia que integram a mesa deste comitê tão maravilhoso. Vejo vocês em breve!

Meus caros delegados, é um prazer recebe-los no Grupo de Peritos Governamentais das Nações Unidas. Meu nome é Bryan Robson, tenho 18 anos e estou no terceiro ano de Eletrônica do CEFET-MG. O MOCS é uma simulação muito querida para mim, e fico encantado por ser um dos seus Diretores pela segunda vez.

Projetar este comitê com um tema que tanto me interessa com certeza fez deste ano inesquecível para mim no mundo das simulações. Como a humanidade e a tecnologia irão trilhar seu caminho juntas é um assunto que tem intrigado pesquisadores, juristas e filósofos de todas as áreas, pois se torna cada vez mais necessário uma adaptação ética e racional para mudanças tão rápidas na forma de vida das pessoas. Perante a todas essas mudanças,

acredito ser a segurança cibernética uma das áreas que mais precisa de atenção imediata, pois a desinformação desse campo de conhecimento pode gerar danos severos. Por isso fico feliz em poder levar o debate deste assunto até vocês, e de ter tido a oportunidade de trabalhar com pessoas tão brilhantes e especiais como são as pessoas que compõe essa Mesa. Contudo, espero que todos se divirtam e possam aprender cada vez mais! Bom dia, boa tarde ou boa noite!

Olá, meu nome é Julia Matos e estou no segundo ano de química no CEFET. Essa será minha primeira participação compondo uma mesa diretora no MOCS, que foi onde eu tive meu primeiro contato com simulações, em 2017. Todo o processo, principalmente a criação do guia de estudos, foi um desafio para mim, mas que valeu a pena pelo resultado e aprendizado. Espero que os senhores delegados tenham uma experiência incrível no MOCS VIII e que desfrutem, da melhor forma possível, desse comitê que foi preparado com muito carinho. Vejo vocês em breve, até logo!

Bom dia, boa tarde ou boa noite!! Meu nome é Miguel Scatolin Teixeira, conhecido como Scat e outras variações do meu sobrenome, e sou formado no curso técnico integrado de eletrônica no CEFET-MG. Nasci em Santos, morei em muitos lugares diferentes e vivo em Belo Horizonte a 6 anos. Comecei a simular em 2015 no MOCS V, desde então me apaixonei pelo estudo e pela discussão da geopolítica e do direito internacional.

Acredito que as simulações no geral são uma grande oportunidade para o crescimento pessoal, o desenvolvimento do pensamento crítico e para abrir a mente para a pluralidade de pontos de vistas e posicionamentos. Gosto igualmente de todos os tipos de comitê e vejo em cada um deles a chance de aprender coisas novas.

Como alguém que pretende seguir na área de computação, esse é, sem dúvida, o tema que mais me interessou nesses anos de simulação e será um dos mais intrigantes de assistir e dirigir. Como diretor e como amante de

tecnologia, vocês podem contar comigo para sanar qualquer dúvida a respeito do tema e do evento.

Por ser um tema tão complexo, é de extrema importância que vocês pesquisem além do que se encontra neste guia de estudo, principalmente a respeito do posicionamento da sua delegação. Tenham uma ótima leitura e nos vemos no MOCS VIII!

Sumário

1. Introdução

O aprimoramento da tecnologia de informação, promovido pela Revolução Técnico-científico-informacional a partir da segunda metade do século XX, configurou-se como um grande avanço para as relações e para o desenvolvimento humano. A criação da internet, um sistema global de redes de computadores conectadas entre si, vem proporcionando a comunicação instantânea, o armazenamento de dados, entre outras funcionalidades importantes para a sociedade atual. Dessa maneira, surgiu o novo território sem fronteiras ou barreiras físicas, denominado como espaço cibernético.

Nos dias de hoje, é quase impossível viver sem estar em contato com a tecnologia de informação: ela está presente nas escolas, hospitais, parques industriais, controle aéreo, bancos, em nossas casas e é utilizada por diversos Estados. A globalização foi intensificada, tanto no que diz respeito à comunicação em tempo real e em escala multinacional, quanto no âmbito das relações comerciais.

A internet, embora tenha assegurado inúmeros benefícios à sociedade, não está livre de ameaças. Através de alguns cliques, é possível interromper o fornecimento de energia de um país inteiro ou transferir enormes quantias de dinheiro para diferentes locais, basta que tais informações caiam sobre as mãos erradas. Inúmeros criminosos aproveitam da grande disponibilidade de dados e falta de segurança do ambiente cibernético para cometer delitos que podem ter desde cunho financeiro, até objetivos políticos.

Os crimes cibernéticos configuram-se como uma nova ameaça a ser combatida em categoria nacional e global. Dessa forma, o termo segurança cibernética inevitavelmente vem à tona. A necessidade de se discutir a participação dos Estados e sua colaboração em conjunto para o enfrentamento dos criminosos e prevenção de delitos no ambiente informacional fez com que o Grupo de Peritos Governamentais das Nações Unidas se reunisse para buscar uma resolução para uma problemática tão ligada ao cotidiano do homem do século XXI.

2. O Grupo de Peritos Governamentais das Nações Unidas

No contexto da ascensão e da popularização da internet, começaram a ocorrer questionamentos com relação às ameaças presentes nessa nova tecnologia, não só no âmbito nacional, mas também internacional. Esse assunto foi primeiro citado em um esboço de projeto de resolução da 53ª Assembleia Geral, apresentado em 28 de Outubro de 1998 pelo representante da Federação Russa, tendo como principal foco o uso das tecnologias de comunicação por grupos terroristas, fazendo referência ao anexo A/51/261, referente às medidas para eliminar o terrorismo internacional.

2.1. Funcionamento, responsabilidades e capacidades

Para promover uma maior compreensão com relação ao assunto, foram formados ao longo dos anos Grupos de Peritos Governamentais, para estudar, discutir e com os resultados, orientar a Organização das Nações Unidas e seus Estados Membros. Esses Grupos caem sob a jurisdição do Primeiro Comitê da Assembleia Geral - Desarmamento e Segurança Internacional, sendo convocados pela Assembleia Geral segundo recomendação do primeiro.

O encargo do Grupo, assim como seu tamanho e número de sessões, são decididos em consultas e negociações no Primeiro Comitê, considerando aspectos orçamentários e políticos (UNIDIR, 2015, p.4). Os Grupos são formados com base no princípio de distribuição geográfica igualitária, estando presentes os membros permanentes do Conselho de Segurança (China, Estados Unidos da América, Federação Russa, França e Reino Unido da Grã Bretanha e Irlanda do Norte); as posições restantes são distribuídas de acordo com o agrupamento regional das Nações Unidas. O Gabinete para Desarmamento é o responsável por propor a composição ao Secretário Geral, levando em consideração, além do equilíbrio geográfico e político, o interesse

demonstrado pelos países no assunto. Alguns representantes são acompanhados por conselheiros, comumente especialistas em direito internacional.

Uma vez decididos os países, estes devem escolher seu Perito, normalmente oficiais de governo. Inicialmente os Grupos continham diversos especialistas em segurança de informação e com conhecimentos técnicos, mas agora são compostos principalmente por diplomatas, especialmente aqueles com experiência em desarmamento. Os peritos decidem um presidente para guiar as sessões e utilizam o encargo dado para definir o seu plano de trabalho e agenda. Estar sob a jurisdição do Comitê para Desarmamento e Segurança Internacional influencia no escopo das discussões, trazendo um foco para a desmilitarização das Tecnologias da Informação e Comunicação (TICs) e prevenção de conflitos.

Os Grupos trabalham de acordo com o formato das Nações Unidas, com discussões de seis horas por dia e tradução simultânea para as seis línguas oficiais (UNIDIR, 2015, p.5). As sessões são fechadas, sem presença da mídias ou de membros observadores.

Os Grupos de Peritos Governamentais operam por consenso, de modo que todas as decisões devem ser tomadas com o acordo de todos, inclusive o relatório final. Os relatórios têm um limite total de 10.700 palavras (ESCRITÓRIO DAS NAÇÕES UNIDAS EM GENEBRA, s.d., p.2) e não possuem caráter mandatório, servindo para prover sugestões e conselhos.

A resolução 70/273 da Assembleia Geral encarrega o quinto Grupo de Peritos Governamentais nos Desenvolvimentos na Área de Informação e Telecomunicações no Contexto da Segurança Internacional de

> […] continuar a estudar, com a visão de promover entendimentos em comum, potenciais e existentes ameaças na esfera da segurança da informação e possíveis medidas cooperativas para endereça-las e como o direito internacional se aplica ao uso de tecnologias de informação e telecomunicações por Estados, assim como normas, regras e princípios de comportamento responsável por

parte dos Estados, medidas de construção de confiança e capacidades [1][…] (Assembleia Geral das Nações Unidas, 2016, p.3)

2.2. Histórico

Até o momento houve quatro Grupos diferentes, ocorridos em 2004, 2009-2010, 2012-2013 e 2014-2015. Cada um desses grupos participou de três a quatro encontros de uma semana e todos, exceto o primeiro, atingiram consenso e redigiram relatórios apresentados à Assembleia Geral das Nações Unidas.

2.2.1. Primeiro Grupo

O primeiro Grupo de Peritos Governamentais nos Desenvolvimentos na Área de Informação e Telecomunicações no Contexto da Segurança Internacional foi recomendado pelo comitê de Desarmamento e Segurança Internacional no relatório 53/533 de 14 de Novembro de 2001 e convocado pela resolução 56/19 de 7 de Janeiro de 2002 da Assembleia Geral. Essa resolução requeria ao então Secretário Geral que conduzisse um estudo auxiliado pelo Grupo de Peritos, apontado por ele de acordo com a distribuição geográfica equitativa, e que apresentasse um relatório à Assembleia.

Esse Grupo foi formado por representantes de 15 Estados: África do Sul, Alemanha, Bielorrússia, Brasil, China, Estados Unidos da América, Federação Russa, França, Índia, Jordânia, Malásia, Mali, México, Reino Unido da Grã Bretanha e Irlanda do Norte e República da Coreia. Os representantes tiveram três encontros distintos em sedes da ONU e elegeram como presidente Andrey V. Krutskikh, da Rússia.

Durante os encontros deste primeiro estudo, os peritos não foram capazes de chegar a um relatório apoiado por todos. Os principais pontos de discordância foram quanto destaque deveria ser dado às ameaças digitais e se o grupo deveria discutir as informações em si ou somente a infraestrutura da

[1] "continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behavior of States, confidence-building measures and capacity-building"

tecnologia de informação. Outras discussões que não tiveram uma conclusão foram quanto à afirmação de que “informações transnacionais deveriam ser controladas pelos Estados como medida de segurança nacional” e ao apoio e compartilhamento de tecnologias de informação com países em desenvolvimento.

2.2.2. Segundo Grupo

O segundo Grupo manteve o número de 15 peritos; além dos cinco membros permanentes do Conselho de Segurança, participaram alguns outros países que também estavam presentes no Grupo anterior, sendo eles: África do Sul, Alemanha, Bielorrússia, Brasil, Índia e República da Coreia. Os novos países participantes foram: Catar, Estônia, Israel e Itália.

Os principais focos da discussão foram as ameaças, riscos e vulnerabilidades das tecnologias de informação e comunicação, sendo alguns pontos fundamentais: o crescente desenvolvimento técnico dos métodos utilizados para perpetuar atos criminosos na rede, o potencial que essas tecnologias possuem de serem explorados por grupos terroristas, o aumento da utilização de TICs por estados, a vulnerabilidade em infraestruturas internacionais essenciais criada pelo uso de serviços da internet, a disparidade de desenvolvimento técnico na segurança das novas ferramentas de comunicação entre os diversos países, e o consequente aumento da fragilidade da rede global como um todo.

Outro ponto destacado nas discussões e no relatório final foi o das medidas cooperativas internacionais com relação ao espaço digital internacional, sua importância e as consequências da falta desta. Alguns dos pontos destacados pelos peritos foram: a possibilidade de mal entendidos com relação às normas do uso das Tecnologias da Informação e Comunicação por parte dos Estados, derivados da discordância internacional e a imprescindibilidade da cooperação global frente ao crescimento em complexidade e escala de atividades disruptivas, com efeitos no ambiente digital internacional.

Para concluir o relatório e direcionar os países na Assembleia Geral, o grupo redigiu recomendações com relação às decisões a serem tomadas no assunto discutido. Em resumo, essas recomendações foram o aumento do dialogo internacional e troca de visões nacionais com relação ao uso de tecnologias da informação por Estados, debates com relação a legislações, tecnologias e estratégias de segurança informática nacionais, elaboração de termos e definições relevantes ao assunto e identificação de medidas para desenvolvimento de capacidades na área da telecomunicação em países em desenvolvimento.

2.2.3. Terceiro Grupo

Também com 15 peritos, participaram pela primeira vez do grupo representantes da Argentina, Austrália, Canadá, Egito, Indonésia e Japão, além de Alemanha, Bielorrússia, Estônia, Índia e dos Membros Permanentes. Esse fgrupo teve três encontros de uma semana, acontecidos em 2012 e 2013, e elegeu unanimemente a Sr.ª Deborah Stokes, representante da Austrália, para presidir as reuniões.

O relatório, apresentado na sexagésima oitava Assembleia Geral das Nações Unidas, reitera os pontos levantados pelo segundo grupo quanto ameaças, riscos e vulnerabilidades digitais de escala global. Segundo o Grupo, as Nações Unidas deveriam tomar um papel de liderança para viabilizar diálogos em relação à promoção de um senso comum quanto à segurança e ao uso de TICs (Assembleia Geral das Nações Unidas, 2013, p.7).

Os peritos compuseram diversas recomendações a respeito de normas, regras e princípios de comportamento responsável dos Estados no contexto da tecnologia de informação, seus usos em interesses nacionais e suas seguranças. Algumas das principais conclusões foram: a carta das Nações Unidas e o direito internacional são aplicáveis e essenciais para manter a paz e estabilidade no contexto digital; a soberania de um Estado se aplica à TICs e às suas infraestruturas; medidas visando segurança cibernética devem sempre se manter fiéis à Declaração Universal de Direitos Humanos; os Estados devem seguir suas obrigações com relação aos seus atos ilegais cometidos no

ciberespaço, não fazer uso de terceiros para cometer esses atos e nem permitir que seu território seja usado por agentes de qualquer natureza para este fim.

Em relação a ações práticas para desenvolver a segurança das Tecnologias da Informação e Comunicação, o Grupo indica uma troca expressiva e constante de informações e visões nacionais no assunto, comunicação entre agências de diferentes Estados em relação à técnicas e incidentes digitais e foco em iniciativas bilaterais, multilaterais e regionais de cooperação. Essas medidas, em conjunto com as contribuições do setor privado e da população civil, eventualmente construirão experiência prática e diretrizes bem estabelecidas para futuras ações.

2.2.4. Quarto Grupo

Este grupo foi composto por 20 peritos; participaram novamente do grupo representantes da Alemanha, Bielorrússia, Brasil, Egito, Estônia, Israel, Japão, Malásia, México, além de Colômbia, Espanha, Gana, Paquistão e Quênia, que integravam pela primeira vez, e dos Membros Permanentes. Nesse grupo o Sr. Carlos Luís Dantas Coutinho Perez, representante do Brasil, presidiu os quatro encontros ocorridos em 2014 e 2015.

Com relação às ameaças no ciberespaço, o Grupo reiterou diversos pontos dos relatórios anteriores e citou que diversos Estados estão desenvolvendo capacidades militares, usando Tecnologias da Informação e Comunicação, e a possibilidade do uso dessas capacidades para conflitos futuros está aumentando. Visando a paz e estabilidade internacional, foi recomendado que no caso de incidentes no ciberespaço, os Estados devem considerar o contexto, todas as informações disponíveis, a dificuldade de localizar responsáveis por ações online e a dimensão das consequências.

O Grupo reforçou a importância do respeito aos Direitos Humanos, tendo como base as resoluções do Conselho de Direitos Humanos (20/8 e 26/13) e da Assembleia Geral (68/167 e 69/166) quanto à proteção de direitos humanos e privacidade na internet. Também foram relembrados os princípios da humanidade, necessidade, proporcionalidade e distinção, essenciais para o direito internacional.

No relatório, apresentado na 70ª Assembleia Geral, o Grupo encoraja os Estados Membros a estabelecerem equipes de resposta a incidentes de cibersegurança ou incumbir essa tarefa a órgãos adequados e a estimular cooperação entre essas equipes. Também foi recomendado atender à pedidos de ajuda de outros Estados para mitigar ataques digitais direcionados a infraestruturas, principalmente em casos onde o ataque seja originado daquele que recebeu o pedido.

Os peritos indicaram como importante para futuros estudos, os conceitos relevantes para o uso de TICs pelos Estados.

3. A Evolução da tecnologia e seus impactos na vida social

3.1. Comunicação antes da internet

3.1.1. Contexto histórico

A internet desempenha atualmente um papel importante na vida de todas as pessoas, tanto que as novas gerações nem imaginam um mundo sem essa ferramenta. Porém, antes do seu surgimento, outros meios de comunicação eram utilizados para a conexão e comunicação entre pessoas. A invenção que foi o ponto inicial da tecnologia de informação com uso de eletricidade foi o telégrafo, equipamento patenteado pelo inventor Samuel Morse em 1837. Esse instrumento utilizava como base o código Morse, linguagem que usa pontos e traços para se comunicar, e que no telégrafo, usava pulsos elétricos intermitentes para representar esses caracteres. Essa foi a primeira tecnologia que promoveu a transmissão de dados de forma quase instantânea a longas distâncias.

Muitas modificações foram feitas até que o telégrafo mostrasse seu verdadeiro valor e assim atraísse maiores interesses relacionados ao seu uso.

Empresas e até mesmo o exército adotaram o equipamento que atendia de forma satisfatória seus interesses. No entanto, fraudes começaram a ocorrer nessa forma de comunicação, sendo que nem todos conheciam o código Morse, e dependiam de outra pessoa para fazer a tradução. Dessa forma, alguns países obrigaram as empresas telegráficas a manterem o histórico das mensagens, para que a polícia tivesse acesso às informações, caso fosse necessário para alguma investigação.

O uso do telégrafo perdurou durante muitos anos, até que falhas consideráveis relacionadas ao seu uso apareceram e novas tecnologias o deixaram obsoleto. Com a necessidade de um novo artefato técnico que fosse capaz de enviar mensagens entre dois pontos distantes utilizando apenas um fio, surgiu o telefone. Sobre a invenção do telefone, acredita-se que os cientistas inglês e americano, Alexander Graham Bell e Elisha Gray, exploraram a área telegráfica e descobriram, quase ao mesmo tempo, porém de maneiras diferentes, que uma enorme gama de tons sonoros poderia ser mandada de uma só vez usando o fio telegráfico. Os dois cientistas possuíam expectativas diferentes sobre a descoberta, porém Graham Bell se antecipou e ganhou a corrida na invenção.

Em 1874, Gray construiu um receptor com um diafragma vibrante de aço colocado na frente de um ímã. Bell e seu assistente, Thomas Watson, em 1875, construíram um dispositivo parecido, com uma membrana vibratória e uma mola, aquela sendo o transmissor e esta, o receptor. Mais uma vez, ele conseguiu maior prestígio com sua invenção e, apoiado pelo sucesso do invento na Exposição Centenária da Filadélfia, criou, com seu assistente, a Associação Telefônica Bell.

Depois disso, houve muitos aperfeiçoamentos técnicos envolvendo o telefone. Theodore Vail, um administrador profissional, desenvolveu a ideia de um “Sistema Nacional de Telefone”, destacando a importância da rede de comunicação – network. Assim, em 1878, entrou em operação o primeiro telefone mecanizado através de um quadro de distribuição. Com esse invento, o telefone poderia ser completamente explorado, visto que todo aparelho poderia ser conectado a qualquer outro, de forma a realizar a visão de Vail, o

que possibilitou que o usuário pudesse falar de lugar para lugar e estabelecer contatos sociais.

Alguns anos após o surgimento e desenvolvimento do telefone, o rádio apareceu como uma outra fonte de comunicação a distância. Tudo começou quando, em 1895, o estudante italiano Guglielmo Marconi conseguiu transmitir sinais em código Morse no jardim de sua casa, sem o uso de fios. Após a descoberta, ele se mudou com a família de Bolonha, na Itália, para a Inglaterra, onde ele pôde aperfeiçoar seu método de transmissão, chegando a milhas de distância. O sucesso desses experimentos rendeu-lhe o Prêmio Nobel de Física de 1909. O início do uso do rádio, de forma significativa, foi em 1920, com a inauguração da KDKA, de Pittsburgh, cidade da Pensilvânia nos EUA, que foi a primeira rádio comercial do mundo. Em contrapartida, o rádio não comercial, mantido com uma taxa recolhida pelos proprietários de receptores, estabeleceu-se na Inglaterra, em 1922, com o início das transmissões da BBC de Londres.

Embora todos saibam que Marconi foi o inventor desse meio de comunicação, o padre brasileiro Roberto Landell de Moura é reconhecido como um dos pioneiros de talento por ter demonstrado publicamente a viabilidade do uso das ondas hertzianas, ao transmitir sinais de áudio, em uma distância de oito quilômetros, da Avenida Paulista à colina de Santana em 1899. Desacreditado pelo governo brasileiro, o padre registrou diversas patentes no *US Patent Office*, no Estados Unidos.

3.1.2. Comunicação em tempos de guerra

No século XX o mundo vivia grandes conflitos por território e Nações. Em 1914, imerso nesse contexto, Francisco Ferdinando, herdeiro do trono austríaco, foi assassinado em Sarajevo, se tornando o estopim para a eclosão da Primeira Guerra Mundial, conhecida como a Grande Guerra. Naquele tempo, a comunicação utilizada não tinha a capacidade de transmitir informações de forma rápida e eficiente como a televisão e a internet fazem no mundo globalizado. Na Europa, por exemplo, a Alemanha e o Império Austro-

Húngaro sofriam pela falta de uma comunicação mútua que os impedia de saber os planos do exército.

Em seu livro Estratégias de Comunicação (Lisboa, 1990), Adriano Duarte Rodrigues, professor catedrático da Faculdade de Ciências da Comunicação da Universidade de Lisboa, salienta que a comunicação é peça fundamental para as guerras e que muitas armas, assim como instrumentos de comunicação, foram criados inicialmente para fins militares:

> Não existe técnica militar sem dispositivos de sideração mineralizadora do adversário. É por isso que o instrumental bélico é revelador da tecnologia moderna; [...] Não admira, por isso, que a fotografia, o cinema, o megafone, a telefonia, o telégrafo, a televisão tenham sido logo associados, desde os primeiros tempos ao campo militar. A história, senão a origem dos media, depende em grande parte da história das próprias armas.
>
> LISBOA, 1990

O maior avanço nesse âmbito foi nas comunicações sem fio, porque apesar de promoverem o compartilhamento de mensagens de forma instantânea entre comandantes e unidades designadas, os fios eram vulneráveis ao fogo da artilharia e poderiam ser cortados facilmente por outras patrulhas durante a noite, o que fazia com que equipes de reparo entrassem com uma grande frequência no campo de batalha. Dessa forma, os meios de comunicação que não dependiam de fios tiveram papel muito importante nesse período, principalmente pelo seu grande alcance.

O rádio teve destaque no uso militar das tecnologias de comunicação. Por proporcionar o contato instantâneo durante as batalhas, esse meio de comunicação ajudava na movimentação de tropas e na troca de informações entre as posições dos soldados no front. Com esse novo instrumento foi possível a instalação mais rápida das comunicações à alcances mais longos do que o telefone de campo conseguia chegar. Por ter grande potencial e ser de interesse dos envolvidos na guerra, melhorias ligadas ao rádio e investimento

em novas tecnologias com aplicabilidade em situações de conflitos e guerras foram contínuas durante e depois do período da Grande Guerra.

Uma outra forma de comunicação sem fio utilizada no mesmo contexto foi a tecnologia usada por aviões de reconhecimento e zeppelins (dirigíveis rígidos) no qual um compacto aparelho transmitia as informações e as condições de manobras do inimigo para a estação mais próxima, isso a 90km de distância no máximo, que era o limite da transmissão.

21 anos depois da Grande Guerra, eclodiu a Segunda Guerra Mundial e os nazistas souberam utilizar as tecnologias que vinham surgindo a seu favor, fortalecendo sua campanha a fim de atrair adeptos para seu movimento. O rádio e a televisão (criada alguns anos após o surgimento do rádio), foram os principais meios de comunicação utilizados por eles para transmitir os discursos de Hitler, o principal líder nazista. Até mesmo o cinema, visto hoje como meio de entretenimento, foi usado como forma de propaganda política na época.

Durante todo o período da Guerra, houve diversos avanços na área de telecomunicações. Mas apesar disso, algumas tecnologias já existentes continuam em uso ou continuaram por muito tempo. O grande exemplo disso é o rádio, que foi usado durante as duas guerras mundias como estratégia militar e hoje é utilizado como forma de entretenimento.

3.2. O Surgimento da Internet

Após a Segunda Guerra Mundial, os países tinham a necessidade de se reestruturar e isso fez com que a conquista tecnológica e geopolítica se tornasse a prioridade. Além disso, o capitalismo, sistema econômico e político vigente no período, entrou em declínio, o que fez com que ideologia marxista-leninista, que defendia a maior intervenção do Estado mediante a aplicação de um regime socialista comunista, se expandisse como uma nova esperança.

A chamada Guerra Fria se instaurou a medida que a influência da URSS (União das Repúblicas Socialistas Soviéticas), com um grande poder bélico, e seu novo sistema, contrário à política econômica e geopolítica dos Estados

Unidos, cresceu e se espalhou. Esse dualismo impactou todo o mundo, gerando uma bipolarização que culminou em uma guerra de caráter tecnológico e geopolítico, sem a ocorrência de conflitos diretos entre as duas potências da época.

Nesse contexto conflituoso, surgiu a internet (ou “rede”), ferramenta indispensável para grande parte da sociedade nos dias atuais. Com o intuito de conseguir uma forma de transmitir as mensagens com rapidez, flexibilidade, tolerância a erros, onde vários computadores pudessem operar individualmente sem interromper o fluxo das informações, criou-se uma rede de computadores (Um grupo de computadores com capacidade de comunicar entre si a distância) montada pela agência ARPA: Advanced Research Projects Agency. Essa agência foi formada em 1958 pelo Departamento de Defesa dos Estados Unidos para mobilizar recursos de pesquisa com o objetivo de alcançar superioridade tecnológica e militar em relação à União Soviética.

A ARPAnet foi iniciada para fins militares e começou operando em quatro computadores. No início, a intenção era conectar os mais importantes centros universitários dos EUA com o Pentágono, a fim de trocar informações com facilidade e eficiência que também poderia ser utilizada caso houvesse uma guerra nuclear. Dessa forma, pode-se perceber que a internet, que nessa época ainda não tinha essa denominação, tinha como principal propósito estabelecer uma rede sólida de transferência de informações de forma segura e confiável.

O nome internet, propriamente dito, surgiu muito tempo depois de sua criação, quando a tecnologia ARPAnet passou a ser usada para conectar universidades e laboratórios, algo que começou nos Estados Unidos e depois expandiu para outros países. Esse novo instrumento ficou durante duas décadas restrito ao ambiente acadêmico e científico até que em 1987 seu uso comercial foi liberado em seu país de origem. Alguns anos depois, a internet foi se tornando cada vez mais popular e várias empresas surgiram como provedoras do acesso à Internet nos EUA.

A criação da WEB (World Wide Web), em 1991, por Tim Berners-Lee em um laboratório chamado CERN na Suíça, impulsionou a Internet, ao criar uma

linguagem que serviu para interligar computadores do laboratório e outras instituições de pesquisa e possibilitar a exibição de documentos científicos de uma forma simples e fácil de acessar. Essa nova ferramenta surgiu fundamentada numa relação cliente-servidor, em que o servidor e o cliente, que são programas distintos e que trabalham separadamente, mantém uma conexão e troca de dados independente do lugar onde se encontram.

Hoje a internet faz parte da rotina de trabalho, estudo e da vida das pessoas em geral. Com isso, surgiu um maior interesse do governo e das empresas no uso dessa ferramenta, que foi integrada com diversas áreas do conhecimento. Isso possibilitou uma maior proximidade das pessoas pelo mundo.

Com esse crescimento da influência da internet no mundo, a descentralização dos serviços e a soberania dos países no acesso e controle de informações se tornou alvo de debate em nível internacional e surgiu a necessidade de criar medidas para viabilizar o uso adequado da internet. Dessa forma, surgiu uma série de organizações, com objetivos individuais específicos.

A IETF - Internet Engineering Task Force, Força-tarefa de Engenharia da Internet em português, um novo modelo de gerenciamento para a internet, surgiu com o objetivo de contribuir com o seu desenvolvimento por meio de um modelo de gestão cooperativa, baseada em consenso, envolvendo uma variedade de setores e indivíduos. Ele conta com diversos grupos de trabalhos para temas específicos que influenciam (ou que influenciarão) de alguma maneira o funcionamento da Internet. Outra organização que surgiu um pouco depois foi a Corporação da Internet para Nomes e Números Atribuídos (ICANN - Internet Corporation for Assigned Names and Numbers), que é ainda hoje a principal organização responsável pela distribuição dos endereços IP e dos nomes de domínio.

Em 21 de dezembro de 2001, a Assembleia Geral das Nações Unidas aprovou uma resolução que encorajava a contribuição de governos, setores privados e sociedade civil nos trabalhos de preparação de fóruns presenciais, e recomendava a ativa participação de todos os setores durante esses fóruns.

Um desses encontros foi a Cúpula Mundial sobre a Sociedade da Informação (WSIS - World Summit on the Information Society) que teve como resultado a criação de um grupo de trabalho, o WGIG, Grupo de Trabalho sobre Governança da Internet (Working Group on Internet Governance), que preparou o relatório a ser utilizado como base para as discussões no encontro seguinte, que foi feito para dar andamento aos aspectos práticos do Plano de Ação de Genebra, bem como buscar soluções nos diversos campos da Governança da Internet, nas formas de financiamento e implementação dos demais documentos.

Um fato marcante do segundo encontro foi o estabelecimento do Fórum de Governança da Internet (Internet Governance Forum - IGF), que se consolidaria por fim como um espaço de debates, mantendo o objetivo e o caráter da WSIS, sendo convocado anualmente pela Secretaria Geral das Nações Unidas.

O primeiro Fórum de Governança da Internet aconteceu em Atenas, de 30 de outubro a 2 de novembro de 2006. Quatro temas foram tratados em outros encontros que o antecederam, que foram se tornando os fundamentos do uso da internet:

● Abertura - Liberdade de expressão, livre fluxo de informação, ideias e conhecimento.

● Segurança - Criando credibilidade e confiabilidade de forma colaborativa, particularmente protegendo usuários dos spams, phishings e vírus, preservando a privacidade.

● Diversidade - Promovendo o multilinguismo, incluindo internacionalização de nomes de domínios e conteúdos locais.

● Acesso - Conectividade à Internet: política e custo, lidando com a disponibilidade e viabilidade financeira nas questões de inclusão do acesso à Internet, interoperabilidade e padrões abertos.

Em 2007, o encontro aconteceu no Rio de Janeiro e os temas principais foram acesso, diversidade, abertura, segurança, como no encontro anterior, e a

administração de recursos críticos da Internet, que trata dos aspectos técnicos e políticos envolvidos na manutenção da infraestrutura da Internet e não estava presente anteriormente. A terceira edição do Fórum de Governança da Internet aconteceu em Hyderabad, na Índia, entre os dias 3 e 6 de dezembro de 2008, com destaque para o tema Internet para todos. Colocando em prática a questão de inclusão, o IGF ofereceu uma contribuição prática, ao criar no início do mesmo ano um grupo de trabalho responsável por viabilizar que pessoas e organizações pudessem participar ativamente por meio de recursos na Internet. O evento foi integralmente transmitido em áudio e vídeo na rede e mais de 500 pessoas assistiram.

A cada novo encontro, o IGF buscou a implementação de novas discussões acompanhando as mudanças e diferentes abordagens do uso da internet. Com o surgimento das redes sociais e o aumento dos crimes no ambiente virtual, as reuniões foram tomando caminhos diversificados, porém sem deixar de discutir assuntos ligados à base dessa tecnologia que já eram discutidos desde sua primeira edição.

3.3. O Surgimento de Hackers

A infraestrutura da internet se espalhou pelo mundo para criar a moderna rede mundial de computadores existente atualmente. Ela atravessou os países ocidentais e tentou adentrar nos países em desenvolvimento, criando acesso global à informação e comunicação sem precedentes, mas também uma divisão digital no acesso a essa nova tecnologia. Foi apropriada por indivíduos e grupos do mundo inteiro e com todos os tipos de objetivos. O fato é que, com o passar do tempo, sua utilização foi se tornando cada vez mais abrangente e o seu emprego trouxe impactos enormes e principalmente consequências sociais.

O que trouxe maior força para a internet foi sua abertura, que resultou no seu desenvolvimento autônomo e na liberdade dos usuários, que com o tempo, tornaram-se produtores da tecnologia e “criadores” de toda rede. Qualquer pessoa com conhecimento técnico podia se ligar à Internet, e isso acarretou em uma série de aplicações nunca planejadas, que vão da criação do e-mail, das

salas de bate-papo, até chegar ao hipertexto (uma página com várias entradas, onde o internauta escolhe seu percurso pelos links). Os hackers surgiram nesse contexto de crescimento da internet.

O que é entendido como hacker pela maioria das pessoas é uma definição que se atribui a crackers: aqueles empenhados em quebrar códigos, penetrar sistemas ilegalmente ou criar caos no ambiente virtual. Os “crackers”, na realidade, são rejeitados pela cultura hacker, que é muito mais complexa e que possui um universo muito mais vasto. Segundo Eric Raymond (que se destaca como observador e membro da cultura hacker), a diferença entre as duas denominações é que hackers constroem coisas, e crackers as destroem. A cultura hacker dominante vê os crackers com receio, afinal eles denigrem a imagem de toda comunidade que é vista como irresponsável, principalmente pela mídia, que não faz essa distinção.

Em geral, Raymond defende que hackers são pessoas com um conhecimento amplo sobre computadores, que possuem habilidades ligadas a programação e acreditam na liberdade e na ajuda mútua voluntária. Por acreditarem nisso, resolvem problemas e constroem coisas.

Na cultura hacker, prestígio, reputação e estigma social estão ligados à relevância da doação feita à comunidade. Ou seja, os hackers desenvolvem programas, ou softwares, conjuntos de instruções em linguagens compreensíveis pelos computadores que utilizam o poder de processamento destes, informações do computador, da internet e inseridas pelo usuário para realizar uma tarefa desejada, e divulgam suas contribuições na expectativa de uma retribuição.

Segundo Castells (p.43, 2001), começa-se a ser um hacker a partir de um ímpeto individual de criar, independente do cenário dessa criação,

> É por isso que há hackers na academia, em escolas secundárias, em grandes empresas e nas margens da sociedade. Eles não dependem de instituições para sua existência intelectual, mas dependem, efetivamente, de sua comunidade autodefinida, construída em torno de redes de computadores.

A base dessa cultura é um sentimento comunitário existente entre os membros, que têm integração ativa na comunidade com costumes e princípios bem estruturados, mesmo que informalmente. O que define a identidade de cada um nesse espaço é o nome divulgado na Internet, pois as identidades reais são geralmente ocultas.

Acredita-se, muitas vezes, que a cultura dos hackers só possa se desenvolver sob as condições de uma sociedade pós-escassez, ou seja, por essa visão os hackers só atuam se tiverem suas necessidades básicas garantidas para poderem se dedicar inteiramente às criações intelectuais. Entretanto, em muitos países pobres, como em alguns da América Latina, os hackers existem justamente para criar soluções para os problemas que cercam sua própria realidade. Isso mostra que ser um hacker não está ligado ao ambiente de vivência ou às condições das pessoas ligadas a essa "rede". Essa é uma cultura que existe baseada, principalmente, na liberdade, cooperação e criatividade de todos os membros.

4. Os crimes cibernéticos, o ciberterrorismo e o ciberativismo

4.1. Conceitos introdutórios

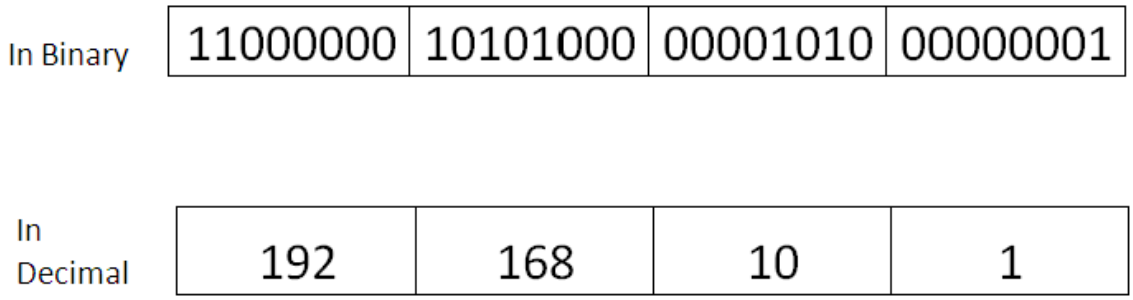
Existem vários tipos de criminosos e crimes cibernéticos. Porém, antes de aprofundarmos nos estudos dos crimes cibernéticos e do ciberterrorismo, é preciso conhecer alguns conceitos técnicos para entender o funcionamento básico da internet.

4.1.1. Nomes e números na rede

Entender como os computadores são identificados na Internet é requisito fundamental para entender como um ato criminoso nesse âmbito pode ocorrer. Todo computador na Internet possui um identificador único, que

conhecemos como endereço IP. O IP é a abreviação de “Internet Protocol”, ou “Protocolo de Internet” em português. De forma técnica, um endereço IP é um número inteiro de 32 bits (Bits é nome atribuído para os dígitos do sistema de numeração binário). Um bit é a menor unidade de informação que pode ser armazenada ou transmitida. O bit na computação é representado pelos valores 0 (zero) ou 1 (um), embora fisicamente seja uma carga elétrica abaixo ou acima de um nível padrão.

Figura 1 - Exemplo de endereço de IP



Fonte:

Apesar dos computadores trabalharem internamente com os bits, é inviável que este trabalho seja acompanhado por um ser humano, devido a quantidade de dígitos envolvidos. Dessa maneira, é feito a conversão do número para o sistema de numeração decimal, como mostrado na Figura X. Porém, essa não é a melhor forma de se representar um endereço de páginas na internet. É por esse fator e diversos outros que surgiu a necessidade de se atribuírem os números binários a nomes, que são muito mais próximos da linguagem de comunicação humana. Sendo assim, os resultados obtidos são endereços como “www.exemplo.com”.

4.1.2. Distribuição de endereços IP na Internet

A alocação de endereços IP’s na Internet deve ser realizada de forma muito bem organizada, pois é preciso garantir que cada um dos milhões de hosts seja unicamente identificado na rede mundial de computadores. Um host

é qualquer dispositivo conectado a uma rede. Em geral são computadores pessoais, servidores de rede e roteadores. Todo host na Internet possui um endereço IP único e público. Em outras palavras, não deve existir mais de um host compartilhando o mesmo endereço IP na Internet. Para este fim é adotado um modelo hierárquico, onde a organização americana denominada IANA "Internet Assigned Numbers Authority" ou Autoridade para Atribuição de Números da Internet, aparece no nível mais alto desta estrutura.

A IANA aloca grandes blocos de endereçamento IP para organizações conhecidas como RIR's, ou Registros Regionais de Internet, que por sua vez, alocam sub-blocos para os NIR's ou Registros Nacionais de Internet, para os LIR's ou Registros Locais de Internet, ou diretamente para grandes operadores de rede e provedores de acesso à Internet (também conhecidos por ISPs - Internet Service Providers). Os ISPs finalmente são os responsáveis pelo fornecimento de IP's para as residências, empresas e outras organizações menores, que no jargão técnico são referenciados como Sítios ou Usuários Finais.

4.1.3. Endereços IP públicos, privados ou reservados

O IP privado é o endereço utilizado para a identificação de um dispositivo dentro de uma rede que não são válidos na internet. Por outro lado, o IP público é para dispositivos acessíveis na internet. O endereço IP privado é feito para ser usado em redes privadas, como redes domésticas e de escritório. Eles são os mesmos endereços de IP públicos a nível de protocolo, no entanto, deferem organizacionalmente. Esses endereços só podem ser usados dentro de uma única administração, o que significa que eles não são utilizados na internet em geral.

Na maioria dos casos, os internautas não estão interessados em serem acessados. Portanto, é desnecessário possuírem um endereço IP público. Desta maneira, um único IP público fornece acesso a milhares de computadores com IP's privados à Internet.

Na prática, isso implica ao internauta encontrar dificuldades se quiser utilizar seu computador para hospedar algum conteúdo ou prover algum serviço na Internet e reduz a possibilidade de intrusões por outros internautas ao seu computador, uma vez que seu IP não é (imediatamente) alcançável na Internet. E para as autoridades em caso de investigação, implica encontrar dificuldades nas investigações, uma vez que a quebra de sigilo telemático de um único IP público pode abranger uma diversidade de clientes do provedor de acesso. Para contornar tal fato, o provedor deve armazenar os logs, ou registros, dos seus usuários, mapeando o endereço IP privado utilizado por cada cliente em cada conexão, de modo que seja possível localizá-lo posteriormente.

4.1.4. Buscando informações na rede através de um endereço IP

Existem bases de dados públicas que são mantidas pelas organizações que alocam endereçamentos IP citadas no tópico 4.1.2 (RIRs, NIRs, LIRs etc). Para este tipo de base de dados dá-se o nome de WHOIS. De uma maneira geral, as bases WHOIS fornecem informações de contato da pessoa (indivíduo ou corporação) responsável pelo registro de endereço IP na Internet. Ou seja, pode-se buscar nas bases WHOIS quem deve responder legalmente por uma ocorrência criminosa na rede.

4.2. Crimes cibernéticos

A definição do conceito de “Crime cibernético” ainda está em amplo debate por estudiosos da área do Direito Penal. De acordo com o jurista alemão Klaus Tiedemann, denomina-se “criminalidade informática” todas as formas de comportamento ilegal que venham a, de qualquer forma, provocar danos sociais, por intermédio de um computador. Porém, o doutor brasileiro em Direito Penal Marcelo Crespo adota o nome de “crimes digitais”, fundamentando sua nomenclatura no fato da informática ser uma das coisas ainda a serem reguladas, ou ainda porque a informática é um pressuposto de outro meio onde se cometem atos ilícitos, a telemática.

Conforme explicado pela jurista brasileira Ivette Senise Ferreira (2001, p. 208), não há um consenso acerca do conceito de crime cibernético entre os estudiosos porque:

> As várias possibilidades de ação criminosa na área informática, assim entendida em seu sentido lato, abrangendo todas as tecnologias da informação, do processamento e da transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais fornecem um denominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores.

Portanto, é perceptível que não há uma nomenclatura exata para os crimes cibernéticos. De toda forma, a diferença é apenas como os crimes são chamados por profissionais da área. Sendo assim, será tratado neste documento “Crimes cibernéticos” como sendo qualquer ato criminoso que seja usado dispositivos com capacidade de processamento (Computadores, Smartphones,etc) imersos em uma rede como ferramenta ou como vítima do ato em si.

4.2.1. O Direito Penal e os crimes cibernéticos

De acordo com advogado e teórico penal alemão Edmund Mezger (1946, p.27-28) define-se direito penal como: “O direito penal é o exercício do poder punitivo do Estado, que conecta ao delito, como pressuposto, e a pena, como consequência jurídica”.

A definição é correta, mas incompleta, visto que, além de definir crimes e cominar penas, o direito criminal estabelece os princípios e regras que regulam a atividade penal do Estado, fixando os fundamentos e os limites ao exercício do poder punitivo, a exemplo dos princípios de legalidade, irretroatividade, humanidade das penas, etc.

4.2.2. Bem jurídico no âmbito digital

Bem jurídico é toda coisa que pode ser objeto do Direito. Bem é tudo quanto pode ser valorizado pelo ser humano, mas em termos jurídicos, bens são os valores materiais ou imateriais que podem ser objeto de uma relação de direito próprio. São coisas úteis e de expressão econômica, suscetíveis de apropriação. De acordo com o jurista Francisco de Assis Toledo (1994, p. 16) define-se Bens jurídicos como:

> Bens jurídicos são valores éticos sociais que o Direito seleciona, com o objetivo de assegurar a paz social, e coloca sob a sua proteção para que não sejam expostos a perigo de ataque ou a lesões efetivas.

O bem jurídico na área da informática poderá ser diferente em relação aos bens jurídicos tutelados no Direito Penal tradicional, no entanto merecem proteção por esta área do direito se for um bem valioso para o indivíduo ao qual o bem pertence.

Assim, Crespo (2011, p. 56) afirma:

> A evolução grandiosa da informática estabeleceu um importante ponto de referência na história da comunicação e das relações sociais, buscando novas ideias no que tange a bens jurídicos, até mesmo influenciando nas classificações sobre os fatos que sejam crimes digitais.
>
> Ao considerarmos as condutas ilícitas por meio da informática, verificamos a possibilidade de lesão a outros bens jurídicos. Assim, pode-se falar em condutas dirigidas a atingir não só aqueles valores que já gozam de proteção jurídica, como a vida, a integridade física, o patrimônio, a fé pública, mas, também as informações armazenadas (dados), a segurança dos sistemas de redes informáticas ou de telecomunicações.

Seguindo o pensamento de Enrique Roriva Del Canto, Crespo afirma que o principal bem jurídico nos crimes digitais é a informação e de forma suplementar os dados ou os sistemas. Partindo do fato de que os dados são apenas a representação eletrônica ou digital da informação, mesmo que os valores variem, os sistemas são os mecanismos materiais de funções automáticas de armazenamento, tratamento e transferência.

É importante então, que seja observado qual o bem jurídico lesado, quando se está diante de um crime cometido pelo meio virtual ou contra os

dados e sistemas de dispositivos informáticos. Pois o objeto do crime pode ser a informação digital direta contida em dispositivos, ou o dispositivo pode ser uma ferramenta para alcançar um bem material físico.

4.3. Classificação dos crimes cibernéticos

Das condutas criminosas praticadas no espaço virtual podemos citar as mais frequentes:

• Crimes contra a honra: São os crimes de calúnia, difamação e injúria. Os criminosos são incentivados pelo anonimato e os crimes podem ocorrer em chats, blogs, pelo envio de spams, através de publicações em homepages, dentre outros meios de postagem eletrônica. Além das dificuldades de investigação inerentes à Internet, a polícia também esbarra na questão de territorialidade, pois se o site está hospedado em um provedor estrangeiro, de um país como os Estados Unidos da América, onde é totalmente livre qualquer tipo de manifestação de opinião, então não é possível exigir a retirada do site ou das mensagens, nem mesmo processar o autor do crime.

• Crimes contra a liberdade individual: São os crimes de ameaça, violação de correspondência, divulgação de segredos contidos ou não em sistemas de informação ou bancos de dados. O crime de violação de correspondência é um tipo plenamente aplicável a conduta de interceptação de e-mail, sendo a Internet uma evolução dos meios de comunicação, como a telegráfica, pois o bem jurídico que visa proteger é o sigilo das informações, a liberdade de comunicar-se e se expressar através de correspondência.

• Crimes contra o patrimônio: Compreende os crimes de furto, extorsão, dano e estelionato. O bem jurídico protegido nos tipos de furto e roubo é o patrimônio, então é desnecessária a criação de outro tipo penal somente para discriminar o meio de execução do delito que costuma ser através de manipulação de dados (fraude por manipulação

de um computador contra um sistema de processamento de dados) para modificação de depósitos bancários e obtenção de vantagem econômica ou a obtenção de dados como senhas para manipular contas bancárias e obter vantagem financeira. Para alguns juristas é necessária a criação de uma área específica para lidar com o que chamamos de furto virtual; dentre esses está o advogado criminalista Ramalho Terceiro, que coloca a problemática na diminuição do patrimônio, pois não haverá a diminuição do patrimônio da vítima se o criminoso somente copiar arquivos ou informação de banco de dados.

• Crimes contra os costumes: São os crimes de favorecimento à prostituição de escrito ou objeto obsceno e à pedofilia. É muito comum encontrar páginas (sites) de pornografia e de prostituição, aliás, é muito difícil fazer uma pesquisa em um site de busca, sobre qualquer tema, em que não apareça pelo menos um resultado indicando um link sobre pornografia.

Nos últimos anos se intensificou o movimento mundial contra a pedofilia, tendo a Convenção de Budapeste, também conhecida como Convenção sobre Crimes Virtuais, dando ênfase à proteção da criança e do adolescente.

• Lavagem de dinheiro no âmbito digital: A lavagem de dinheiro é uma expressão usada para referenciar o ato de práticas econômico-financeiras que têm por finalidade dissimular ou esconder a origem ilícita de determinados ativos financeiros ou bens patrimoniais, de forma a que tais patrimônios aparentem uma origem lícita que pelo menos, a origem ilícita seja difícil de provar. Com esse objetivo, muitos criminosos usam o ambiente virtual para cometer tais crimes. Como por exemplo, converter o dinheiro real em moedas virtuais que permitem fazer transações em anonimato, ou até mesmo utilizando jogos online, onde é possível converter dinheiro do mundo real em serviços ou bens que podem, mais tarde, ser convertidos de volta para o dinheiro real.

• Pirataria Digital: Pirataria digital é o ato de distribuir ou comercializar na internet obras das quais você não possui os direitos. A

pirataria acontece quando qualquer pessoa, não detentora dos direitos de distribuição e comercialização de uma obra, oferece uma cópia digital dela por meio de downloads gratuitos ou da venda desse material a um preço muito mais baixo. Nesses casos, tanto quem oferece o material tanto quem o adquire, tendo consciência da sua origem, está cometendo um crime e pode responder judicialmente por suas ações.

• Espionagem Digital: Também conhecida como ciberespionagem, é a prática de obter informações através do meio digital, de caráter secreto ou confidencial, sobre governos ou empresas sem sua autorização, para assim alcançar certa vantagem militar, política, econômica, tecnológica ou social. A prática manifesta-se geralmente como parte de um esforço organizado (ou seja, como ação de um grupo governamental ou empresarial).

• Falsidade ideológica: Consiste na utilização de identidade de um terceiro ou até mesmo fictícia, com o objetivo de cometer atos criminosos. De acordo com o código penal brasileiro, define-se: “Art. 307 – Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem”. No meio virtual aplica-se a mesma lógica. Falsidade ideológica se torna um crime cibernético a partir do momento que é feita através de um algum dispositivo digital ou na internet.

Além dos crimes citados, também podem ocorrer na Internet lesões a direitos humanos (terrorismo, crimes de ódio, racismo, etc.), destruição de informações, jogos ilegais, falsificação do selo ou sinal público, modificação ou alteração não autorizada de sistema de informação, violação de sigilo funcional, fraude em concorrência pública, dentre inúmeros outros.

4.4. O ciberterrorismo

O terrorismo corresponde a atos ou ataques contra alguma organização ou Estado que possuem como objetivo promover uma causa ou percepção de mundo através de um ato que cause terror ou desordem. Tal denominação teria surgido durante a Revolução Francesa, mais precisamente no intervalo

em que os jacobinos estiveram no poder, período que ficou conhecido como um período de “terror”. Ao longo de toda história, existem diversos casos de atitudes caracterizadas como terroristas, que tiveram como motivações diferentes causas que vão desde questões religiosas, à conflitos territoriais. Ao longo do século XX e XXI, incontáveis atentados foram relatados nos jornais todos os dias. Entre as principais estratégias utilizadas pelos criminosos, estão os ataques suicidas, que na maioria das vezes acabam por machucar e matar os inocentes que estão ao redor. Também se dedicam à depredação de monumentos históricos, cultural ou economicamente relevantes, e ao sequestro e até mesmo fuzilamento de inocentes. Entre os mais relevantes grupos terroristas das últimas décadas, podemos citar o Boko Haram, Estado islâmico, Talebã, Al-Qaeda (grupo responsável pelos ataques de 11 setembro), Hamas, IRA, ETA e as FARC. Conforme SAINT-PIERRE (1996, p.3) afirma, não é necessário o uso real de violência para aterrorizar:

> Os atos terroristas podem ser utilizados para fins políticos ou não, podendo também ter fins econômicos, religiosos, entre outros. Um fato interessante acerca do fenômeno é que não é preciso o uso real da violência para aterrorizar. Há casos em que só ameaça basta para chegar ao objetivo, por ser, muitas vezes, improvável determinar se é um blefe ou uma ameaça real.

Após os atentados de 11 de setembro, uma nova tipologia de crime cibernético teve suas bases estabelecidas e reconhecidas: o ciberterrorismo. Conquanto os ataques não fossem cibernéticos, os extremistas utilizaram a Internet para se prepararem para a investida contra o Estado americano. Uma grande discussão se iniciou a respeito do uso da tecnologia de informação pelos terroristas, que já não era novidade para os Estados. De acordo com a União Internacional das Telecomunicações (UIT), durante a década de 1990, os ataques tinham como objetivo prejudicar a infraestrutura de outros países e obter informações confidenciais. A grande maioria desses delitos, suas causas e efeitos, não foram relatados:

> Naquela época, o grau de interconexão era pequeno em comparação com os dias de hoje, e é muito provável que isso, além do interesse dos Estados em manter confidenciais os ataques bem-sucedidos - é uma das principais razões pelas quais muito poucos desses incidentes foram relatados. (UIT, 2011, p. 102)

4.4.1. O uso da Internet em ataques ciberterroristas

Hoje, sabe-se que os criminosos utilizam a tecnologia de informação e internet para promover propagandas, coletar informações, preparar ataques no mundo real e no próprio âmbito digital, para publicar material de treinamento e recrutamento, comunicação interna e externa ao grupo, financiamento dos ataques e atentados contra a infraestrutura básica de algum país (fornecimento de energia, água e gás, bancos, sistemas de transporte), entre outras utilizações.

Conforme a União Internacional de Telecomunicações explicita em 1998, apenas 12 das 30 organizações terroristas estrangeiras listadas pelo Departamento de Estado dos Estados Unidos mantiveram sites para informar o público sobre suas atividades. Os extremistas passaram a utilizar comunidades de compartilhamento de vídeos, como o Youtube, para enviar mensagens em escala global. Sites e fóruns também são amplamente empregados para divulgar a atividade terrorista, recrutar novos membros e divulgar vídeos de execução. Pode-se citar como exemplo a divulgação em janeiro de 2016 de um vídeo de cerca de 11 minutos, de autoria do ISIS, em que são executados cinco reféns. Ademais, além de exibirem a execução, discursavam a respeito de seus objetivos e motivos.

A comunicação por e-mail também é amplamente utilizada. No contexto do atentado de 11 de setembro, as investigações do Estado norte-americano apontaram que os membros da Al-Qaeda se comunicaram através do serviço de correio eletrônico e estabeleceram, por meio de diálogo virtual, quais seriam os alvos e o número de atacantes. A criptografia, técnica em que uma informação é codificada de maneira que apenas o receptor e emissor consigam

compreender a mensagem, permite que os transgressores se comuniquem de maneira anônima, dificultando a tradução.

As informações dispostas na Internet também são bastante visadas. Nos dias de hoje, é possível encontrar em rede, plantas e projetos arquitetônicos de diversos monumentos e edifícios, o que pode vir a facilitar a entrada dos extremistas nos locais onde desejam realizar um ataque suicida. Imagens de satélite em alta resolução, que no passado estavam somente disponíveis para instituições militares, atualmente podem ser facilmente localizadas. Informações confidenciais ou de grande importância sobre os Estados que não estão adequadamente protegidas podem ser acessadas através de simples mecanismos de pesquisa. Além disso, há instruções de como construir bombas e até mesmo treinamentos virtuais para o uso de armamento:

> Em 2008, os serviços secretos ocidentais descobriram um servidor de Internet que forneceu uma base para o intercâmbio de material de treinamento e comunicação. Diferentes sites foram informados por serem operados por organizações terroristas para coordenar atividades. (UIT, 2011, pag. 107)

A tecnologia de informação pode também ser aplicada na busca e determinação de perfis. Os dados dos usuários disponíveis em redes sociais permitem aos terroristas a identificarem pessoas que possam se simpatizar e aderir ao movimento, ou até mesmo solicitar contribuições para financiá-lo. Embora o contrabando de petróleo seja a grande fonte de renda, a maioria dessas organizações depende de doações e o rastreamento dessas transações apresenta-se como uma das maiores dificuldades para os Estados. Existem várias formas de como a arrecadação pode ser feita; uma delas pode ser citada a partir do exemplo da organização fundamentalista "Hizb al-Tahrir", que deseja unificar todos os países muçulmanos. A abordagem consistia em publicar, em um de seus sites, instruções sobre como doar dinheiro e os dados das contas bancárias destinadas às transações. Outra maneira, utilizada pelo IRA, grupo que intenciona a reunificação entre Irlanda e Irlanda do Norte, consiste em doações via cartão de crédito. Contudo, em ambos os casos, a possibilidade de rastreamento é maior.

Dessa forma, cada vez mais os terroristas estão buscando alternativas para mascarar a arrecadação. Utiliza-se de sites legais de doações, mas com

anúncios de instituições de caridade falsas ou corruptas (usuários podem estar doando pensando em contribuir para alguma causa de importância social, quando na verdade estão ajudando na fabricação e compra de material bélico). Uma opção que também pode ser utilizada é a criação de lojas virtuais falsas, que possuem como uma de suas vantagens a possibilidade de serem operadas em escala global. Comprovar que as compras na verdade configuram operações monetárias a fim de financiar o terrorismo é um dos grandes desafios enfrentados pelos investigadores, pois seria necessário observar cada transação, considerando que nem toda loja opera de maneira semelhante. Segundo o Instituto Europeu para Estudos em Segurança, essas contribuições podem ser feitas em bitcoin, para fugir do sistema bancário. As transações com as moedas digitais não revelam emissores e receptores, apenas as contas de origem e destino.

A vulnerabilidade e a emergente dependência da tecnologia da informação tornam necessários a prevenção e combate de atos terroristas no âmbito digital, pois o espaço virtual se tornou um novo alvo do terrorismo contra os Estados. A interrupção de serviços, como o fornecimento de energia, gás, água, bancos, sistemas de transporte e telecomunicações, entre outros, representam uma grande ameaça para a economia de um país, sendo vitais para a estabilidade e sustentabilidade. Logo, apresentam-se como alvos potenciais para os atentados.

> O ciberterrorismo tem suas vantagens, uma delas é “invisibilidade”, pois de imediato não se sabe realmente quem está do outro lado ou o que pode este realmente fazer (apesar das especulações), limitando assim, a defesa ou contra-ataque parte da vítima. [...] é, com certeza, uma opção atraente para terroristas tecnologicamente modernos que procuram anonimato e o potencial de infligir danos maciços, causar impacto psicológico e utilizar-se dos recursos de mídia. (CHAGAS, 2012, pag, 32)

Segundo CHAGAS (2012), o terrorismo cibernético apresenta-se como uma forma mais barata e rápida do que os métodos tradicionais (com uso de armamento e violência). É possível realizar ataques simultâneos e atingir alvos diversos localizados à longas distâncias, mantendo em anonimato a identidade do usuário. A inexistência de barreiras físicas como fronteiras e postos de fiscalização concedem aos criminosos maior liberdade de decisão sobre suas

ações. A facilidade de recrutamento e treinamento também contribui para que o ciberterrorismo ganhe cada vez mais atenção.

Devido à possibilidade de ataques aos Estados, a comunidade internacional cada vez mais tem se mobilizado em prol do aumento da segurança para evitar e parar ataques cibernéticos. A valorização do cooperativismo também reforça a luta contra o cibercrime. Através do direito internacional e da harmonização política, os governos nacionais devem dialogar entre si.

4.5. A navegação anônima e o ciberativismo

O espaço cibernético é vasto e não se resume a apenas as respostas que os buscadores mais comuns nos dão. O nível de acesso à informação não é o mesmo para todos os dados. Os resultados que encontramos à partir de uma busca no Google, Yahoo! ou Bing fazem parte da "superfície" da Internet, também conhecida como *Surface Web*, que de acordo com o pesquisador Denis Shestakov, representa apenas a "ponta do iceberg". A parte mais inacessível da Internet é conhecida como *Deep Web*. Nessa subcamada, é possível acessar sites que não estão catalogados por buscadores comuns e dessa forma encontrar a mais diversas informações que vão desde PDF's de livros universitários a conteúdos ilícitos.

O acesso é possibilitado a partir de redes que ocultam a identidade do usuário, como o TOR (abreviação de The Onion Route), a Freenet e I2P. Tais plataformas estão disponíveis para download na rede convencional e possibilitam que aqueles os utilizem não sejam localizados, tenham maior privacidade e proteção contra a censura.

Como apresenta uma maneira mais específica de ser acessada, a Deep Web oferece ao usuário maior privacidade e liberdade para utilizar a internet como quiser e ainda é capaz de promover o acesso anônimo ao conteúdo. Devido à tal particularidade, muitas pessoas e instituições utilizam a rede para armazenar e compartilhar arquivos que não podem estar na internet

convencional. Contudo, tem quem a utilize para fins pacíficos e aqueles que buscam disseminar pela rede, arquivos relacionados à pornografia infantil, tráfico de drogas e órgão, venda de armamento, encomenda de assassinatos e até mesmo conteúdo terrorista. Dessa forma, a mesa diretora do comitê não recomenda o acesso à rede em decorrência da possibilidade de se deparar com algum desses conteúdos, os quais podem ser desagradáveis e estimulam crimes do mundo real.

É importante ressaltar que alguns usuários querem apenas navegar anonimamente, sem intuito de promover tais crimes. Boa parte dos usuários são curiosos, que querem apenas ver o que existe por lá e ter a sensação de adentrar em um território da internet que é cercado de tabus, conforme dito pelo advogado e especialista em tecnologia e mídia Ronaldo Lemos. Ativista de grupos como o Wikileaks e Anonymous fazem uso da rede para divulgar informações sigilosas que são de interesse público e que na internet convencional provavelmente seriam censuradas. Em 2013, o ex-técnico da CIA, Edward Snowden divulgou, através de plataformas como essa, dados antes confidencias sobre o governo americano e seu programa de espionagem nacional e internacional.

4.5.1. O ciberativismo

O ativismo no espaço cibernético é um termo que pertence ao século XXI e que consiste na utilização da Internet por grupos politizados que divulgam informações ,sigilosas ou não, e reivindicam soluções para as questões sócio-políticas e econômicas. Entre as ações dos ciberativistas, podemos citar a promoção de petições, o compartilhamento através das redes sociais de campanhas sobre uma causa e o hacktivismo.

O autor Sandor Vegh no livro "Classifying forms of online activism: the case of cyberprotests against the World Bank", de 2003 cita três categorias de atuação do ativismo online: 1) conscientização e promoção de uma causa, por exemplo, divulgar o outro lado de uma notícia que possa ter afetado a causa ou uma organização; 2) organização e mobilização, convocar manifestações, fortalecer ou construir um público; e 3) ação e reação.

O ativismo hacker tem como um de seus objetivos divulgar informações sigilosas obtidas através da invasão de sistemas dos governos, instituições ou empresas que apresentem controvérsias, ou que sejam de relevância política. O interesse de cada um desses grupos ou legiões é variado e entre eles podemos citar a legião Anonymous e a organização Wikileaks.

4.5.2. O Wikileaks

Trata-se de uma organização transnacional criada em 2006 pelo jornalista e ciberativista australiano-equatoriano Julian Assange. Apesar de sua denominação, não se trata de uma “wiki” que pode ser editada pelos próprios leitores, como a Wikipédia. Seu nome e emblema fazem referência ao vazamento de informações secretas de empresas e Estados. A página tornou-se relevante nas buscas a partir de 25 de julho de 2010, quando liberou ao público 91 mil documentos secretos sobre a guerra no Afeganistão. Em entrevista ao jornalista Paul Marks, da New Scientist, Assange afirma que:

> O primeiro ingrediente da sociedade civil é direito do povo saber, porque sem essa compreensão, nenhum ser humano pode escolher para apoiar significativamente nada. O conhecimento é o condutor de todo processo político, todas as constituições, todas as leis e todos os regulamentos

Em 1997, Assange publicou em um livro sua filosofia de "hacker", de não prejudicar os sistemas de informática ao invadir, não modificar informações e sim, compartilhar os dados apurados. Além disso, a organização se compromete a não proteger os interesses de alguma Nação e afirma que não é preciso que os governos temam o Wikileaks, se forem sinceros com seu povo.

4.5.3. Anonymous

O Anonymous se auto-define como uma legião, isto é, um conjunto de pessoas que lutam pelo mesmo ideal, mas que não possuem líderes. O brasão da legião representa um homem de terno e gravata, que possui uma interrogação no lugar do rosto, o que remete à ideia de anonimato e à ausência de um dirigente. Seus membros constantemente aparecem em vídeos e manifestações, utilizando máscaras inspiradas no protagonista do filme “V de

Vingança". O lema do grupo é "Nós somos Anonymous. Somos uma legião. Nós não esquecemos. Nós não perdoamos. Esperem por nós".

O movimento surgiu em 2004 e tem como objetivos a luta contra a corrupção, a plena liberdade de expressão e a preservação de outros direitos, como a dignidade e a justiça. Segundo o site brasileiro da legião, seus participantes não estão ligados à partidos políticos, grupos religiosos ou ideologias quaisquer e se encontram espalhados por todo o mundo. Além disso, qualquer um que se interessar pode se juntar, anonimamente, e aderir à causa da legião.

Em 2015, o grupo declarou guerra ao Estado Islâmico após os ataques do grupo à sede do jornal Charlie Hebdo, que teriam como motivação a publicação de charges satíricas relacionadas ao islamismo. Em um vídeo publicado no Youtube, um membro do coletivo aparece dizendo que o grupo realizará cada vez mais ataques cibernéticos e colaborará para o desmonte do movimento jihadista. Segundo a revista "Foreign Policy", após os ataques o grupo conseguiu derrubar 149 sites ligados ao Estado Islâmico. Também foi divulgado uma lista com mais de 100 mil contas do Twitter relacionadas aos terroristas, além de mais de 5 mil vídeos.

O coletivo não realiza colaborações com as autoridades, salvo algumas exceções. Em operações contra a pedofilia, quando há alguma denúncia que possa levar alguém a ser preso, as informações podem ser cedidas à polícia. Contudo, não se trata de contribuir com a instituição, mas sim punir o indivíduo. Em uma entrevista ao site TECMUNDO, um membro do movimento cita:

> É bom lembrar que não somos prestadores de serviço. Queremos criar uma cultura de independência e emancipação, em oposição ao paternalismo do estado, dos partidos e de outras estruturas verticais. Queremos que as pessoas sejam livres. Inclusive, que sejam livres para questionar os próprios posicionamentos do Anonymous. (Anônimo, 2015)

5. Os criminosos na rede

Além de compreender os crimes cibernéticos, é preciso entender também os criminosos que cometem esses delitos. Ou seja, para uma investigação eficaz, ou mesmo para criação de medidas preventivas, é

necessário que haja um entendimento dos perfis de criminosos que atuam na área virtual. Sendo assim, podemos estabelecer os criminosos e as vítimas como sujeito ativo e sujeito passivo.

5.1.1. Sujeito ativo

Desta forma, para essa autora, o criminoso não precisa possuir habilidades e conhecimentos acima da média de informática para cometer crimes por meio da internet. Porém, de acordo com o jurista Túlio Lima (2011, p. 40), de todo modo, são os especialistas e os habilidosos operadores de computadores e sistemas, normalmente com idade abaixo da maioridade penal, que são os verdadeiros criminosos no âmbito virtual. Esses criminosos são denominados por muitos autores como hackers e crackers.

- Hackers: Os hackers são pessoas capazes de invadir ou modificar máquinas e sistemas virtuais. Eles usam seu conhecimento com o intuito de se promover, fazer testes de segurança para empresas ou mesmo para ajudar em investigações. Sendo assim, nem todo hacker pode ser considerado um criminoso, pois depende da forma e objetivo com que suas habilidades são utilizadas.

- Crackers: São considerados os verdadeiros criminosos da rede, sendo que utilizam do conhecimento que possuem para invadir sistemas, destruir sites, e ainda fazem da internet ferramenta importante para conseguirem roubar bens e informações.

Uma pessoa que comete um crime cibernético pode fazê-lo por motivos individualistas ou por motivos ideológicos. Os criminosos individualistas buscam no crime cibernético uma aquisição financeira (roubos, vendas ilegais, etc.) ou satisfação de um prazer pessoal (difamação, pornografia infantil, falsidade ideológica, etc.) e normalmente agem sozinhos ou em pequenos grupos. No entanto, os criminosos que agem por uma ideologia buscam através dos crimes cibernéticos uma forma de manifestação (Corromper sites de empresas, alterar dados de um sistema, vazar informações, etc.) e podem

atuar tanto sozinhos, quanto em grandes grupos ao redor do mundo que são adeptos a um mesmo ideal. Essas categorias não são exatas, podendo ter facilmente uma conexão entre elas.

5.1.2. Sujeito passivo

Podemos definir que os sujeito passivos, ou a vítima dos crimes de computador, são aquelas sobre as quais recai a conduta criminosa omissiva ou comissiva do sujeito ativo, e em relação aos crimes informáticos. As vítimas podem ser indivíduos, instituições de créditos, bancos e governos. Muitas das vezes as vítimas são associadas a uma ignorância na área da informática, o que não é verdade. Qualquer indivíduo ou corporação podem ser vítimas de um crime cibernético, independente do seu conhecimento ou segurança virtual.

No caso de empresas ou Estados, em muitos casos os ataques sofridos são omitidos com o propósito de não demonstrar fraqueza ou falhas de segurança em seu sistema, para não prejudicar seu nome. A segurança cibernética hoje se tornou um símbolo de respeito a instituições, como dito por Vladimir Aras (2002, p. 122):

> […] qualquer profissional que pretenda ser bem-sucedido, qualquer empresa ou empreendimento que busque o êxito, deverá estar na rede e cercar-se de conhecimentos e especialistas em diversos campos, a fim de que se tornem visíveis e alcançáveis os horizontes desse mar cibernético.

5.2. Ciberespaço

Uma das principais diferenças entre um criminoso padrão e um criminoso virtual é o meio em que os dois agem. A exposição do criminoso virtual ao cometer um crime na internet é muito menor do que um crime cometido em território físico. Essa diferença entre o espaço físico e o espaço virtual é essencial para entender o porquê dos crimes cibernéticos estarem cada vez mais chamativos e trazendo consigo um aumento de criminosos. Esse espaço abstrato onde ocorrem os crimes cibernéticos é denominado Ciberespaço.

Explica o pesquisador Paulo Kaminski (2000, p. 40), o que é ciberespaço tendo como base a definição da Unesco:

> [...] o ciberespaço é um novo ambiente humano e tecnológico de expressão, informação e transações econômicas. Consiste em pessoas de todos os países, de todas as culturas e linguagens, de todas as idades e profissões fornecendo e requisitando informações; uma rede mundial de computadores interconectada pela infraestrutura, de telecomunicações que permite à informação em trânsito ser processada e transmitida digitalmente.

O ciberespaço permite àqueles que estejam inclusos neste ambiente a liberdade de trafegar internacionalmente e ter acesso a dados remotos, ficando usuários e máquinas em lugares distintos. É importante destacar que, o ciberespaço não é uma coisa que sai do poder da jurisdição do mundo real. Usuários de computadores, sistemas provedores, conexões em rede e centrais de dados podem encontrar-se reunidos todos no mesmo país, e assim, pertencerem a uma mesma jurisdição.

O fato de que alguns componentes presentes no ciberespaço, que se encontram no mesmo país e podem fazer parte de uma mesma jurisdição, é explicada por Corrêa (2002, p. 72) da seguinte forma:

> A questão reside no fato de a Internet residir em um grande número de jurisdições diferentes. Surgem duas grandes controvérsias: a primeira diz respeito à efetiva responsabilidade de determinado país por determinado crime, e a segunda à competência do poder de polícia para dirimir eventuais problemas.

Sendo assim, com o surgimento do meio ambiente virtual surgem questões obscuras no que tange à aplicação da lei penal no tempo e no espaço; isso ocorre pelo fato de ter uma definição de território diferente estabelecido pelo Código Penal. Neste sentido, são as palavras de Crespo (2011, p. 117) que explicam:

> Justamente o surgimento do denominado “mundo virtual” ou “ciberespaço”, apresentando novas concepções de tempo e espaço, gerou empecilhos à correta aplicação da lei penal, vez que a tradicional concepção de território (como espaço físico) ganha outra denotação, qual seja, a de espaço virtual, ambiente onde há transcendência dos limites territoriais físicos.

Assim, não sendo o ciberespaço de fato um território, se caracteriza especificamente pelo fluxo de informações por intermédio de redes de

comunicação. Com isso, o que fica importante é a localização da informação, sendo esta a indicadora do território; é preciso considerar ainda que em diversos casos, os crimes realizados nesse “ambiente virtual” tem caráter transnacional, fato esse que vem a exigir dos países maior compromisso para combater esse tipo de criminalidade.

Essa característica do Ciberespaço e as complicações na legislação são o que mais atrai os criminosos virtuais. Dessa maneira, países devem trabalhar juntos para desenvolver e criar medidas para acabar com essas brechas, para aplicação das leis e para evitar que mais pessoas se interessem nesses crimes, pela grande chance de saírem impunes. As ação internacionais contra os crimes cibernéticos e o ciberterrorismo serão abordados mais à frente.

6. O Estado e os crimes cibernéticos

6.1. Jurisdição

Antigamente, as pessoas resolviam os conflitos entre si dentro da sociedade por meio do exercício de sua própria justiça. É a chamada “autotutela”, que fazia parte da vida de muitos, e ainda hoje pode ser observada. A autotutela acontece quando as pessoas agem por conta própria, exercendo sua justiça, ao invés de pedir ajuda de quem de fato possui prerrogativa para resolver conflitos, o Estado-Juiz. A vida no meio social gera conflitos que muitas vezes não é possível de serem evitados e na maior parte, esses conflitos são resolvidos pelas próprias pessoas que estão envolvidas, seja por negociações diplomáticas ou violentas.

Acontece que a autotutela está proibida, exceto quando em legítima defesa ou estado de necessidade. Fora a casos específicos, o Estado deve intervir nos conflitos da sociedade para seguir o propósito pelo qual foi criado: trazer ordem e paz para o meio social.

Temos que a jurisdição surge como uma necessidade do Direito, com o objetivo de impedir que a “autodefesa”, cheia de excessos e sem limites, conduza a sociedade a uma desordem grandiosa e ao mesmo tempo, como

uma garantia da liberdade perante o autoritarismo da força bruta. É verdade, que a autotutela ainda existe, mas de forma rigorosa dentro dos limites que não podem ser violados. Para o jurista Guilherme Nucci, pode se definir jurisdição como: “o poder atribuído constitucionalmente ao Estado para aplicar a lei ao caso concreto, compondo litígios e resolvendo conflitos”. (2013, p. 258)

Essa interferência do Estado para a aplicação da lei é feita através da figura de um Juiz pela competência que lhe cabe. No entanto, como a interferência ocorre depende do país ao qual o Estado pertence e até mesmo a regiões dentro de um mesmo território.

6.2. Conceito de competência

Para o jurista Fernando Capez, define-se competência como “a medida e o limite da jurisdição, dentro dos quais o órgão judicial poderá dizer o direito”. Ou seja, apesar da jurisdição ser uma só, como poder de soberania que o Estado possui, é evidente que não pode ser exercida por um só juiz sem ter limites. Se a área do Estado fosse escassa e a quantidade de pessoas pequena, da mesma forma como acontece com pequenos munícipios, um ou dois juízes podem ser suficientes para resolver os conflitos que existam ali. Porém, em grandes áreas isso não é o ideal.

É claro que somente um juiz não possui condições físicas e materiais de julgar todas as causas e diante disso, a lei distribui a jurisdição por vários órgãos do Poder Judiciário. Assim, cada órgão imbuído de jurisdição só poderá aplicar o direito se estiver dentro dos limites que lhe foram dados nessa distribuição. Ou seja, sua competência.

6.3. Competência nos crimes cibernéticos

O ambiente virtual permite a observação de certo “anonimato” daquele que visa praticar crimes neste meio, considerando o fato de que uma pessoa poderá executar um crime de um computador que esteja num endereço qualquer em um território nacional, mas isso não pode determinar que a

pessoa que for encontrada neste lugar é a mesma que usou esse dispositivo para cometer o delito.

É importante mencionar ainda que os crimes efetuados no âmbito virtual poderão atingir várias cidades de um mesmo território e até mesmo ultrapassar seus limites internos, atingindo outras Nações, criando a necessidade de colaboração de todos os países atingidos pela prática delituosa, para que efetivamente seja possível punir o criminoso.

É necessário para uma boa interpretação sobre a competência de julgamento dos crimes cibernéticos, entender primeiramente qual o lugar que está sendo considerado para fins jurídicos, por exemplo, o local onde são cometidos tais crimes. Já que os crimes são capazes de ultrapassar os limites territoriais do país de origem, é importante verificar qual o tempo de realização desse tipo de crime.

Assim, a Soberania dos Estados estabelece que sejam aplicadas suas leis em todo o território, que é considerado como: superfície terrestre, espaço aéreo e águas dos territórios. Porém, as leis de um Estado não podem interferir na soberania de outro Estado, mesmo se o crime possuir consequências em ambos os países.

A aplicação da Lei penal no espaço tradicional segue de acordo com a doutrina de cinco princípios, que são: princípios da territorialidade, nacionalidade, proteção, da representação e da justiça universal.

De forma breve, Castro explana sobre cada um desses princípios, conforme mostrado abaixo:

A lei penal no espaço é regida pelos seguintes princípios:

- Princípio da Territorialidade, através do qual aplica-se a lei do Estado aos fatos ocorridos dentro do território nacional.

- Princípio da Nacionalidade, no qual a lei do Estado é aplicável aos seus cidadãos onde quer que esteja.

• Princípio da Defesa, no qual a lei do Estado é aplicável em razão da nacionalidade do bem jurídico tutelado.

• Princípio da Justiça Penal Universal, no qual a lei do Estado é aplicável a qualquer crime, independentemente da nacionalidade do agente, do bem jurídico lesado e do local do fato.

• Princípio da Representação, no qual a lei do Estado é aplicável em aeronaves e embarcações privadas, quando realizado o crime no estrangeiro.

Apesar de as condutas efetuadas por meio da internet não possuírem um território físico certo ou uma nacionalidade que não está conceituada no ciberespaço, é verdade que o agente possui uma personalidade existente de fato, que ultrapassa aquela utilizada no mundo virtual e produz resultados no mundo real.

Olhando de uma forma prática, uma pessoa que vive no Brasil pode alterar dados que estejam guardados na Itália, deslocando-os para a Alemanha, visando obter vantagem ilícita, do mesmo modo que um vírus pode ser criado por um país e espalhado para milhares de computadores pelo mundo. A transmissão de dados pode incluir vários países, de tal forma que o lugar do crime seja definido de forma quase aleatória.

Existem três teorias para explicar a questão do lugar do crime, conforme as palavras de Capez:

1. Teoria da atividade, onde o lugar do crime é o da ação ou omissão, sem ter importância o local onde ocorreu o resultado.

2. Teoria do resultado, onde o lugar do crime é o que se configurou o resultado, sem ter importância o lugar da conduta.

3. Teoria da ubiquidade ou mista, em que o lugar do crime pode ser tanto o local do crime como o do resultado. Desta forma, onde se deu qualquer momento do *iter criminis* (sucessão dos vários atos que devem ser praticados pelo criminoso para atingir o fim desejado).

Fica claro assim a dificuldade de julgar um criminoso cibernético, pois a competência estabelecida ao poder judiciário pode variar conforme a teoria de local do crime que cada Estado admite. Portanto, na maioria dos casos, os países se unem com o intuito de estabelecer legislações parecidas em relação ao ciberespaço e assim conseguir que a justiça seja aplicada.

7. As relações internacionais no combate ao crime cibernético

7.1. Das dificuldades para a cooperação entre os países no combate ao cibercrime

Uma das características relacionadas à segurança cibernética que complica a sua discussão no contexto internacional é a variedade de ações maliciosas cibernéticas. A definição e discussão dessas ações são importantes para definir as normas de comportamento responsável dos Estados, estabelecendo as respostas adequadas a diferentes ofensas no ambiente digital, por parte dos países e também da comunidade internacional

No momento, existe certo consenso, apesar de não existirem tratados ou normas oficialmente reconhecidas pela comunidade internacional, a respeito da prática de Denial of Service (Negação de Serviço), que procura derrubar ou tornar lento um serviço ou site através da sobrecarga do mesmo. Esses ataques não são considerados ataques, mas sim uma forma incômoda e espalhafatosa de protestos online.

Os ataques que já são considerados como “uso de força” ou “ataque armado”, de acordo com a Carta das Nações Unidas, são aqueles que causam dano físico, destruindo infraestruturas e muitas vezes causando mortes. O grande desafio dessa discussão é definir, segundo o direito, as ações que ficam no meio do espectro, como a invasão de sistemas com o objetivo de obter ou destruir informações.

Outra complicação das relações internacionais no ciberespaço surgiu de uma compreensão equivocada de que a internet é um bem global, sem fronteiras e fora da influência das soberanias nacionais, uma ideia que surgiu nos princípios de tecnologia, devido à facilidade e velocidade de conexão com outros países. Essa percepção diminuíam e tornavam confusas as responsabilidades dos Estados com relação à proteção das infraestruturas, segurança e aplicação da lei nesse novo espaço.

Diversas ações diplomáticas e legais relacionadas a incidentes cibernéticos dependem da identificação dos responsáveis. Algumas companhias privadas e poucos países possuem certa capacidade para localizar, através de investigação forense e inteligências nacionais, os responsáveis atos maliciosos, sua localização e o destino de informações roubadas, quando é o caso.

O reconhecimento da aplicação da soberania e consequentemente, das leis nacionais e compromissos internacionais, e da responsabilidade por ações realizadas pelos Estados, por seus cidadãos ou em seu território no ciberespaço, cresce internacionalmente. O foco dos debates passa a ser o escopo da soberania, a aplicação de leis nacionais em casos que envolvam o território cibernético de mais de um Estado e é o equilíbrio entre soberania nacional e valores internacionais.

8. Perguntas a serem respondidas

- Até que ponto o Estado pode regulamentar o espaço cibernético sem que inflija princípios como a liberdade de expressão?
- Quais medidas podem ser tomadas para estimular a criação de leis nacionais contra o crime cibernético?
- Como desenvolver e estabelecer uma base internacional para os planos de segurança cibernética?

- Como diminuir a presença, financiamento e recrutamento de grupos terroristas no ciberespaço?

- Como expandir e fortalecer a cooperação entre os Estados para investigar e combater ataques cibernéticos?

- Qual a responsabilidade dos Estados em relação aos atos de autoria não estatais contra a infraestrutura cibernética de outros países?

9. Representações

9.1. Alemanha

Alemanha ou República Federal da Alemanha é um país situado na Europa e é um dos mais importantes países do mundo, em decorrência do elevado PIB e do desenvolvimento econômico, tecnológico, militar e qualidade de vida.

As primeiras formas de responsabilização penal pelos delitos tecnológicos no país se deram em meados da década de 1980 e as leis surgiram aos poucos, pois a conduta delituosa em crimes informáticos não possuía grande relevância, devido à sua pequena incidência.

Atualmente, a Alemanha é um grande alvo de ataques cibernéticos e no seu Código Penal, são várias seções que estão ligadas aos cibercrimes, ou que se relacionam a esse. No dia 20 de setembro de 2006 foi criado um projeto de lei visando acabar com as lacunas ainda existentes no âmbito do cibercrime, que abordou as seções como espionagem, fraudes em computadores, manipulação de dados, sabotagem de computadores, formação de organizações terroristas, incitamento de ódio, entre outras.

9.2. Austrália

Localizada na Oceania, a Austrália possui o segundo maior Índice de Desenvolvimento Humano (IDH) do mundo. A economia é uma das mais desenvolvidas de todo o globo, ocupando a 17º posição no ranking das maiores economias.

O país apresenta legislação e delegacias especializada em crimes cibernéticos, os quais cada vez mais tem aumentado no país. Logo, a demanda por profissionais qualificados em segurança das tecnologias de informação cresceu ao ponto de faltar mão de obra, o que levou o governo a passar a apoiar a formação de novos especialistas.

Em 2013, a polícia australiana anunciou a prisão do "líder autoproclamado" do grupo ativista hacker Lulz Security, mais conhecido pela sigla LulzSec. O conjunto foi criado em 2017 e era formado, principalmente, por ex-membros da legião Anonymous. Tornaram-se famosos após serem responsabilizados por ataques ao site da Sony e da CIA. O jovem de 24 anos foi acusado de ter invadido e alterado um site do governo australiano. No mesmo ano, o país ratificou a Convenção de Budapeste, um tratado internacional que apresenta os crimes praticados através da Internet e suas formas penalizações.

Já em 2017, empresas com filiais no país sofreram prejuízos com um ciberataque de escala global. O vírus, batizado de "Petya", assumia o controle dos computadores e exigia pagamento em bitcoins para liberar o acesso.

9.3. Botsuana

Situado na porção sul do continente africano, Botsuana, ou Botswana, faz fronteira com a Zâmbia, África do Sul, Zimbábue e Namíbia. O país ocupa a 98º posição no ranking de Índice de Desenvolvimento Humano (IDH) e sua economia baseia-se na extração de recursos minerais, como o diamante e o cobre.

Em 2017, empresas com filiais no país sofreram prejuízos com um ciberataque de escala global. O vírus, batizado como "Petya" assumia o

controle dos computadores e exigia pagamento em bitcoins para liberar o acesso, cibercrime conhecido como “ransomware”. No mesmo ano, houve uma inovação no âmbito cibernético nacional: uma clínica privada passou a receber o bitcoin como pagamento para tratamentos médicos.

A SADC – Comunidade de Desenvolvimento da África Austral – aprovou em 2012 três modelos de leis a serem implantadas nos países membros do grupo. Entre elas, a lei de comércio eletrônico, proteção de dados e cibercriminalidade. Com a assistência da União Internacional das Telecomunicações e apoio da SADC, Botsuana tem investido na elaboração de uma estratégia nacional de segurança cibernética e implementação das leis.

9.4. Brasil

O Brasil é uma República Federativa Presidencialista e está localizado na América do Sul, integrando os países latino-americanos. Apesar de ter uma economia considerada emergente, possui padrões avançados em comparação com boa parte das demais economias periféricas. Dos países da América do Sul, ele é o país que concentra a maior quantidade de usuários de internet, mas ainda assim, pela falta de capacidade de punir os criminosos, está entre as 10 primeiras posições dos hackers mais ativos do mundo.

A principal lei relacionada a esse tipo de delito foi aprovada em 2012 e é apelidada de Lei Carolina Dieckmann, a Lei dos Crimes Cibernéticos (12.737/2012), que tipifica como crimes, infrações relacionadas ao meio eletrônico, como invadir computadores, violar dados de usuários ou "derrubar" sites. O uso de dados de cartões de débito e crédito sem autorização do proprietário também está previsto na lei, sendo equiparado à falsificação de documento particular. Em 2014, foi sancionada no país a Lei do Marco Civil da Internet, que tem como pontos principais a manutenção da privacidade, vigilância na web, internet livre, dados pessoais, fim do marketing dirigido, liberdade de expressão, conteúdo ilegal e armazenamento de dados.

Segurança e defesa cibernética são tratadas no Brasil por diversos organismos. No geral, os órgãos responsáveis pelas ações operacionais relacionadas à segurança no âmbito cibernético são o DISC (Departamento de

Segurança da Informação e Comunicações). E a defesa, pelo CDCiber (Centro de Defesa Cibernética), que compõe a estrutura do Exército Brasileiro (EB), vinculado ao Ministério da Defesa (MD).

O Brasil possui uma postura internacional de promoção da paz e utilização das Forças para proteger ou repelir ameaças estrangeiras. Entretanto, não possui medidas definidas para casos de ataques cibernéticos, tratando cada caso individualmente, de uma forma estabelecida de acordo com cada grupo de ameaça.

9.5. Canadá

O Canadá é um país localizado na América do Norte ou América Anglo-Saxônica, seu território encontra-se no hemisfério norte ocidental. Apresenta um dos melhores indicadores sociais do mundo, desse modo, os índices de analfabetismo são baixos, assim como os de mortalidade infantil e natalidade.

A definição de “crime de computador” no país é retirada da “Convenção Internacional sobre o Cibercrime”, de 23 de novembro de 2011. Nessa convenção, o Canadá foi um dos signatários da proposta de legislação para os países envolvidos com cibercrimes, tais como: os crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos; delitos de computador conexos; infrações relacionadas com a violação dos direitos de autor e direitos conexos; e responsabilidade acessória.

O governo do Canadá está atualmente revisando sua abordagem de segurança cibernética para conseguir aumentar o benefício das tecnologias digitais para canadenses e empresas, e para promover sua capacidade de segurança cibernética e inovação. Em relação a essas medidas, a Estratégia de Segurança Cibernética do Canadá está trabalhando em todos setores do governo para garantir de forma mais rígida essa segurança. O país também acredita que qualquer abordagem para lidar com ameaças cibernéticas deve acompanhar o respeito pelos direitos humanos e liberdades fundamentais.

9.6. China

A República Popular da China é o maior país da Ásia Oriental, fica localizado a leste do continente asiático e situado a oeste do Oceano Pacífico. O país se preocupa com a sua segurança cibernética e defende a cooperação entre países para a garantia da mesma.

Em 2013, os representantes da China, EUA e Rússia se encontraram para discutir os princípios do combate ao cibercrime. As discussões vieram após a publicação do primeiro documento sobre a aplicação do direito internacional vigente para as guerras cibernéticas, chamado Guia de Tallinn, que foi elaborado por especialistas do Centro de Excelência em Defesa Cibernética Cooperativa da Organização do Tratado Atlântico Norte (OTAN).

A China faz parte da Organização de Cooperação de Xangai, composta também por Cazaquistão, Federação Russa, Quirguistão, Tajiquistão e Uzbequistão. A Organização possui acordos relacionados à cooperação na Segurança de Informação e enviou ao Secretário Geral da Organização das Nações Unidas uma proposta de Código de Conduta Internacional para Segurança da Informação (UNIDIR, p.106, 2013).

9.7. Egito

O Egito, considerado o berço de uma das mais importantes civilizações da Antiguidade, é localizado na porção nordeste do continente africano, na região denominada África Mediterrânea. A sua política é baseada no republicanismo, com um sistema semipresidencial de governo.

O país se encontra na nona posição no Índice Global de Segurança Cibernética, de acordo com o Global Cybersecurity Index (GCI) da UIT, que é uma iniciativa multipartidária para medir o compromisso dos países com a segurança cibernética.

A Equipe Egípcia de Preparação para Emergências de Computadores (EG-CERT), criada pela Autoridade Reguladora Nacional de Telecomunicações em Abril de 2009, oferece suporte 24 horas e tem a missão de fornecer um

sistema de alerta precoce contra ataques maciços direcionados a infra-estrutura de informação crítica egípcia.

Em 2015, o governo egípcio aprovou uma lei antiterrorismo, intensificando a perseguição contra opositores e indo de encontro à lei dos crimes virtuais, que permite a punição de internautas por crimes como ameaça à unidade nacional ou perturbação da ordem pública.

9.8. Estados Unidos da América

Os Estados Unidos da América são um país da América do Norte e atualmente, a maior economia do mundo, apresentando forte desenvolvimento tecnológico e um alto IDH. De acordo com informações da Divisão de Estatísticas das Nações Unidas, o país possui uma população de aproximadamente 324 milhões de habitantes e 87% de seus cidadãos tem acesso à internet. Os Estados Unidos integra o Índice Global de Segurança Cibernética na 2ª posição.

O país norte-americano possui extensiva legislação quanto à crimes cibernéticos e diversas regulamentações acerca da segurança cibernética. Os Estados Unidos possuem duas Equipes de Resposta a Emergências de Computador (CERT) uma nacional e uma específico para sistemas de controle industrial, uma estratégia internacional de segurança cibernética e uma ordem executiva que aborda a segurança cibernética de infraestruturas críticas. As autoridades responsáveis por monitorar e coordenar a implementação da estratégia nacional de segurança cibernética são o Departamento de Defesa e o Departamento de Segurança da Pátria. Os Estados Unidos também possuem três roteiros relacionados a diferentes aspectos da segurança cibernética nacional (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, p.1-2, 2015). Em 2012, um documento denominado “Guerra Cibernética Fundacional (Plano X)”, da Agência Projetos Avançados de Pesquisa de Defesa dos Estados Unidos, solicitou pesquisas a respeito da realização de uma guerra cibernética (UNIDIR, p.54, 2013).

O país possui um acordo nacional para o compartilhamento de informações entre agências internas e tem parcerias com diversos países,

entre eles o Canadá e a Estônia. Os Estados Unidos da América são signatários da Convenção sobre Crimes Cibernéticos do Conselho da Europa, têm uma cooperação com a União Europeia com relação à Segurança Cibernética e do Ciberespaço e participa do Fórum de Resposta a Incidentes e Equipes de Segurança.

Em um relatório acerca da segurança cibernética no contexto internacional, os Estados Unidos afirmam que, independentemente das estratégias internas tomadas pelos Estados, a colaboração internacional em estratégias para reduzir ameaças às TICs é essencial para assegurar a segurança de todos. O país reconhece que as características especiais de ferramentas maliciosas da tecnologia da informação, como a sua habilidade de permanecer despercebidas e a dificuldade de localizar sua origem, tornam estratégias como as medidas de desarmamento ineficazes e criam a necessidade de novas abordagens (ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS, p.14-15, 2011).

9.9. Estônia

Situada na região nordeste do continente europeu, a Estônia é uma das três repúblicas bálticas (banhada pelo mar Báltico) e faz fronteira com a Rússia e com a Letônia. A Nação pertencia à União das Repúblicas Socialistas Soviéticas (URSS) e atualmente apresenta uma economia bem consolidada, sustentada pelo setor de serviços e industrial. Além disso, ocupa a 30º posição no Índice de Desenvolvimento Humano.

Em 2001, tornou-se um dos signatários da Convenção de Budapeste, um tratado internacional que apresenta os crimes praticados através da Internet e suas formas penalizações. A ratificação do documento ocorreu em 2003 e a partir de 2004, vigorou no país.

Sendo um país em que 98% da população tinha acesso à Internet, em 2005, a Estônia se tornou o primeiro país a permitir eleições governamentais através da internet. Grande parte do serviço público também se encontra disponível em rede, o que facilitaria o acesso da população. Contudo, a experiência teve efeitos negativos: o país se tornou alvo potencial de ataques

cibernéticos. Em 2007, uma série de ataques que duraram três semanas deixaram diversos sites inacessíveis e foram direcionados para os provedores de Internet do país. A ameaça foi combatida em colaboração com a Organização do Tratado do Atlântico Norte (OTAN) e a Finlândia. Especulou-se que a autoria do atentado teria sido do governo russo ou de russos, os quais se apresentavam contra a remoção de um estátua de bronze de um soldado soviético na capital, Tallinn. Contudo, não se pode afirmar realmente a que Nação pertenciam os criminosos.

Em 2017, a cidade de Tartu sediou a Cyber Coalition, a qual se tratava de um evento de exercício de treinamento de defesa da OTAN, que reuniu cerca de 700 especialistas em tecnologia da informação e direito de diversos Estados membros. O objetivo da reunião era testar se os países estavam aptos à combaterem ameaças cibernéticas e promover a cooperação em nível internacional e nacional a respeito da segurança do espaço virtual.

9.10. Federação Russa

A Federação Rússia é um enorme país localizada no norte da Eurásia, com a maior extensão territorial do planeta e é uma das grandes economias em desenvolvimento. De acordo com a Divisão de Estatísticas das Nações Unidas, o país tem uma população de aproximadamente 143 milhões de pessoas, das quais 70% têm acesso à internet; está na 10ª colocação do Índice Global de Segurança Cibernética.

A Federação Russa possui extensiva regulamentação no quesito de segurança cibernética e seu código criminal abrange crimes na esfera de informação. O país possui quatro CERTs ativos, o GOV-CERT.RU, responsável pela resposta à incidentes relacionados a organismos governamentais, o RU-CERT e CERT-GIB, encarregados dos incidentes não relacionados a agências governamentais e o FinCERT, do Banco da Rússia, para lidar com incidentes financeiros e de crédito (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, p.2, 2015). A Rússia tem padronizações, gerais e específicas, de segurança cibernética e uma certificação de agências públicas e nacionais. O país adota diversas políticas, estratégias e princípios

relacionados à segurança da informação, tanto nacional quanto internacionalmente, e um curso voltado para esse tópico.

O CERT-RU participa de associações internacionais para cooperação e intercâmbio de informação, o Fórum para Resposta à Incidentes e Equipes de Segurança e o Trusted Introducer, uma plataforma europeia que lista CERTs existentes e credencia aqueles que atingirem os requisitos definidos, ganhando assim acesso aos serviços disponíveis. O país participa da Organização para Cooperação em Segurança na Europa, que possui diversas medidas de construção de confiança visando a prevenção de conflitos no uso de TICs.

A Federação Russa faz parte da Organização de Cooperação de Xangai, composta também por China, Cazaquistão, Quirguistão, Tajiquistão e Uzbequistão. A Organização possui acordos relacionados a cooperação na Segurança de Informação e enviou ao Secretário Geral da Organização das Nações Unidas uma proposta de Código de Conduta Internacional para Segurança da Informação (UNIDIR, p.106, 2013).

9.11. Finlândia

A Finlândia, oficialmente República da Finlândia, é um país do norte europeu, membro da união europeia, possui alto IDH e elevada expectativa de vida. Mais de 90% de sua população possui acesso à internet (União Internacional de Telecomunicações, p.1, 2015) e se encontra na 16ª posição do Índice Global de Segurança Cibernética.

O país nórdico tem diversos crimes cibernéticos previstos em seu código criminal e possui uma legislação específica sobre segurança cibernética na forma do Ato Sobre a Proteção de Privacidade em Comunicações Eletrônicas. A Finlândia dispõe de uma Equipe de Resposta à Incidentes Computacionais (CERT) com o nome de FICORA, sigla em inglês para Autoridade Finlandesa Regulatória de Comunicações, ou Viestintävirasto, em finlandês; possui também estratégia nacional de segurança cibernética desde 2013 (União Internacional de Telecomunicações, p.1, 2014).

Com relação às iniciativas de segurança cibernética internacionais, os finlandeses participam da Colaboração de CERTs Nacionais Nórdicos, colaboração da qual também fazem parte Dinamarca, Islândia, Noruega e Suécia e a FICORA é membra do Fórum de Resposta a Incidentes e Equipes de Segurança. O país participa do grupo de CERTs Governamentais Europeus e tem uma parceria com a empresa Codenomicon, para desenvolver um sistema de detecção de intrusos e um serviço automático de relatório de incidentes nacionais (UIT, p.44, 2017).

No âmbito do diálogo global, a Finlândia é ativa na Organização para Segurança e Cooperação na Europa, faz parte do Conselho da Convenção Europeia sobre Segurança Cibernética e participa da Convenção de Budapeste desde 2007(ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS, p.10, 2016). No relatório de suas visões, quanto ao Grupo de Peritos Governamentais, o país ressalta a continuidade de medidas de construção de confiança e o fortalecimento das parcerias com atores privados nacional e internacionalmente.

9.12. França

A França, oficialmente República Francesa, é um país localizado na Europa Ocidental, é uma grande potência econômica e é um dos membros permanentes do Conselho de Segurança. Tem uma população de aproximadamente 65 milhões, 84% dos quais tem acesso à internet, segundo a Divisão de Estatísticas das Nações Unidas, e ocupa a 8ª posição do Índice Global de Segurança Cibernética, e 2ª posição na Europa.

A legislação francesa abrange o ciberespaço desde 2004 e o país possui diversas regulamentações relacionadas ao uso da internet. A França goza de um CERT nacional e diversos outros para fins específicos, padronizações e certificações para agências e profissionais. A Agência Nacional de Segurança de Sistemas da Informação é responsável pelas políticas específicas e pesquisas sobre padronizações, boas práticas e diretrizes para segurança cibernética.

A agência nacional de TI reconheceu como parceiros quanto à troca de informações relacionadas a incidentes e práticas de segurança cibernética, agências de segurança de países como Alemanha, Estados Unidos, Estônia, Holanda e Reino Unido (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, p.2, 2015). A França participa da Agência da União Europeia para Segurança de Informação e de Rede, da Organização para Segurança e Cooperação na Europa e do Fórum para Resposta à Incidentes e Equipes de Segurança.

Segundo o Índice Cibernético, o país está desenvolvendo capacidades ofensivas para guerras cibernéticas e possui unidades de ataque cibernético, tanto no exército, quanto na aeronáutica (UNIDIR, p. 22, 2013). Os quatro objetivos franceses no ciberespaço são se tornar uma potência global em defesa cibernética, garantir soberania na informação e liberdade de decisão, assegurar infraestruturas críticas e manter a privacidade no ciberespaço.

9.13. Holanda

A Holanda, oficialmente Países Baixos, é uma monarquia constitucional parlamentar democrática, localizada na Europa Ocidental; possui uma ótima qualidade de vida, tendo a 7ª posição no Índice de Desenvolvimento Humano. 93% dos seus 17 milhões de habitantes tem acesso à internet, conforme a Divisão de Estatísticas das Nações Unidas, e se encontra na 15ª posição do Índice Global de Segurança Cibernética.

O país tem crimes cibernéticos previstos em seu código e possui algumas regulamentações específicas, especialmente o Ato de Proteção à Informação.

A organização responsável por segurança cibernética e resposta a incidentes na Holanda é o Centro Nacional de Segurança Cibernética, que adota a Estratégia de Segurança Cibernética Nacional. O país possui um programa para promover conscientização e cursos de especialização em segurança cibernética para os setores público e privado, além de realizar pesquisas relativas a diretrizes, boas práticas e padronizações em segurança cibernética através do Centro Nacional de Segurança Cibernética.

A Holanda possui um programa nacional para compartilhamento de informações relevantes para a segurança cibernética com os setores público e privado e tem uma parceria com a empresa CSIRT. Internacionalmente, o país participa do Fórum para a Resposta de Incidentes e Equipes de Segurança, da Agência da União Europeia para Segurança de Informação e Rede e do grupo dos CERTs de Governos Europeus (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, p.2, 2015).

Segundo o Índice Cibernético, A Holanda inclui em sua estratégia de segurança cibernética o estabelecimento de parcerias público-privadas e a busca por cooperação internacional. (UNIDIR, p. 37, 2013). Em um relatório, o país expressa sua intenção de intensificar seu compromisso com a diplomacia cibernética, para manter a paz e a estabilidade no ciberespaço, promover a ordem jurídica e desenvolver uma cultura de segurança colaborativa, “construindo pontes digitais” (ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS, p.18, 2017).

9.14. Índia

A Índia, ou República da Índia, é um país asiático localizado em uma região chamada de subcontinente indiano. O país tem como sistema político uma democracia parlamentar centrada no federalismo e sua população é predominantemente rural, com grande parte de sua produção vinculada à agricultura de subsistência, aplicando técnicas tradicionais de plantio.

Configura-se um dos maiores centros de TI (Tecnologia da Informação) no mundo e apresenta um grande número de casos relacionados à crimes cibernéticos, que vêm crescendo nos últimos tempos. O país não possui uma estratégia oficial ligada à segurança e defesa cibernética, e não há um órgão exclusivamente responsável pela condução das ações relacionadas a esse tipo de crime. O tema é abordado, pelos órgãos, à medida que couber a cada um e por meio da cooperação geral, é possível conduzir as ações de proteção.

Apesar de apresentar baixo investimento para a manutenção da segurança no âmbito cibernético, a Índia está atenta aos acontecimentos do

mundo e procura cada vez mais se aproximar das discussões ligadas a esse tema.

9.15. Indonésia

A Indonésia, ou República da Indonésia, é um país asiático localizado em um arquipélago; possui uma grande economia, mas seu IDH não é alto. Segundo dados da Divisão de Estatísticas das Nações Unidas, a Indonésia tem uma população de mais de 260 milhões de habitantes, dos quais apenas 17% tem acesso à internet, e se encontra na 70ª posição do Índice Global de Segurança Cibernética.

No quesito legal, o país possui uma legislação voltada para as TICs desde 2008 e múltiplas regulamentações. A Indonésia dispõe de quatro CERTs diferentes e de aproximadamente 500 profissionais certificados em segurança cibernética no setor público, mas não tem estratégias oficiais ou planos de implementação para segurança cibernética. Os órgãos nacionais responsáveis pela segurança cibernética são o Ministério de Comunicação e Segurança da Informação, a Diretoria Geral de Aplicações de Informática e a Diretoria de Segurança da Informação (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, p.2, 2014).

O país tem uma parceria oficial com o Conselho Nacional de Segurança da Informação do Japão e é um membro da iniciativa UIT-IMPACT, a Aliança Multilateral Internacional Contra Ameaças Cibernéticas (International Multilateral Partnership Against Cyber Threats). A Indonésia participou de atividades de segurança cibernética com o Fórum de Resposta a Incidentes e Resposta e Equipes de Segurança, a Equipe de Resposta a Incidentes Computacionais da Ásia-Pacifico e o Conselho de Ação de Segurança em Rede da Associação de Nações do Sudeste Asiático, entre outros (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, p.2-3, 2014).

9.16. Japão

O Japão é um país localizado no extremo oriente e seu território é constituído por um arquipélago de relevo acidentado. O seu sistema político é baseado na democracia constitucional.

O país foi signatário da Convenção de Budapeste sobre o Cibercrime - aprovada pelo Conselho da Europa em 2001 -, juntamente com 42 países. Na convenção estão previstos, por exemplo, medidas contra os crimes de acesso ilícito; interceptação ilícita; interferência em dados e em sistemas; produção, venda, obtenção para utilização, importação e distribuição de dispositivos concebidos para a prática de crimes cibernéticos.

Em 2016, uma nova lei foi aprovada no país, visando aumentar o número de especialistas em ataques cibernéticos frente aos jogos olímpicos e paraolímpicos de 2020, que acontecerão em Tóquio. Foram convidados hackers para testar o sistema, seguindo o exemplo da Grã-Bretanha, que fez o mesmo durante a preparação para os Jogos Olímpicos de Londres-2012.

A segurança cibernética do Japão é compartilhada entre a Agência Nacional da Polícia e quatro ministérios, e o número de casos de ataques virtuais estão crescendo cada vez mais no país e, em detrimento disso, os gastos com a segurança nesse âmbito estão mais altos.

9.17. México

O México, oficialmente Estados Unidos Mexicanos, é uma república constitucional federal, localizada na América do Norte, e possui uma das maiores economias do continente americano. De acordo com a Divisão de Estatísticas das Nações Unidas, o país tem uma população de aproximadamente 129 milhões de pessoas, das quais 44% tem acesso à internet, e o Índice Global de Segurança Cibernética o coloca na 28º posição.

O código criminal mexicano prevê crimes cibernéticos e o país possui uma regulamentação específica sobre segurança cibernética, a Lei Sobre Assinaturas Eletrônicas Avançadas. No México, o responsável pela resposta à incidentes é o CERT-MX e todas as instituições governamentais devem seguir

o padrão ISO 207001. O Comitê Especializado de Segurança da Informação é o responsável por desenvolver a Estratégia Nacional de Segurança da Informação. O país organiza diversas conferências para instituições governamentais e educacionais, com o objetivo de aumentar a consciência com relação à segurança cibernética, e proporciona aos funcionários da Divisão Científica treinamentos especializados do Sistema de Desenvolvimento Policial do México e de agências de países como Colômbia, Estados Unidos, Holanda e Japão (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, p.2, 2015).

O CERT mexicano, seguindo a Estratégia Nacional de Segurança da Informação, é responsável por compartilhar recursos e informações de segurança com o setor público e com empresas. O México Integra o Fórum para a Resposta de Incidentes e Equipes de Segurança e o Comitê Interamericano contra o Terrorismo (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, p.2, 2015), da Organização dos Estados Americanos, que segue a Estratégia Integral Inter-Americana para Combater Ameaças à Segurança Cibernética.

O país deposita grande importância na questão jurídica, considerando-a necessária para a proteção da informação no ciberespaço, chegando a citar em um relatório a adoção e melhoria de legislação relativa e o treinamento de juízes em questões de segurança cibernética como medidas para fortalecer a segurança cibernética global (UNITED NATIONS GENERAL ASSEMBLY, p.8, 2010).

9.18. Quênia

O Quênia localiza-se no continente africano, mais precisamente na região conhecida como África Subsaariana. A maioria dos habitantes vive abaixo da linha de pobreza, ou seja, com menos de 1,25 dólar por dia. Outro aspecto social negativo é a alta taxa de mortalidade infantil. Apesar disso, é o país mais inovador e com a internet mais rápida da África.

Em 2014, a polícia queniana prendeu 77 cidadãos chineses acusados de dirigir uma rede cibercriminosa e um misterioso ‘centro de controle’ em um

elegante bairro de Nairóbi. Eles pretendiam lançar um ataque contra os sistemas de comunicação do país e possuíam material que permitiria invadir contas bancárias, caixas eletrônicos e serviços de pagamento via celular. Apesar de pouca expressão no cenário cibernético, o país se preocupa e procura lidar da melhor forma possível com os casos que ocorrem em seu território.

9.19. Reino Unido

O Reino Unido, oficialmente Reino Unido da Grã-Bretanha e Irlanda do Norte, é uma monarquia parlamentarista localizada na Europa ocidental, berço da revolução industrial e uma das maiores economias mundiais. Segundo a Divisão de Estatísticas das Nações Unidas, o país tem 65 milhões de habitantes, 92% dos quais têm acesso à internet, e se encontra em 12º lugar no Índice Global de Segurança Cibernética.

O Reino Unido tem leis que englobam crimes cibernéticos desde 1990 e também regulamentos específicos à segurança cibernética. O país possui inúmeros CERTs, responsáveis, por exemplo, por infraestruturas críticas, redes governamentais e redes militares, além de organizações que emitem certificados, como o Instituto de Profissionais da Segurança da Informação (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, p.1, 2014). O Reino Unido implementa, desde 2011, sua estratégia de segurança cibernética nacional em planos quinquenais, que recebem amplo financiamento do governo e são de responsabilidade do Escritório de Segurança Cibernética e Segurança da Informação. O país adotou um programa de conscientização da população e publicou orientações para o setor privado alcançar uma maior segurança cibernética.

O Reino Unido integra organizações de segurança, como a Organização do Tratado do Atlântico Norte e a Agência da União Europeia para Segurança da Rede e da Informação, e de padronizações relacionadas às TICs, como o Common Criteria e a União Internacional de Telecomunicações. O país também está presente em grupos para a cooperação de CERTs

internacionalmente, como o Trusted Introducer e o grupo de CERTs Governamentais Europeus.

O país enxerga como fundamental a colaboração de todas as sociedades na governança da internet e no combate às ameaças cibernéticas, visto que os governos não possuem monopólio sobre a infraestutura ou operação do ciberespaço e que o reconhecimento da pluralidade do controle da internet levará ao aumento da segurança e da estabilidade e à promoção de progresso social e econômico. O país também encoraja maior cooperação entre os órgãos de aplicação das leis de acordo com a Convenção de Budapeste sobre Crimes Cibernéticos. O Reino Unido vê grande importância em se assegurar de que os esforços para aumentar a segurança cibernética não sejam usados para restringir a liberdade de expressão, de acordo com a Declaração Universal dos Direitos Humanos e a resolução 20/8 de 2012 do Conselho dos Direitos Humanos, que afirma que os direitos desfrutados pelas pessoas devem também ser protegidos online (FOREIGN & COMMONWEALTH OFFICE, p.3, 2016). O país acredita que esse Grupo de Peritos Governamentais se configura como uma excelente oportunidade para continuar a considerar como as leis internacionais se aplicam ao ciberespaço e quais normas de comportamento podem promover segurança e evitar conflitos. O Reino Unido tem a visão de que, atualmente, tentativas de firmar tratados multilaterais compreensivos não trariam qualquer contribuição benéfica para a segurança cibernética internacional.

9.20. Senegal

Senegal é uma república semipresidencialista localizada à oeste do continente africano, possui uma economia centrada no setor terciário e um baixo Índice de Desenvolvimento Humano. O país tem 16 milhões de pessoas, com uma parcela de 18% da população tendo acesso à internet, de acordo com a Divisão de Estatísticas das Nações Unidas, e se encontra na 89º colocação no Índice Global de Segurança Cibernética.

Senegal possui uma lei sobre o crime cibernético e regulamentações de segurança cibernética, como as leis de Criptologia, Proteção de Dados e Transações Eletrônicas. O país não possui um CERT, mas faz parte da UIT-IMPACT, a Aliança Multilateral Internacional Contra Ameaças Cibernéticas, que realizou uma avaliação nacional para uma futura implementação de um Centro.

Um estudo publicado pela Companhia Europeia de Inteligência Estratégica afirma que os ataques cibernéticos na África Ocidental teriam aumentado em 132% entre 2013 e 2015, que os prejuízos seriam de aproximadamente 2,7 milhões de dólares e que somente 30% dos criminosos foram presos. Senegal teve 47 sites governamentais invadidos pelo grupo Anonymous em 2014 e os hackers voltaram a atacar em 2015.

Em 2016, Senegal ratificou a Convenções de Malabo sobre Segurança Cibernética e Dados Pessoais e a Convenção de Budapeste sobe Crime Cibernético. O país tem uma parceria com a União Europeia e com a Ação Global sobre Cibercrime e também participa do AfricaCERT.

10. Referências

ALTERMAN, Denis. **O que é o Wikileaks e por que ele incomoda tanta gente?.** Disponível em: https://www.midiatismo.com.br/o-que-e-o-wikileaks-e-por-que-ele-incomoda-tanta-gente. Acesso em: 10 fev. 2018.

ANONYMOUS BRASIL. **Quem somos nós.** Disponível em: http://www.anonymousbrasil.com/sobre-anonymous. Acesso em: 2 fev. 2018

AZEVEDO, Carlos. **Meios de comunicação como armas de guerra.** Universidade Federal da Paraíba, 2001. Disponível em: http://bocc.ubi.pt/pag/azevedo-carlos-comunicacao-armas-guerra.html. Acesso em: 14 fev. 2018.

BBC. **Austrália prende 'líder' de grupo de hackers LulzSec.** Disponível em: http://www.bbc.com/portuguese/noticias/2013/04/130424_australia_prisao_hacker_lulzsec_rw. Acesso em: 10 fev. 2018

BRASIL ESCOLA. **Canadá.** Disponível em: http://brasilescola.uol.com.br/geografia/canada.html. Acesso em: 16 fev . 2018.

CAMARA, Ismaïla. **It's time for Senegal to have its cert.** *Social Net Link.* Disponível em: http://www.socialnetlink.org/2017/06/il-est-temps-que-le-senegal-ait-son-cert/. Acesso em: 21 fev. 2018

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. In: Âmbito Jurídico, Rio Grande, XV, n. 99, abr 2012. Disponível em: http://www.egov.ufsc.br/portal/conteudo/crimes-virtuais-elementos-para-uma-reflex%C3%A3o-sobre-o-problema-na-tipifica%C3%A7%C3%A3o.

CASTELLS, Manuel. **A galáxia da internet: Reflexões sobre a internet de negócios e a sociedade.** 1 ed. Zahar, 2001.

CASTRO, Manuela. **Após 25 anos do fim da URSS, Cazaquistão comemora economia forte e estabilidade.** Disponível em: http://agenciabrasil.ebc.com.br/internacional/noticia/2016-12/apos-25-anos-do-fim-da-urss-cazaquistao-comemora-crescimento-economico/. Acesso em: 15 fev. 2018.

CAVALCANTE, Waldek Fachinelli. **Crimes cibernéticos: noções básicas de investigação e ameaças na internet.** Conteudo Juridico, Brasilia-DF: 16 out. 2015. Disponivel em: http://www.conteudojuridico.com.br/?artigos&ver=2.54548&seo=1. Acesso em: 18 fev. 2018.

CEBRIÁN, B. D.. **Cibertaque: o vírus WannaCry e a ameaça de uma nova onda de infecções.** Disponível em: https://brasil.elpais.com/brasil/2017/05/14/internacional/1494758068_707857.html. Acesso em: 15 fev. 2018.

CERQUEIRA, Silvio Castro; ROCHA, Claudionor. **Crimes cibernéticos: desafios da investigação.** Cadernos Aslegis, Brasília, n. 49, p. 131-161, maio/ago. 2013.

CHAGAS, Morgana Santos das. **CIBERTERRORISMO: AS POSSIBILIDADES DA EXPANSÃO DO TERROR NAS RELAÇÕES INTERNACIONAIS.** 2012. 52 f. Monografia (Especialização) - Curso de Relações Internacionais, Uepb, João Pessoa, 2012. Disponível em: http://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/11089/1/PDF - Morgana Santos das Chagas.pdf. Acesso em: 21 jan. 2018

CIO. **Escassez de mão de obra em segurança cibernética é global. Disponível em:** http://cio.com.br/tecnologia/2016/08/01/escassez-de-mao-de-obra-em-seguranca-cibernetica-e-global/ . Acesso em: 9 fev. 2018.

CONSELHO DA EUROPA. **Quadro das assinaturas e ratificações do Tratado 185.** Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures . Acesso em: 15 fev. 2018

CRESPO, Marcelo. **Crimes digitais: do que estamos falando?** Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/. Acesso em: 2 fev. 2018

DAVID, Hadassa Ester; CAETANO, Márcia Mariano Raduan. **A influência das guerras na comunicação: a relação entre os conflitos e a produção de discursos midiáticos.** Instituto de Ensino Superior de Rio Verde, Rio Verde, GO. Disponível em: http://intercom.org.br/papers/regionais/centrooeste2011/resumos/r27-0137-1.pdf. Acesso em: 14 fev. 2018.

DEPARTMENT OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS CANADA. **Cyber security**. Disponível em: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-en.aspx. Acesso em: 16 fev. 2018.

DUARTE, Adrien Carlos. **Marco civil da internet: o que é e o que muda na sua vida.** Disponível em: https://www.oficinadanet.com.br/post/12558-o-marco-civil-da-internet-foi-aprovado-entenda-o-que-e-e-o-que-muda-na-sua-vida. Acesso em: 14 fev. 2018.

EMBAIXADA DO JAPÃO NO BRASIL. **Estrutura governamental.** Disponível em: http://www.br.emb-japan.go.jp/cultura/estruturagovernamental.html. Acesso em: 16 fev. 2018.

ENCICLOPÉDIA DO HOLOCAUSTO. **A disseminação da informação jornalística nazista**. Disponível em: https://www.ushmm.org/wlc/ptbr/article.php?moduleid=10007821. Acesso em: 14 fev. 2018.

EUROPEAN GOVERNMENT CERTS GROUP. **Members of the European Government CERTs group.** Disponível em: http://www.egc-group.org/contact.html. Acesso em: 18 fev. 2018.

EXAME. **Quênia prende 77 chineses em operação contra cibercrime.** Disponível em: https://exame.abril.com.br/tecnologia/quenia-prende-77-chineses-em-operacao-contra-cibercrime/. Acesso em: 17 fev. 2018

FERNANDES, Claudio. **Terrorismo.** *História do mundo*. Disponível em: http://historiadomundo.uol.com.br/idade-contemporanea/terrorismo.htm. Acesso em: 11 fev. 2018.

FOREIGN & COMMONWEALTH OFFICE. **Response to General Assembly resolution 70/237 "Developments in the field of information and telecommunications in the context of international security".** Disponível em: https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/10/UK.pdf. Acesso em: 18 fev. 2018.

FERRARI, Bruno. **Hackers do Anonymous reforçam declaração de guerra a terroristas do Estado Islâmico.** Disponível em: http://epoca.globo.com/vida/experiencias-digitais/noticia/2015/11/hackers-do-anonymous-reforcam-declaracao-de-guerra-terroristas-do-estado-islamico1.html. Acesso em: 2 fev. 2018.

FRANCISCO, Wagner de Cerqueira e. **Austrália.** *Brasil Escola* Disponível em: http://brasilescola.uol.com.br/geografia/australia.htm. Acesso em: 11 fev. 2018.

_____. **Botsuana.** Brasil Escola Disponível em: http://brasilescola.uol.com.br/geografia/botsuana.htm. Acesso em: 11 fev. 2018.

_____. **Cazaquistão.** *Brasil Escola* Disponível em: http://brasilescola.uol.com.br/geografia/cazaquistao.htm. Acesso em: 11 fev. 2018.

_____. **Egito.** *Brasil Escola* Disponível em: http://brasilescola.uol.com.br/geografia/egito-1.htm. Acesso em: 16 fev. 2018.

_____. **Estônia.** *Brasil Escola*. Disponível em <http://brasilescola.uol.com.br/geografia/estonia.htm>. Acesso em: 15 fev.de 2018.

_____. **Índia.** *Brasil Escola.* Disponível em: http://mundoeducacao.bol.uol.com.br/geografia/india.html. Acesso em: 15 fev. 2018.

_____. **Quênia.** *Brasil Escola.* Disponível em: http://mundoeducacao.bol.uol.com.br/geografia/quenia.html. Acesso em: 17 fev. 2018.

FREE SOFTWARE FOUNDATION. **Historia de internet.** Nov. 2002. Disponível em: http://cmapspublic2.ihmc.us/rid=1239136955718_1163871558_10281/historia%20internet.pdf. Acesso em: 14 fev. 2018.

FREITAS, Eduardo de. **Alemanha.** Disponível em: http://brasilescola.uol.com.br/geografia/alemanha.html. Acesso em: 16 fev. 2018.

FREITAS, Eduardo de. **Índia**. Disponível em: http://brasilescola.uol.com.br/geografia/india.html. Acesso em: 15 fev. 2018.

G1. **Bolívia, Suécia, Etiópia e Cazaquistão entram para Conselho de Segurança.** Disponível em: http://g1.globo.com/mundo/noticia/2016/06/bolivia-suecia-etiopia-e-cazaquistao-entram-para-conselho-de-seguranca.html. Acesso em: 11 fev. 2018.

_____. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA.** Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 5 fev. 2018.

_____. **Estado Islâmico usa de WhatsApp a Twitter para promover 'terrorismo viral'.** Disponível em: http://g1.globo.com/tecnologia/noticia/2015/11/estado-islamico-usa-de-whatsapp-twitter-para-promover-terrorismo-viral.html. Acesso em: 5 fev. 2018.

_____. **Hackers declaram guerra ao Estado Islâmico: 'Vamos encontrá-los'.** Disponível em: http://g1.globo.com/mundo/noticia/2015/11/hackers-declaram-guerra-ao-estado-islamico-vamos-encontra-los.html. Acesso em: 5 fev. 2018.

_____. **Internet oculta: os segredos de um universo paralelo.** Disponível em: http://g1.globo.com/tecnologia/noticia/2014/07/internet-oculta-os-segredos-de-um-universo-paralelo.html. Acesso em: 5 fev. 2018.

GERCKE, M. **ENTENDENDO O CIBERCRIME: UM GUIA PARA PAÍSES EM DESENVOLVIMENTO.** 2. ed. Genebra, 2011. 493 p. Disponível em: <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>. Acesso em: 28 jan. 2018

GOCACHE - NEXT-GEN CDN. **Veja os 10 países do mundo com maior número de hackers e crimes cibernéticos.** Disponível em:

https://www.gocache.com.br/seguranca/dez-paises-com-mais-ataques-de-hackers/. Acesso em: 15 fev. 2018.

GOMES JÚNIOR, José. **A publicidade no rádio: origem e evolução.** In: INTERCOM - SOCIEDADE BRASILEIRA DE ESTUDOS INTERDISCIPLINARES DE COMUNICAÇÃO, 2000, São Paulo.Disponível em: http://www.portcom.intercom.org.br/pdfs/40c31f36d4d023b0726c48094dd32b21.pdf. Acesso em: 11 fev. 2018.

HAJE, Lara. **Saiba como os crimes na internet são tratados em outros países.** Disponível em: http://www2.camara.leg.br/camaranoticias/noticias/ciencia-e-tecnologia/199806-saiba-como-os-crimes-na-internet-sao-tratados-em-outros-paises.html. Acesso em: 17 fev. 2018.

HARADA, Eduardo. **TecMundo Explica: o que é essa tal de "Deep Web".** *TECMUNDO.* Disponível em: https://www.tecmundo.com.br/tecmundo-explica/74998-tecmundo-explica-tal-deep-web.htm. Acesso em: 11 fev. 2018.

IT FORUM 365. **Clínica privada em Botswana passa a receber bitcoin como pagamento.** Disponível em: https://www.itforum365.com.br/tecnologia/clinica-privada-em-botswana-passa-receber-bitcoin-como-pagamento/. Acesso em:13 fev. 2018.

INTERNATIONAL TELECOMUNICATION UNION. **CYBERWELLNESS PROFILE FINLAND**. Ago. 2014.

_____**. CYBERWELLNESS PROFILE FRANCE.** Jan. 2015.

_____. **CYBERWELLNESS PROFILE INDONESIA**. Aut. 2014.

_____. **CYBERWELLNESS PROFILE MEXICO**. Fev. 2015.

_____. **CYBERWELLNESS PROFILE REPUBLIC OF CUBA.** Mar. 2015.

_____. **CYBERWELLNESS PROFILE REPUBLIC OF SENEGAL**. Mar. 2015.

_____. **CYBERWELLNESS PROFILE RUSSIAN FEDERATION**. Jan. 2015.

_____. **CYBERWELLNESS PROFILE THE NETHERLANDS**. Jan. 2015.

_____. **CYBERWELLNESS PROFILE UNITED KINGDOM**. Ago. 2014.

_____. **CYBERWELLNESS PROFILE UNITED STATES**. Jan. 2015.

_____. **Global Cybersecurity Index (GCI) 2017.** Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

JÚNIOR, Samuel César Da Cruz. **A segurança e defesa cibernética no brasil e uma revisão das estratégias dos estados unidos, rússia e índia para o espaço virtual.** Instituto de Pesquisa Econômica Aplicada (IPEA), Brasília, p. 1-58, jun. 2013.

KASPERSKY LAB. **O telégrafo, a invenção que deu início à era da informação**. Disponível em: https://www.kaspersky.com.br/blog/telegraph-grandpa-of-internet/5431/. Acesso em: 10 fev. 2018.

KELLY, Tim; KUBO, Nobuhiro **Japão faz primeira simulação de ataque cibernético de olho na olimpíada de 2020.** Disponível em: https://oglobo.globo.com/mundo/japao-faz-primeira-simulacao-de-ataque-cibernetico-de-olho-na-olimpiada-de-2020-11910973. Acesso em: 17 fev. 2018.

LOPEZ, Felix G. **Política e burocracia nos estados da Índia e do Brasil.** Revista Sociologia e Politica vol.16,Curitiba, ago. 2008

LUCAS, Giovana Azevedo Pampanelli. **A evolução do telefone e uma nova forma de sociabilidade: o flash mob**. Disponível em: http://www.razonypalabra.org.mx/anteriores/n41/gazevedo.html. Acesso em: 10 fev. 2018.

MACHADO, Lucyana A. **Crimes cibernéticos - A consciência digital, independente da idade, é o caminho mais seguro para o bom uso da internet, sujeita às mesmas regras de ética, educação e respeito ao próximo.** Nov. 2014. Disponível em: https://www.direitonet.com.br/artigos/exibir/8772/Crimes-ciberneticos. Acesso em: 18 jan. 2018.

MARTINS, Thiago De Souza. **Crimes cibernéticos e a impunidade legal.** Universidade estadual de goiás, Anápolis, nov. 2012. Disponível em: http://www.ccet.ueg.br/biblioteca/arquivos/monografias/01-tc_-_thiago_de_souza_martins.pdf. Acesso em: 12 jan. 2018.

MINIONU INTERPOL. **Egito.** Disponível em: https://2minionuinterpol.wordpress.com/2017/05/25/egito/. Acesso em: 16 fev. 2018.

MINISTÉRIO PÚBLICO FEDERAL. **Combate aos crimes cibernéticos.** Disponível em: http://www.cnmp.mp.br/portal/images/Palestras/Atua%C3%A7%C3%A3o_do_MP_no_combate_aos_crimes_cibern%C3%A9ticosINFANCIA_E_JUVENTUDE.pdf.

MINISTÉRIO PÚBLICO FEDERAL. **Roteiro de atuação sobre crimes cibernéticos.** Brasília, 2013. Disponível em : http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf.

MINISTRY FOR FOREIGN AFFAIRS OF FINLAND. **Response to the General Assembly resolution 70/237 on "Developments in the field of information and telecommunications in the context of international security".** Mai. 2016.

MONTEIRO, Luís. **A internet como meio de comunicação: Possibilidades e limitações.** INTERCOM – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, XXIV Congresso Brasileiro da Comunicação, Campo Grande, MS, set. 2001. Disponível em: http://www.jack.eti.br/www/arquivos/documentos/trabalhos/fae/Trabalho_Redes_Adinarte_26032008.pdf. Acesso em: 14 fev. 2018.

MOTTA, Diego Airoso Da. **Os direitos humanos no jornal nacional e no diário gaúcho: entre a dominação e emancipação.** 34.º ENCONTRO ANUAL DA ANPOCS. ST 08 – DIREITOS HUMANOS, POLÍTICAS E DIVERSIDADE CULTURAL, 2010.

OLIVEIRA, Maria Engel de. **ORKUT: O Impacto da Realidade da Infidelidade Virtual**. Departamento de Psicologia da Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, fev. 2017. Disponível em: https://www.maxwell.vrac.puc-rio.br/9888/9888_4.PDF. Acesso em: 14 fev. 2018.

ORGANIZATION OF AMERICAN STATES. **Cyber Security.** Disponível em: https://www.sites.oas.org/cyber/en/pages/default.aspx. Acesso em: 15 fev. 2018.

PACIEVITCH, Thais. **Geografia da china.** Disponível em: https://www.infoescola.com/geografia/geografia-da-china/ .Acesso em: 17 fev. 2018.

PAYÃO, Felipe**. Entrevista com Anonymous: o que eles querem, fazem e o que são OPs?.** *TECMUNDO.* Disponível em: https://www.tecmundo.com.br/polemica/91540-anonymous-brasil-ops-eles-querem-o-que-eles.htm. Acesso em: 11 fev. 2018.

PAULO, Valdeirton Ventura**. Internet, planejamento, terrorismo e privacidade - Protejam-se!.** Disponível em: http://www.administradores.com.br/artigos/tecnologia/internet-planejamento-terrorismo-e-privacidade-protejam-se/45443/. Acesso em: 4 fev. 2018.

PENA, Rodolfo F. Alves. **Geografia do brasil.** Disponível em: http://brasilescola.uol.com.br/brasil/. Acesso em: 14 fev. 2018.

_____. **Japão.** Disponível em: http://mundoeducacao.bol.uol.com.br/japao/. Acesso em: 17 fev. 2018.

_____. **Principais grupos terroristas da atualidade.** *Brasil Escola.* Disponível em http://brasilescola.uol.com.br/geografia/grupos-terroristas-mundo.htm. Acesso em: 5 fev. 2018

PINHEIRO, Emeline Piva. **Crimes Virtuais: uma análise da criminalidade informática e da resposta estatal.** Pontifice Universidade do Rio Grande do Sul, 2006.Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/emeline.pdf.

PORTAL SÃO FRANCISCO. **Política do egito.** Disponível em: http://www.portalsaofrancisco.com.br/turismo/politica-do-egito. Acesso em: 16 fev. 2018.

POTOTSKI, Dan. **China, rússia e eua discutem métodos de combate ao cibercrime.** Disponível em: https://br.rbth.com/internacional/2013/06/08/china_russia_e_eua_discutem_metodos_de_combate_ao_cibercrime_19709. Acesso em: 17 fev. 2018.

QUEIROZ, Paulo. **Conceito de direito penal.** Disponível em: http://www.pauloqueiroz.net/conceito-de-direito-penal/ Acesso em: fev. 2018

RAPOSO, Henrique. **Parceria Estratégica EUA-Índia: Poder e Identidade no Sistema Inter-Estatal Pós-Atlântico.** Revista Nação & Defesa, p. 91-122, 2007.

RAYMOND, Eric Steven. **How to become a hacker**. Disponível em: http://www.catb.org/esr/faqs/hacker-howto.html. Acesso em: 14 fev. 2018.

REGIONAL NEWS. **Kdka, a primeira rádio comercial do mundo**. Disponível em: https://rnews.com.br/kdka-a-primeira-radio-comercial-do-mundo.html. Acesso em: 11 fev. 2018.

REVISTA GALILEU. **Wikileaks: o que Julian Assange espera alcançar?.** Disponível em: http://revistagalileu.globo.com/Revista/Common/0,,EMI191495-17770,00-WIKILEAKS+O+QUE+JULIAN+ASSANGE+ESPERA+ALCANCAR.html. Acesso em: 4 fev. 2018.

RINCÓN, Maria Luciana. **Você sabe de onde as organizações terroristas tiram tanto dinheiro?.** Disponível em: https://www.megacurioso.com.br/guerras/67286-voce-sabe-de-onde-as-organizacoes-terroristas-tiram-tanto-dinheiro.htm. Acesso em: 11 fev. 2018.

RODRIGUES, Adriano Duarte. **Estratégias de comunicação : Questão comunicacional e formas de sociabilidade.** Artes gráficas Lda, 1990, p. 226.

SALVATO, Fernanda. **De ferdinando a obama: um século de comunicação**. Disponível em: http://agenciatarget2009.blogspot.com.br/2009/11/os-meios-de-comunicacao-na-primeira.html. Acesso em: 11 fev. 2018.

SALGADO, Hugo David Marques. **Código morse: o que é e como surgiu.** Coimbra, Portugal. Disponível em: https://student.dei.uc.pt/~hsalgado/CP/artigo.htm. Acesso em: 10 fev. 2018.

SHARE AMERICA. **Quênia: o centro da inovação da áfrica.** Disponível em: https://share.america.gov/pt-br/quenia-o-centro-da-inovacao-da-africa/. Acesso em: 17 fev. 2018.

SILVA, Ana Karolina da. **O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira.** Âmbito Jurídico, Rio Grande, fev. 2013. Disponível em: http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12778. Acesso em: 16 fev. 2018.

TAIT, Tânia Fátima Calvi. **Evolução da internet: do início secreto à explosão mundial.** Jornal PET Informática, Maringá-Paraná, 01 ago. 2007. 5. Disponível em: http://www.din.uem.br/~tait/evolucao-internet.pdf. Acesso em: 14 fev. 2018.

TAPARELLI, Carlos Henrique Antunes. **A evolução tecnológica do rádio.** Revista USP, São Paulo, 2003. Disponível em: http://www.revistas.usp.br/revusp/article/viewfile/33801/36539. Acesso em: 11 fev. 2018.

TERRA. **Saiba quem é Julian Assange, o criador do site WikiLeaks.** Disponível em: https://www.terra.com.br/noticias/mundo/estados-unidos/saiba-quem-e-julian-assange-o-criador-do-site-wikileaks,9c482ed4f18da310VgnCLD200000bbcceb0aRCRD.html. Acesso em: 2 fev. 2018.

TRUSTED INTRODUCER. **Overiview of TI Processes.** Disponível em: https://www.trusted-introducer.org/processes/overview.html. Acesso em: 20 fev. 2018

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH. **The Cyber Index: International Security Trends and Realities.** Geneva, Mar. 2013. Disponível em: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

UNITED NATIONS GENERAL ASSEMBLY. **A/51/261 – MEASURES TO ELIMINATE INTERNATIONAL TERRORISM.** Ago. 1996. Disponível em: http://undocs.org/A/51/261.

_____. **A/53/576 - Role of science and technology in the context of security, disarmament and other related fields Report of the First Committee.** Nov. 1998. Disponível em: http://undocs.org/A/53/576.

_____. **A/56/533 - Developments in the field of information and telecommunications in the context of international security Report of the First Committee.** Nov. 2001. Disponível em: http://undocs.org/A/56/533.

_____. **A/60/202 - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Report of the Secretary-General.** Ago. 2005. Disponível em: http://undocs.org/A/60/202.

_____. **A/65/154 - Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General.** Jul. 2010. Disponível em: https://undocs.org/A/65/154.

_____. **A/65/201 - Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.** Jul. 2010. Disponível em: https://undocs.org/A/65/201.

_____. **A/66/15 - Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General.** Jul. 2011. Disponível em: https://undocs.org/A/66/152.

_____. **A/68/98 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.** Jun. 2013. Disponível em: https://undocs.org/A/68/98.

_____. **A/70/172 - Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General.** Jul. 2015. Disponível em: https://undocs.org/A/70/172.

_____. **A/70/174 - Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.** Jul. 2015. Disponível em: https://undocs.org/A/70/174.

_____. **A/70/237 - Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455)].** Dez. 2015. Disponível em: https://undocs.org/A/70/237.

_____. **A/71/172 - Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General.** Jul. 2016. Disponível em: https://undocs.org/A/71/172.

_____. **A/C.1/53/INF/1/Add.1 - Documents of the First Committee Note by the Secretariat.** Nov. 1998. Disponível em: http://undocs.org/A/C.1/53/INF/1/Add.1.

_____. **A/RES/53/70 - RESOLUTION ADOPTED BY THE GENERAL ASSEMBLY [on the report of the First Committee (A/53/576)].** Jan. 1999. Disponível em: https://undocs.org/A/RES/53/70.

_____. **A/RES/56/19 - Resolution adopted by the General Assembly**

[on the report of the First Committee (A/56/533)]. Jan. 2002. Disponível em: https://undocs.org/A/RES/56/19.

_____. **A/RES/70/237 - Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455)].** Dez. 2015. Disponível em: https://undocs.org/A/RES/70/237.

UNITED NATIONS OFFICE AT GENEVA. **FACT SHEET: DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY.** Jul. 2015

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS. **Developments in the field of information and telecommunications in the context of international security.** Disponível em: https://www.un.org/disarmament/topics/informationsecurity/. Acesso em: 17 fev. 2018.

UNITED NATIONS STATISTICS DIVISION. **Country profile: Cuba.** Disponível em: http://data.un.org/CountryProfile.aspx?crName=cuba . Acesso em: 19 fev. 2018.

_____. **Country profile: Finland.** Disponível em: http://data.un.org/CountryProfile.aspx?crName=Finland. Acesso em: 13 fev. 2018.

_____. **Country profile: France.** Disponível em: http://data.un.org/CountryProfile.aspx?crName=France. Acesso em: 2 fev. 2018.

_____. **Country profile: Indonesia.** Disponível em: http://data.un.org/CountryProfile.aspx?crName=Indonesia. Acesso em: 12 fev. 2018.

_____. **Country profile: Mexico.** Disponível em: http://data.un.org/CountryProfile.aspx?crName=Mexico. Acesso em: 15 fev. 2018.

_____. **Country profile: Netherlands.** Disponível em: http://data.un.org/CountryProfile.aspx?crName=Netherlands. Acesso em: 16 fev. 2018.

_____. **Country profile: Russian Federation.** Disponível em: http://data.un.org/CountryProfile.aspx?crName=Russian%20Federation. Acesso em: 18 fev. 2018.

_____. **Country profile: Senegal.** Disponível em: http://data.un.org/CountryProfile.aspx?crName=Senegal. Acesso em: 20 fev. 2018

_____. **Country profile: United Kingdom.** Disponível em: http://data.un.org/CountryProfile.aspx?crName=United%20Kingdo. Acesso em: 18 fev. 2018.

_____. **Country profile: United States of America.** Disponível em: http://data.un.org/CountryProfile.aspx?crName=United%20States%20of%20America. Acesso em: 18 fev. 2018.

UOL NOTÍCIAS. **Um mundo invisível: você sabe o que é a famosa "Deep Web"?.** Disponível em: https://tecnologia.uol.com.br/noticias/redacao/2017/11/12/um-mundo-invisivel-o-que-e-a-deep-web.htm . Acesso em: 11 fev. 2018.

_____. **Vários empreendimentos são afetados por ciberataque na Austrália.** Disponível em: https://noticias.uol.com.br/ultimas-noticias/efe/2017/06/28/varios-empreendimentos-sao-afetados-por-ciberataque-na-australia.htm. Acesso em: 11 fev. 2018

UOL VESTIBULAR. **Ciberativismo: ativismo nasce nas redes e mobiliza as ruas do mundo.** Disponível em: https://vestibular.uol.com.br/resumo-das-disciplinas/atualidades/ciberativismo-o-ativismo-da-rede-para-as-ruas-o-ativismo-da-rede-para-as-ruas.htm. Acesso em: 2 fev. 2018.

VEILLARD, Bruno. **O exercício cibernético da OTAN na Estônia.** Disponível em: https://jornal.ceiri.com.br/o-exercicio-cibernetico-da-otan-na-estonia/. Acesso em: 15 fev. 2018.

VICTORIA, Arthur. **Notícias cibernéticas da última semana de novembro de 2017.** Disponível em: https://pt.linkedin.com/pulse/notícias-cibernéticas-da-última-semana-de-novembro-2017-victoria. Acesso em: 11 fev. 2018.

VIDIGAL, Inês Maria Andrade. **As políticas de combate ao cibercrime na europa.** Lisboa, jan. 2012.

XAVIER, Fernanda Ollé. **Episódios da guerra fria: seu início, meio e fim.** Disponível em: http://www.faccrei.edu.br/wp-content/uploads/2016/10/diartigos51.pdf. Acesso em: 07 fev. 2018.