UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM ARQUITETURA E GESTÃO DE INFRAESTRUTURA DE TI

ANDERSON CASTRO DOS SANTOS

CRIMES CIBERNÉTICOS

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2021

ANDERSON CATRO DOS SANTOS

CRIMES CIBERNÉTICOS

Monografia de Especialização, apresentada ao Curso de Especialização em Arquitetura e Gestão de Infraestrutura de TI, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA
2021

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização em Arquitetura e Gestão de Infraestrutura de TI

TERMO DE APROVAÇÃO

CRIMES CIBERNÉTICOS

por

ANDERSON CASTRO DOS SANTOS

Esta monografia foi apresentada em 21 de Dezembro de 2021 como requisito parcial para a obtenção do título de Especialista em em Arquitetura e Gestão de Infraestrutura de TI. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Orientador

_____
Prof. Dr. Joilson Alves Junior
Membro titular

_____
Prof. M. Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho à minha mãe, meu pai, meus irmãos, minha tia que sempre me incentivou com lindas palavras Ir Gorette, a vocês meu muito obrigado, fica aqui registrado minha eterna gratidão, pelo apoio nos momentos em que as palavras de vocês, fizeram meus passos se tornarem firmes.

AGRADECIMENTOS

Certamente estes parágrafos não irão atender a todas as pessoas que fizeram parte dessa importante fase de minha vida. Portanto, desde já peço desculpas àquelas que não estão presentes entre essas palavras, mas elas podem estar certas que fazem parte do meu pensamento e de minha gratidão.

Agradeço ao meu orientador Prof. Dr. Kleber Kendy Horikawa Nabas, pela sabedoria com que me guiou nesta trajetória.

Aos meus colegas de sala.

A Secretaria do Curso, pela cooperação.

Gostaria de deixar registrado também, o meu reconhecimento à minha família, especialmente a minha tia Ir Gorette, pois acredito que sem o apoio deles seria muito difícil vencer esse desafio.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

RESUMO

SANTOS, Anderson Castro dos. **Crimes cibernéticos**. 2021. 34 p. Monografia de Especialização em Arquitetura e Gestão de Infraestrutura de TI, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2021.

Hoje em dia vivemos na era da tecnologia, onde tudo fica mais fácil e mais rápido de ser realizado, tarefas que antes demoravam horas para serem realizadas, hoje em dia podem ser feitas em questões de minutos dependendo da habilidade de quem está operando o computador. Não somente tarefas mais com este avanço da tecnologia conseguimos nos conectar com pessoas no mundo inteiro, saber de notícias praticamente em tempo real entre outras coisas. Porém com esse mundo virtual disponível tão facilmente para todos, infelizmente existem pessoas que tem grande conhecimento destas máquinas e tiram proveito de usuários mais leigos afim de beneficiarem a si mesmos, aplicando golpes e crimes através deste mundo digital. O presente trabalho visa demonstrar quais são estes crimes e como os mesmos são realizados, afim de informar a população.

Palavras-chave: Crimes Cibernéticos. Tecnologia. Crimes. Golpes. Internet.

ABSTRACT

SANTOS, Anderson Castro dos. **Cyber crimes**. 2021. 34 p. Monografia de Especialização em Arquitetura e Gestão de Infraestrutura de TI, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2021.

Nowadays we live in the age of technology, where everything is easier and faster to accomplish, tasks that took hours before, nowadays can be done in minutes depending on the ability of the person who is operating the computer. Not only more tasks with this advancement of technology we can connect with people around the world, know virtually real-time news among other things. But with this virtual world so easily available to everyone, unfortunately there are people who have a great knowledge of these machines and take advantage of more laymen to benefit themselves by applying scams and crimes through this digital world. This paper aims to demonstrate what these crimes are and how they are carried out, in order to inform the population.

Keywords: Cyber Crimes. Technology. Crimes. Scams. Internet.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Pode-se ver que hoje em dia tudo acaba envolvendo tecnologia, e cada vez mais tem-se ela no dia-a-dia, otimizando tarefas, encurtando distâncias com pessoas que estão através do mundo, informações praticamente em tempo real, facilidade nos estudos e até mesmo como lazer. A grande massa da população utiliza os equipamentos eletrônicos que estão conectados na rede mundial da internet, para se comunicar e realizar diversas coisas a todo instante.

1.1 CONSIDERAÇÕS INICIAIS

Com esse grande avanço tecnológico da mesma maneira que acaba facilitando nossas vidas, surgem as ideias em pessoas que querem, prejudicar os demais para tirar proveito da falta de informação destes, e beneficiar a si próprio, ou seja, acabam cometendo crimes virtuais.

1.2 PROBLEMA OBJETO DO TRABALHO

Através deste trabalho, busca-se informar em primeiro momento, quais são os tipos de crimes virtuais que são praticados, esclarecer os conceitos destes variados crimes que são cometidos na rede mundial da internet, com base em uma pesquisa feita frente aos principais autores que relatam sobre estes crimes que ocorrem virtualmente.

1.3 OBJETIVOS

Nesta seção são apresentados os objetivos geral e específicos do projeto, relativos ao problema anteriormente apresentado.

1.3.1 Objetivo Geral

Este trabalho foi efetuado, com base em uma pesquisa bibliográfica a partir de materiais relacionados a este assunto, constituído de artigos científicos disponíveis na internet, revistas, documentos eletrônicos e também livros, visando colher informações sobre quais as características da compreensão dos crimes, frente a conhecer os crimes cibernéticos que existem.

1.3.2 Objetivo Específicos

Para atender ao objetivo geral, neste trabalho de conclusão de curso de especialização, os seguintes objetivos específicos serão abordados:

- Quais os tipos de crimes cibernéticos que existem;
- Conhecer quais os métodos mais realizados;
- Como são realizados estes crimes virtuais;
- Aspectos sobre se existe alguma lei que pode ser utilizada para enquadrar os praticantes destes crimes.

Será demonstrado neste trabalho como a Convenção de Budapeste auxilia no combate dos crimes virtuais por todo o mundo, e também brevemente em como é difícil o trabalho dos peritos forenses e em apurar estes tipos de crimes no ambiente virtual. Esse estudo tem por finalidade realizar uma pesquisa aplicada, uma vez que utilizará conhecimento da pesquisa básica para resolver problemas.

1.4 JUSTIFICATIVA

Para um melhor tratamento dos objetivos e melhor apreciação desta pesquisa, observou-se que ela é classificada como pesquisa exploratória. Detectou-se também a necessidade da pesquisa bibliográfica no momento em que se fez uso de materiais já elaborados: livros, artigos científicos, revistas, documentos eletrônicos e enciclopédias na busca e alocação de conhecimento sobre os crimes como forma de demonstrar como são realizados estes, correlacionando tal conhecimento com abordagens já trabalhadas por outros autores. Como procedimentos, podemos citar a necessidade de pesquisa bibliográfica, isso porque faremos uso de material já publicado, constituído principalmente de artigos e livros, também entendemos como um procedimento importante o estudo de caso como procedimento técnico.

Tem-se como base para o resultado da pesquisa um caso em específico que poderá ser expandido futuramente. O problema foi direcionando a pesquisa para as áreas de conhecer os crimes cibernéticos que existem e ainda a pesquisa como estudo de caso, sendo este com a compreensão dos crimes em uma análise geral como forma de demonstrar como são realizados estes crimes.

2 HISTÓRIA E DESENVOLVIMENTO DO COMPUTADOR

2.1 ORIGEM DO COMPUTADOR

Como pode-se observar os computadores estão presentes na vida das pessoas como nunca, seja no trabalho, em casa, na escola, ou em qualquer outro lugar, as máquinas estão sempre presentes. As tarefas que antes eram realizadas, em um longo prazo, hoje em dia podem ser feitas em pouco tempo.

Charles Babbage, é considerado o pai do computador que tem-se hoje em dia, ele construiu em 1830 o primeiro computador do mundo, cem anos antes de se tornar realidade. O projeto dele acabava apresentando certas desvantagens como por exemplo, o computador precisava ser mecânico e a outra questão é relacionada a engenharia da época em que vivia, devido a mesma ser muito precária. Charles tinha a intenção de cria uma máquina inteligente, com múltiplos propósitos capaz de simular o raciocínio humano.

Desde então começaram a surgir cada vez mais nomes que acabaram de se envolvendo para a criação de computadores. De forma independente o alemão Konrad Zuse e o americano Jhon Atanasoff foram as pessoas que criaram o primeiro computador digital. O americano acabou sendo uma fonte de inspiração para a equipe de outro americano Jhon Mauchly em 1946, onde acabaram criando o ENIAC, o primeiro computador a realizar múltiplas funções, onde por ventura esta construção foi toda financiada pelo governo dos Estador Unidos para uso militar, esta máquina era de uma grande escala visto que a mesma média por volta de 140 metros, pesava cerca de 30 toneladas e era necessário ter pelo menos 5 pessoas para operá-la.

Na década de 60 o cientista visionário, Douglas Engelbart desenvolveu as interfaces de usuário, inclusive mouse e teclado que hoje em dia são indispensáveis para o uso do computador de mesa. A primeira versão que realmente foi possível ser comercializada foi entre as décadas de 70 e 80 quando Steve Jhobs e Steve Wozniak, fizeram o Apple 1. Pouco tempo depois a Xerox lançou um computador pessoal, porém sem sucesso, já no ano seguinte a intel lançou também uma máquina pessoal. Como podemos ver com o passar do tempo estas máquinas estão cada vez mais evoluindo, e cada vez mais rápido.

2.2 SURGIMENTO DA INTERNET

A internet não teve um início diferente, com surgimento na guerra fria, criada com objetivos militares, seria a ferramenta utilizada pelas forças armadas americanas se comunicarem, caso os inimigos destruíssem os meios de comunicações convencionais. Na década de 80 as além da internet ser utilizada pelos militares, ela também foi muito utilizada no meio acadêmico como troca de mensagens entre professores e estudantes (RAMOS, 2020).

Segundo Ramos (2020), na década de 1990 foi a era de grande expansão da internet, onde o engenheiro inglês Tim Bernes-Lee desenvolveu a *World Wibe Web*, onde então foi possível que a grande população pudesse realizar o uso da internet e criar sites de forma mais dinâmica e melhor visualmente. Para então melhorar ainda a experiência do usuário foi realizada a criação dos browsers, ou seja, dos navegadores que temos hoje em dia para facilitar ainda mais o nosso da internet para o usuário. Sem contar que o surgimento dos provedores de acesso e portais, contribuiu também para este crescimento da internet.

Nos dias atuais é praticamente impossível pensar em um mundo sem a internet, visto que a mesma oferece uma séria imensa de facilidades, como por exemplo, comunicação com pessoas através do mundo inteiro, pesquisas escolares e entre outras formas de apoio.

2.3 CRIMES CIBERNÉTICOS

Antes de mais nada é necessário que tenha-se a compreensão da diferença das nomenclaturas mais utilizadas para referenciar os criminosos:

- **Hacker**: acaba sendo o termo mais utilizado, onde referência a aquela pessoa que tem um grande conhecimento, tanto em internet quando em computadores, sempre visando ter mais e mais conhecimento de forma autodidata, sem o devido intuito de prejudicar outra pessoa.
- **Cracker:** é o indivíduo que tem também grande conhecimento em informática e em internet, porém este tem a ideia de prejudicar os demais para que possa ter vantagem para si.

Como pode-se perceber hoje em dia a internet acabou sendo indispensável para todos, visto que tem-se uma imensa facilidade de realizar tarefas que antes tomavam certo tempo hoje, tem-se tudo isso na palma da mão. Tudo isso graças ao grande avanço da internet e tecnologia. Porém sempre tem o lado ruim da história, do mesmo jeito que a tecnologia acaba avançando rapidamente, pessoas com grandes habilidades acabam utilizando estas ferramentas e praticando crimes virtuais, para realizar quebra de sistemas de segurança, de forma ilegal e totalmente sem ética.

Como “Conceito de Crimes Virtuais”, entende-se como crime virtual toda violação de sistema informático, praticado através de um computador, e também logicamente sendo utilizado uma rede, sendo ela corporativa, pública ou privada, onde este elemento acaba invadindo um sistema o qual ele não tem permissão para a sua utilização, tendo como objetivo a subtração, modificação e danificação de dados, para o sistema o qual foi efetuada a invasão.

Segundo Furlaneto Neto e Guimarães(2003): Crime Informático de uma forma bem abrangente significa: “qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados".

Já este outro autor acaba tendo uma visão um pouco mais detalhada sobre o conceito de crime virtual:

> “É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. o „Crime de Informática‟ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.” (ROSA, 2002).

Para Ramalho Terceiro (2005): “os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas”.

Segundo Rossini (2004)**: "**o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade".

Existem diversos nomes que são dados aos crimes são realizados em ambiente virtual, através da utilização de computadores, não existe uma denominação correta, visto que é usado, cybercrimes, crimes virtuais, crimes informáticos, crimes digitais, delitos de informática, fraude de computador, enfim há uma grande diversidade em relação a nomenclatura em relação a este tipo de crime.

2.4 CYBERCRIMES QUE EXISTEM

Os crimes digitais vem acompanhando todo o avanço da tecnologia, o que acaba gerando uma grande preocupação hoje em dia. O alcance da internet de forma global, junto com toda a sua facilidade, baixo custo e o usuário com a possibilidade de se manter anônimo e com grande distância do seu alvo, estes são alguns dos fatores agregam de grande forma para o aumento da prática deste tipo de crime. Mas o que leva aos praticantes destes crimes realizarem tal fato? Segue abaixo alguns exemplos:

- Demonstração de poder: mostrar que a qualquer momento determinada empresa pode ter o seu sistema como um todo, invadido podendo ter uma perca da base de dados de seus clientes por exemplo, com vários tipos de informações sigilosas;
- Prestígio: uma outra forma de mostrar poder, invadindo sites que são relativamente mais difíceis de serem invadidos para então "se gabar", perante os outros crackers, que você conseguiu realizar tal invasão;
- Disputa entre os grupos com a intenção de mostrar que a sua equipe consegue realizar tal feito, antes que as demais equipes;
- Motivações financeiras, com o propósito de roubar dados sigilosos dos demais usuários para ter benefício para si próprio;

- Motivações comerciais, podendo deixar o site de uma empresa que vende produtos através de seu website para que então a sua reputação caia, e não consiga realizar vendas, logo o usuário não irá comprar neste site e irá para a concorrência;
- Motivações ideológicas, por exemplo deixar o site de um jornal, que tem ideias e expressões diferentes da opinião deste grupo / usuário que está realizando o ataque, afim de não propagar as notícias e matérias.

Segundo Furlaneto Neto e Guimarães (2003), os crimes informáticos são classificados como:

- **Crime virtual puro**: qualquer conduta ilícita, a qual atenta o hardware ou software de um computador, ou seja, tanto a parte física quanto a virtual de um computador. Ex: infestação do computador.
- **Crime virtual misto**: utiliza a internet para realizar a conduta ilícita. Com um objetivo diferente. Ex: transações ilegais de valores de contas correntes.
- **Crime virtual comum**: é utilizar a internet apenas como forma de instrumento para realizar em delito que enquadra no código penal, por compartilhamento de dados. Ex: distribuição de conteúdo pornográfico infantil.

Segundo a CERT.br (2012), são crimes virtuais os seguintes:

- **Furto de identidade (*identity theft*)**: ato pelo qual uma pessoa se passar por outra afim de obter certa vantagem. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade. Quanto mais informações nós publicamos nas redes sociais sobre nossas vidas, mais fácil fica para que um golpista furte a nossa identidade, pois temos tantas coisas pessoais publicadas nas redes sociais, que podemos facilmente ter a nossa identidade furtada. Caso a sua identidade for furtada, poderá acarretar com uma série de dados financeiros, perda de crédito e reputação, sem contar na dor de cabeça que poderemos ter até normalizar tudo, sem contar ainda no tempo que irá demorar para comprovar que não foi realmente você que realizou estes atos.
- **Phishing**: é uma maneira desonesta que cybercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Este crime é praticado por meio de

mensagens eletrônicas, seja por sms, e-mail, onde fazem com que você acesse websites falsos, que são idênticos aos reais por exemplo: Você recebe uma mensagem de e-mail do seu banco onde você tem conta, pedindo que seja feito o pagamento de um boleto de valor X, ao acessar o endereço que encontra-se neste e-mail, você é redirecionado para uma página de internet que é igual à do seu banco, porém como você nem desconfia que é um golpe, acaba inserindo os seus dados de acesso corretos, agência, conta inclusive a sua senha bancária. Após realizar tal acesso, é enviado todos estes seus dados para o golpista, então ele terá todas as suas informações e poderá realizar uma transferência do seu dinheiro para a conta dele. Neste mesmo tipo de crime, você poderá receber uma mensagem de e-mail que vai solicitar desta vez que você baixe algum arquivo, você inocentemente baixa o arquivo e o executa em sua máquina, ao executar este arquivo, nele contém um script malicioso onde é instalado um tipo de vírus, que tudo que você digita o golpista recebe uma cópia, ou seja tudo que você acessar, o golpista irá saber, inclusive senhas de e-mails, conversas que você teve e etc. Segundo CERT.br (2012), para se proteger destes crimes é necessário tomar alguns cuidados como por exemplo:

1. seja cuidadoso ao acessar links. Procure digitar o endereço diretamente no navegador Web;
2. questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança;
3. fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links.

- **Pharming**: é um tipo específico de phishing, onde o usuário é redirecionado para outros sites, o golpista realiza o redirecionamento das DNS (domain name system) do site “original”, para um site falso, assim que a vítima entrar com os seus dados de acesso, o golpista terá acesso as informações digitadas no falso site. Para se proteger deste tipo de crime é bem simples, basta ficar atento caso entre em algum site, você seja redirecionado para

outro e que este solicite que seja instalado algum tipo de programa para que você possa prosseguir com a ação desejada, e, sempre verifique ao acessar o seu internet Banking se a conexão do site é segura.

- **Golpe de comércio eletrônico**: Neste tipo de crime o golpista cria um site fraudulento, que após a vítima realizar a compra e o devido pagamento, nunca recebe a mercadoria que deveria ter recebido. Segundo CERT.br (2012), para que se possa evitar cair neste golpe é necessário:
  1. pesquise na Internet sobre o *site*, antes de efetuar a compra, para ver a opinião de outros clientes;
  2. acesse *sites* especializados em tratar reclamações de consumidores insatisfeitos, para verificar se há reclamações referentes a esta empresa;
  3. fique atento a propagandas recebidas através de *spam*
  4. faça uma pesquisa de mercado, comparando o preço do produto exposto no *site* com os valores obtidos na pesquisa e desconfie caso ele seja muito abaixo dos praticados pelo mercado

3 ATAQUES CIBERNÉTICOS

Ataques cibernéticos são ataques realizados aos computadores, visando colher informações e até mesmo prejudicar estes equipamentos. As consequências destes ataques são das mais variadas, onde alguns tem o intuito de roubar informações dos usuários, e outras afim de deixar a máquina vulnerável para outros tipos de ataques, danificar componentes, excluir arquivos e etc. Com base em CERT.br (2012), as técnicas utilizadas pelos golpistas são:

- **Exploração de vulnerabilidade**: Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.
- **Varreduras em redes (*scan*)**: Esta técnica tem o intuito de realizar uma varredura minuciosa na rede afim de identificar os computadores ativos na rede e coltar informações como por exemplo, programas instalados, portas de rede abertas, serviços disponibilizados. Com base nestes dados é possível realizar as possíveis explorações, e realizar uma manutenção preventiva, afim de não deixar brechas para possíveis invasões.
- **Falsificação de e-mail (*e-mail Spoofing*)**: Esta técnica consiste em realizar a alteração dos campos que compõem o cabeçalho do e-mail, afim de parecer que o e-mail foi enviado de um remetente quando, na realidade o e-mail foi enviado pelo golpista.
- **Sniffer**: Uma técnica utilizada para realizar a interceptação de tráfego da rede afim de identificar os dados que passam nela. Neste caso existe dois lados da moeda, podendo ser utilizada por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados. Porém, pode ser usada por por atacantes, para capturar informações sensíveis, como senhas,

números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

- **Negação de serviço (DoS ou DDoS)**: DoS trata-se de uma técnica utilizada onde o “atacante”.

Utiliza um computador para tirar um determinado serviço de operação seja ele um site, um sistema que esteja conectado à internet. Já o DDoS é quanto se trata de um conjunto de computadores que realizam o ataque de forma coordenada e distribuída. Este tipo de ataque não tem como objetivo realizar roubos de dados sigilosos, invasões ou algo do gênero, onde tem como objetivo somente trazer indisponibilidade nos serviços, ou seja, deixá-los fora de operação.

Segundo CERT.br (2012), estes ataques de negação de serviço podem ser realizados por diversos meios, tais como:

- pelo envio de grande quantidade de requisições para um serviço, consumindo os recursos necessários ao seu funcionamento (processamento, número de conexões simultâneas, memória e espaço em disco, por exemplo) e impedindo que as requisições dos demais usuários sejam atendidas;
- pela geração de grande tráfego de dados para uma rede, ocupando toda a banda disponível e tornando indisponível qualquer acesso a computadores ou serviços desta rede;
- pela exploração de vulnerabilidades existentes em programas, que podem fazer com que um determinado serviço fique inacessível.
- *Brute force* (força bruta): Este tipo de técnica refere-se a realizar um ataque através de tentativa e erro, normalmente refere-se a usuário e senha de acessos a sites e sistemas. Todo e qualquer equipamento que tenha usuário e senha e que, esteja conectado a internet pode sofrer este tipo de ataque. O criminoso caso tenha descoberto o seu usuário e senha poderá efetuar ações maliciosas em seu nome, como por exemplo:
  - trocar a sua senha, dificultando que você acesse novamente o *site* ou computador invadido;
  - invadir o serviço de *e-mail* que você utiliza e ter acesso ao conteúdo das suas mensagens e à sua lista de contatos, além de poder enviar mensagens em seu nome;

  - acessar a sua rede social e enviar mensagens aos seus seguidores contendo códigos maliciosos ou alterar as suas opções de privacidade;
  - invadir o seu computador e, de acordo com as permissões do seu usuário, executar ações, como apagar arquivos, obter informações confidenciais e instalar códigos maliciosos.
- *Defacement* (desfiguração da página): Trata-se de uma técnica que consiste em alterar o conteúdo de uma página, as principais formas que um criminoso, neste caso também chamado de *defacer*, pode utilizar para desfigurar uma página *Web* são:
  - explorar erros da aplicação *Web*;
  - explorar vulnerabilidades do servidor de aplicação *Web*;
  - explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação *Web*;
  - invadir o servidor onde a aplicação *Web* está hospedada e alterar diretamente os arquivos que compõem o *site*;
  - furtar senhas de acesso à interface *Web* usada para administração remota.
- Vírus: São programas desenvolvidos para alterar, softwares instalados no computador, podendo se anexar em qualquer arquivo que tenha em seu computador, podendo também onde ao você efetuar uma cópia de arquivos para um pen-drive, por exemplo, ele se alocar neste pen-drive e consequentemente ir infectando mais e mais usuários. O vírus de computador se espalha assim como o vírus biológico. Porém a grande diferença é que o vírus precisa da ação do usuário para que então, ele se aloque no sistema/computador.
- *Bugs* (falhas de segurança): Todos software, sistemas operacionais e programas no geral, são criados por seres humanos e podem acabar tendo algumas falhas, onde quando alguém com intenções maliciosas descobre estas falhas, pode acabar abusando delas e infectando a máquina do usuário, normalmente sem que o usuário nem se quer note que está infectado.

- *Trojan* (Cavalo de troia): Este *malware*, é um tipo de programa malicioso disfarçado, que ao ser baixado e instalado pelo usuário, onde ele acha que é pra uma finalidade, na realidade trata-se uma ameaça. Este tipo de programa por si só, não se replica e não infecta as demais máquinas que encontram-se na rede, normalmente, fica alocado somente na máquina que foi instalado, coletando informações ou até mesmo configurando brechas na segurança da máquina para que então possa ser invadida.
- *Worms* (vermes): Trata-se de uma praga, onde se replica e infecta a rede como um todo, ou seja se propaga de forma muito rápida. Este tipo de malware diferente do vírus não precisa da ação do usuário para se alocar na máquina, ou seja é um programa completo com grande força de auto propagação.
- *Exploit*: São uma sequência de comandos, que são elaborados por crackers que tiram proveito de uma vulnerabilidade de determinado software que esteja instalado no alvo. Os objetivos dos exploits é causar um comportamento acidental ou imprevisto em determinada aplicação, caso um cracker tenha sucesso com esta técnica ele poderá ter acesso aos processos de seu alvo e conseguir total domínio sobre o mesmo.

4 CRIMES NA INTERNET

4.1 EXPLORAÇÃO SEXUAL DE C RIANÇAS E ADOLECENTES

Com o grande avanço da internet também aumentou lamentavelmente o índice que este crime acaba ocorrendo, visto que graças ao anonimato que o usuário pode conseguir na internet, pessoas podem acabar estimulando este tipo de comportamento doentio pois não está se expondo no ‘mundo real”. Sem contar ainda que a facilidade que os pedófilos têm em se organizar e também de ter contato com as suas vítimas sem se expor, ficou bem grande com a internet. Com este avanço tecnológico, ficou ainda mais fácil a distribuição de materiais seja ele comercializado ou gratuito.

Não somente a distribuição deste tipo de materiais como vídeos, imagens com conteúdo de exploração sexual de menores é crime, mais também quem produzir, reproduzir, dirigir, fotografar, filmar ou registrar através de qualquer meio, envolvendo crianças e adolescentes o infrator será punido conforme o artigo 240 do ECA (Estatuto da Crianças e do Adolescente). Segue abaixo o referido artigo:

> Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.
>
> **Art. 240.** Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
>
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)
>
> **§ 1o** Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena. (Redação dada pela Lei nº 11.829, de 2008)
>
> **§ 2o** Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime: (Redação dada pela Lei nº 11.829, de 2008)
>
> **I** – no exercício de cargo ou função pública ou a pretexto de exercê-la; (Redação dada pela Lei nº 11.829, de 2008)
>
> **II** – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou (Redação dada pela Lei nº 11.829, de 2008)
>
> **III** – prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento. (Incluído pela Lei nº 11.829, de 2008)

5 CONVENÇÃO DE BUDAPESTE

Em 23 de Novembro de 2001, ocorreu uma convenção organizada pelo COE (*Council of Europe* – Conselho da Europa), em Budapeste – Hungria, a devida convenção trata-se de um tratado internacional afim de definir os crimes praticados através da internet e as devidas formas de persecução, que nada mais é a soma de investigação preliminar junto com a devida ação penal. Em resumo a convenção trata da real necessidade da cooperação internacional, com relação a extradição e da assistência mútua entre os Estados, informação espontânea, procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis além da definição da confidencialidade e restrição de utilização.

Vale ressaltar o artigo 22, desta convenção que visa não dizer como deve ser as regras, onde somente deseja orientar sobre como deve ser realizado os procedimentos sobre esta era de cybercrimes:

> Art. 22 – Competência: 1. Cada parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer à competência relativamente a qualquer infração penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infração seja cometida: a) no seu território; b) a bordo de um navio; c) a bordo de aeronave matriculada nessa parte e segundo as suas leis; ou d) por um dos seus cidadãos nacionais, se a infração for punível criminalmente onde foi cometida ou se a infração não for de competência territorial de nenhum Estado. 2. Cada parte pode reservar-se o direito de não aplicar ou de apenas aplicar em casos ou condições específicas as regras de competência definidas no nº 1, alínea b à d do presente artigo ou em qualquer parte dessas alienas; 3. Cada parte adotará medidas que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infração referida no artigo 24, nº1 da presente convenção, quando o presumível autor da infração se encontre no seu território e não puder ser extraditado para outra Parte, apenas com base na sua nacionalidade, após um pedido de extradição. 4. A presente convenção não exclui qualquer competência penal exercida por uma Parte sem conformidade com seu direito interno. 5. Quando mais que uma Parte reivindique a competência em relação à uma presumível infração prevista na presente Convenção, as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal. (CONVENÇÃO DE BUDAPESTE, 2012, p. 14).

A como um todo contém 48 Artigos de fácil entendimento. A convenção foi ratificada por 61 países com pode-se observar na Figura 1, retiradas do próprio site do COE, ilustrado no ano de 2018.

Figura 1 – Convenção em crimes cybernéticos

(continua)

Title	Convention on Cybercrime
Reference	ETS No.185
Opening of the treaty	Budapest, 23/11/2001 - Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States
Entry into Force	01/07/2004 - 5 Ratifications including at least 3 member States of the Council of Europe

☑State who signed ☑State who ratified ☑State who neither signed nor ratified ☑State who suspended ☑State who denounced

	Signature	Ratification	Entry into Force	Notes	R.	D.	A.	T.	C.	O.
Members of Council of Europe										
Albania	23/11/2001	20/06/2002	01/07/2004				A.			
Andorra	23/04/2013	16/11/2016	01/03/2017		R.	D.	A.			
Armenia	23/11/2001	12/10/2006	01/02/2007				A.			
Austria	23/11/2001	13/06/2012	01/10/2012		R.	D.	A.			
Azerbaijan	30/06/2008	15/03/2010	01/07/2010		R.	D.	A.	T.		
Belgium	23/11/2001	20/08/2012	01/12/2012		R.	D.	A.			
Bosnia and Herzegovina	09/02/2005	19/05/2006	01/09/2006				A.			
Bulgaria	23/11/2001	07/04/2005	01/08/2005		R.	D.	A.			
Croatia	23/11/2001	17/10/2002	01/07/2004				A.			
Cyprus	23/11/2001	19/01/2005	01/05/2005				A.			
Czech Republic	09/02/2005	22/08/2013	01/12/2013		R.	D.	A.			
Denmark	22/04/2003	21/06/2005	01/10/2005		R.		A.	T.		
Estonia	23/11/2001	12/05/2003	01/07/2004				A.			
Finland	23/11/2001	24/05/2007	01/09/2007		R.	D.	A.			
France	23/11/2001	10/01/2006	01/05/2006		R.	D.	A.			
Georgia	01/04/2008	06/06/2012	01/10/2012			D.				
Germany	23/11/2001	09/03/2009	01/07/2009		R.	D.	A.			
Greece	23/11/2001	25/01/2017	01/05/2017		R.	D.	A.			
Hungary	23/11/2001	04/12/2003	01/07/2004		R.	D.	A.			
Iceland	30/11/2001	29/01/2007	01/05/2007		R.		A.			
Ireland	28/02/2002									
Italy	23/11/2001	05/06/2008	01/10/2008				A.			
Latvia	05/05/2004	14/02/2007	01/06/2007		R.		A.			
Liechtenstein	17/11/2008	27/01/2016	01/05/2016		R.	D.	A.			
Lithuania	23/06/2003	18/03/2004	01/07/2004		R.	D.	A.			
Luxembourg	28/01/2003	16/10/2014	01/02/2015				A.			
Malta	17/01/2002	12/04/2012	01/08/2012			D.				
Monaco	02/05/2013	17/03/2017	01/07/2017				A.			
Montenegro	07/04/2005	03/03/2010	01/07/2010	55	R.		A.			
Netherlands	23/11/2001	16/11/2006	01/03/2007				A.	T.		
Norway	23/11/2001	30/06/2006	01/10/2006		R.	D.	A.			
Poland	23/11/2001	20/02/2015	01/06/2015		R.		A.			
Portugal	23/11/2001	24/03/2010	01/07/2010			D.	A.			
Republic of Moldova	23/11/2001	12/05/2009	01/09/2009			D.	A.	T.		
Romania	23/11/2001	12/05/2004	01/09/2004				A.			
Russian Federation										
San Marino	17/03/2017									
Serbia	07/04/2005	14/04/2009	01/08/2009	55			A.			
Slovak Republic	04/02/2005	08/01/2008	01/05/2008		R.	D.	A.			
Slovenia	24/07/2002	08/09/2004	01/01/2005				A.			
Spain	23/11/2001	03/06/2010	01/10/2010			D.	A.			
Sweden	23/11/2001									
Switzerland	23/11/2001	21/09/2011	01/01/2012		R.	D.	A.			
The former Yugoslav Republic of Macedonia	23/11/2001	15/09/2004	01/01/2005				A.			
Turkey	10/11/2010	29/09/2014	01/01/2015							
Ukraine	23/11/2001	10/03/2006	01/07/2006		R.	D.	A.			
United Kingdom	23/11/2001	25/05/2011	01/09/2011		R.		A.			

Figura 1 – Convenção em crimes cybernéticos

(conclusão)

Non-Members of Council of Europe										
	Signature	Ratification	Entry into Force	Notes	R.	D.	A.	T.	C.	O.
Argentina		05/06/2018 a	01/10/2018		R.		A.			
Australia		30/11/2012 a	01/03/2013		R.		A.			
Cabo Verde		19/06/2018 a	01/10/2018				A.			
Canada	23/11/2001	08/07/2015	01/11/2015		R.	D.	A.			
Chile		20/04/2017 a	01/08/2017		R.	D.	A.			
Colombia				4						
Costa Rica		22/09/2017 a	01/01/2018			D.	A.			
Dominican Republic		07/02/2013 a	01/06/2013			D.	A.			
Ghana				4						
Israel		09/05/2016 a	01/09/2016		R.		A.			
Japan	23/11/2001	03/07/2012	01/11/2012		R.	D.	A.			
Mauritius		15/11/2013 a	01/03/2014				A.			
Mexico										
Morocco		29/06/2018 a	01/10/2018				A.			
Nigeria				4						
Panama		05/03/2014 a	01/07/2014				A.			
Paraguay		30/07/2018 a	01/11/2018				A.			
Peru				4						
Philippines		28/03/2018 a	01/07/2018				A.			
Senegal		16/12/2016 a	01/04/2017				A.			
South Africa	23/11/2001									
Sri Lanka		29/05/2015 a	01/09/2015		R.		A.			
Tonga		09/05/2017 a	01/09/2017				A.			
Tunisia				4						
United States of America	23/11/2001	29/09/2006	01/01/2007		R.	D.	A.			

Total number of signatures not followed by ratifications	4
Total number of ratifications/accessions	61

Fonte: Autoria própria.

Como pode-se ver o Brasil não ratificou esta convenção que em vigor em 01 de julho de 2004. Porém logo a seguir, apresentaram-se mais alguns novos paizes, incluindo o Brasil: África do Sul, Andorra, Argentina, Armenia, Austrália, Austria, Azerbaijão, Bélgica, Benin, Bésnia e Herzegovina, Brasil, Bulgária, Burkina Faso, Cabo Verde, Canadá, Chile, Colômbia, Costa Rica, Croácia, Chipre, República Checa, Dinamarca, República Dominicana, Estónia, Finlândia, França, Geórgia, Alemanha, Gana, Grécia, Guatemala, Hungria, Islândia, Irlanda, Israel, Itália, Japão, Letónia, Liechtenstein, Lituânia, Luxemburgo, Malta, Maurícias, República da Moldávia, Monaco, Montenegro, Marrocos, Holanda, Macedônia do Norte, México, Nigéria, Noruega, Panamá, Paraguai, Peru, Filipinas, Polônia, Portugal, Romênia, San Marino, Senegal, Sérvia, República Eslovaca, Eslovênia, Espanha, Sri Lanka, Suíça, Tonga, Turquia, Ucrânia, Reino Unido, Estados Unidos da América, Suécia e Tunísia.

6 INVESTIGAÇÃO DOS CYBERCRIMES

Pode-se verificar como demonstrado nos capítulos anteriores deste trabalho, a imensa quantidade de crimes e ameaças que existem e que são praticados através de um sistema eletrônico que se encontra conectado à internet. E como é realizado o trabalho de um perito afim de capturar essas pessoas que praticam os crimes? Logo abaixo iremos demonstrar brevemente como é feito este trabalho.

Todo crime é feito através da internet, logo ao acessar a rede mundial tem-se um *Internet Protocol* (IP, protocolo de internet). Segundo Pisa (2012),

> "O IP (Internet Protocol) é o principal protocolo de comunicação da Internet. Ele é o responsável por endereçar e encaminhar os pacotes que trafegam pela rede mundial de computadores. Pacotes são os blocos de informações enviados na Internet e podem ser considerados como as cartas enviadas pelo serviço de correios. Os pacotes da Internet são divididos em duas partes: o cabeçalho, que, como um envelope, possui as informações de endereçamento da correspondência, e dados, que é a mensagem a ser transmitida propriamente dita".

Quando acessa-se um site, entra-se em uma rede social, em um bate-papo, envia-se um e-mail tudo isso tem associado o endereço IP da máquina que o usuário está utilizando, ou seja, tudo fica armazenado e pode ser rastreado, lembrando que não tem como 2 máquinas diferentes utilizarem o mesmo endereço IP simultaneamente. Logo pode-se concluir que caso o perito forense tenha em mãos o endereço IP, existe uma grande possibilidade de conseguir rastrear esta conexão e conseguir identificar o infrator. As informações de quem usou o endereço IP em um determinado dia e horário são requisitadas pela Justiça ao provedor de acesso responsável pela a faixa de IP identificada, que fornece o log de dados com as informações exigidas.

Outra informação de suma importância para o perito forense, é o log de dados, é nada mais nada menos que um registro das atividades do software, como por exemplo qual usuário acessou o sistema e qual horários, através de qual endereço IP o usuário acessou o sistema, quais os comandos que foram utilizados, erros, acesso a um recurso do sistema, se algo foi alterado no software, ou seja é um arquivo onde mostra tudo que ocorreu no sistema.

Segundo Wendt e Jorge (2013), pode-se dividir a investigação de crimes cibernéticos em duas fases: a) fase de técnico; e b) fase de campo.

A fase técnica trata-se do primeiro ato como assim podemos dizer, ou seja quando a vítima realiza a denúncia do crime que foi cometido com a sua pessoa, onde então a equipe realizar uma série de análises realizando o levantamento de evidências como por exemplo se o crime foi cometido através de chats, grupos fóruns e etc, para então assim verificar quais o métodos que serão necessários para realizar na investigação, então é iniciado os atos administrativos como assim podemos dizer, ou seja é feito o boletim de ocorrência e com base nas análises realizadas nos dados obtidos é solicitado se for o caso, a autorização judicial para a quebra de sigilo, ou seja é solicitado para os logs e dados para os provedores de acesso.

Após todos os levantamentos necessários realizados entra a segunda fase que é a fase de campo, é nesta fase que envolve os agentes que com toda a análise e dados coletados na investigação em mãos é feita a apreensão dos equipamentos utilizados, lembrando que caso aja a apreensão é necessário ter em mãos o mandado judicial.

6.1 COMPUTAÇÃO FORENSE

Com o grande volume de crimes digitais ocorrendo durante os últimos anos, algumas empresas viram uma grande oportunidade de negócio, onde empresas fornecem produtos afim de auxiliar as autoridades com a utilização e comprovação de provas digitais visando constatar realmente um crime digital.

Segundo Freitas (2006):

> “A perícia forense computacional aplicada à informática, também referenciada como computação forense, forense computacional, criminalística computacional, forense digital, investigação eletrônica, é a aplicação de conhecimentos em informática e técnicas de investigação com a finalidade de obtenção de evidências. (…) tornou-se uma prática investigativa importante tanto para as empresas quanto para polícia. Utiliza métodos científicos para identificar, preservar, analisar e documentar evidências localizadas em computadores e outros dispositivos eletrônicos”.

Para provar os fatos ocorridos com a maior clareza possível, o perito digital deve trabalhar de forma sistemática e cuidadosa com as evidências no intuito de preservar a integridade dos dados e detalhar toda a atividade executada no laudo final (PEREIRA, 2010).

O processo pericial na computação forense é divido em quatro etapas segundo (KENT *et al.*, 2006):

1. **Coleta de dados**: identifica as potenciais fontes de dados e a aquisição de dados a partir delas.
2. **Exame de dados**: envolve a avaliação e a extração das informações relevantes a partir dos dados coletados. Pode não ser uma tarefa fácil, longe disso. Um disco rígido apreendido para a investigação pode conter centenas de milhares de arquivos de dados. Identificar os arquivos que realmente contêm informações de interesse à investigação, incluindo aquelas ocultas, necessita do auxílio de ferramentas e técnicas para o exame dos dados.
3. **Análise de dados**: uma vez que a informação relevante foi extraída, o analista deve estudar e avaliar os dados para tirar suas conclusões.
4. **Laudo**: a última etapa consiste na elaboração e apresentação de um relatório contendo, detalhadamente, os procedimentos e as ferramentas utilizados na investigação e que garantiram a integridade dos dados, bem como o que foi encontrado e interpretado nos dados analisados.

Como pode-se notar que é necessário um grande conhecimento técnico para realizar a investigação de crimes digitais, visto que existe uma grande quantidade de dados que precisam ser analisados, diversos procedimentos e técnicas que são difíceis de rastrear, isso tudo aumenta no tempo da investigação isso ainda sem contar que a mesma pode ficar financeiramente inviável.

Visto que existe uma vasta quantidade de técnicas que os criminosos podem se camuflar, afim de se manter anônimo na internet e realizar a prática dos crimes, porém temos profissionais que estão se capacitando cada vez mais buscando mais conhecimento e novas técnicas afim de ajudar a sociedade no combate destes crimes. Ainda assim podemos ver que como temos a internet a informação pode ser propagada de forma mais rápida, onde usuários podem buscar o conhecimento e ver como são realizados estes crimes, tendo certo conhecimento, pelo menos o básico dos mesmos, e cada vez mais propagar este tipo de informação, afim de conscientizar os demais internautas a não caírem nestes crimes que são praticados através do mundo digital, com isso podemos ter certeza que pelos menos o índice destes crimes irá diminuir.

7 CONCLUSÃO

Na presente pesquisa procurou-se demonstrar quais são os cybercrimes mais cometidos, quais as características destes e também como eles são realizados, afim de demonstrar para a população em geral e compreensão dos cybercrimes.

Com base nesta pesquisa ficou claro que existe uma grande variedade dos crimes que podem ser feitos através do computador, onde a cada dia cresce mais e mais o número de golpistas, visto que como a internet trata-se de uma grande rede mundial, fica relativamente fácil de se manter “anônimo” e realizar estes crimes virtuais. Podemos notar que da mesma maneira que a tecnologia avança os criminosos acabam tendo mais e mais conhecimento para propagar os seus golpes, seja realizando prática de roubo de dados através de vírus, criação de sites falsos de grandes e conhecidos bancos, onde a vítima acaba achando que é o site do banco em questão e digita sua conta, senha e todos os seus dados e infelizmente acaba tendo grandes transtornos financeiros, tudo isso pela falta de conhecimento de como são feitos estes tipos de crimes.

Nesta pesquisa também foi mencionado a triste questão da pedofilia infantil, onde com a internet esta prática acabou aumentando devido ao anonimato, com grande divulgação de imagens e vídeos de crianças sendo aliciadas. Ainda podemos mencionar que com a tecnologia ficou mais fácil de o pedófilo ter contato com as suas vítimas iludindo-as atrás de uma tela de computador, sem ter que se expor totalmente.

Com este trabalho ficou claro que ainda existe uma grande falha em relação a punição para os praticantes destes crimes, visto que não existe uma legislação específica para tais, onde é realmente necessário que seja trabalhado em cima desta questão, visto que a tendência é de cada vez mais aumentar tais práticas citadas. Apesar de ter sido citado a Convenção de Budapeste nem todos os países do mundo ratificaram e assinaram a mesma.

Pode-se notar também que o trabalho dos peritos forenses é árduo para obtenção de provas concretas, para que possam ser relevantes o suficiente e que realmente levem ao praticante dos crimes.

REFERÊNCIAS

CERT.br. **Cartilha de Segurança para Internet**, versão 4.0 / Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) – São Paulo: Comitê Gestor da Internet no Brasil (CGI.br), 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 15 nov. 2021.

ETS No. 185. **Convention on cybercrime**. Copyright© Council of Europe, Budapest, 23 nov. 2001. Disponível em: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>. Acesso em: 11 nov. 2021.

FREITAS, Andrey Rodrigues de. **Perícia Forense aplicada a informática**. 1. ed. Rio de Janeiro: Brasport, 2006.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. **Crimes na internet:** elementos para uma reflexão sobre a ética informacional. Revista CEJ, v. 67, N. 20, jan-mar/2003. Disponível em: <https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/523>. Acesso em: 15 nov. 2021.

KENT, K. *et al*. **Guide to integrating forensic techniques into incident response**: recomendations of the National Institute of Standards and Technology. Special publication. Gaithersburg: NIST, 2006.

PEREIRA, Evandro Della Vecchia. **Investigação digital**: conceitos, ferramentas e estudos de caso. III Congresso Tecnológico TI e Telecom InfoBrasil 2010, Fortaleza, mai. 2010.

PISA, Pedro. **O que é IP?** Copyright© Globo Comunicações e Participações S.A. techtudo, publicado em: 07 mai. 2012. Disponível em: <https://www.techtudo.com.br/noticias/2012/05/o-que-e-ip.ghtml>. Acesso em: 25 nov. 2021.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes virtuais**. 2005. Disponível em:<http://www.advogadocriminalista.com.br>. Acesso em: 27 nov. 2021.

RAMOS, Jefferson Evandro Machado. **História da internet**. Copyright ©SuaPesquisa.com, publicado em: 02 set. 2020. Disponível em: <https://www.suapesquisa.com/internet/>. Acesso em: 17 nov. 2021.

ROSA, Fabrízio. **Crimes de informática**. Campinas: Bookseller, 2002.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

WENDT, Emerson; JORGE, Higor V. N. **Crimes cibernéticos**: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2013.