IBMEC – Centro
Trabalho do Curso de Direito da
Disciplina Programação e Direito

Crimes Cibernéticos

Bernardo Pessanha Torres
Giovanna Montenegro Vicente de Sousa
João Vicente Benigno Araújo da Silva
Lorenzo de Almeida
Natan Xavier
Nicolas Quaresma

Rio de Janeiro
2024.2

1. INTRODUÇÃO

1.1 O Que São os Crimes Cibernéticos?

A cibernética é a "ciência abrangente dos sistemas informativos e, especificamente, dos sistemas de informação". Portanto, através do conceito analítico de crime, pode-se concluir que "crimes cibernéticos" englobam todas as ações típicas, antijurídicas e culpáveis realizadas contra ou com o uso de sistemas de informática. Pode-se dizer ainda que é o uso de um sistema de informática para prejudicar um bem ou interesse juridicamente resguardado, seja ele da ordem econômica, da integridade física, da liberdade individual, da privacidade, da honra, do patrimônio público ou privado, da Administração Pública, entre outros.

Os crimes cibernéticos mais comuns são os crimes cibernéticos de espionagem, de ataques e de fraude, além de práticas de alta incidência como o phishing, ransomware e cyberbullying. Ademais, os crimes cibernéticos cada vez mais adentram a preocupante área da pedofilia, com a disseminação de conteúdo pornográfico infantil.

1.2 Contexto Histórico dos Crimes Cibernéticos.

A prática dos crimes cibernéticos passa por uma transformação à medida que nos aproximamos da atualidade, já que em seus primórdios, os crimes cibernéticos eram praticados por indivíduos altamente especializados. Entretanto, com a evolução e ampliação do acesso às tecnologias, esses crimes passaram a ser praticados também por pessoas comuns.

Em relação aos antecedentes históricos, pode-se afirmar que os primeiros casos de crimes informáticos surgiram na década de 1960. Esses crimes consistiam em manipular, sabotar, espionar ou abusar excessivamente de computadores e sistemas. Então, somente a partir de 1980 ocorreu um crescimento nas atividades criminosas, que se manifestaram em ações como manipulação de caixas bancários, abusos de telecomunicações, pirataria de software e pornografia infantil.

Durante o período mencionado, a prática intensa de delitos cibernéticos gerou as primeiras leis que regulavam a execução desses atos ilegais. Em 1984, os Estados Unidos da América estabeleceram a legislação "Crime Control Act", seguida pelo "Computer Fraud and Abuse Act" em 1986. Em 1986, a Alemanha aprovou a Lei "Computer Kriminalitat", que foi seguida pela França, que, em 1988, aprovou a Lei Godfraud. Em 1995, a Espanha incorporou delitos de informática na reformulação do seu Código Penal.

O conceito de "cibercrime" emergiu em Lyon, na França, durante um encontro de um subgrupo dos países do G8 que estudou e debateu os delitos cometidos através de dispositivos eletrônicos ou através da propagação de informações na internet. Isso ocorreu no final dos anos 90, época em que a Internet se espalhou pelos países da América do Norte. O grupo, conhecido como "Grupo de Lyon", empregou o termo de maneira bastante abrangente para caracterizar todos os tipos de delitos cometidos na internet ou nas novas redes de telecomunicações, que se tornaram cada vez mais acessíveis a um grande número de usuários.

No dia 23 de novembro de 2001, o Conselho da Europa (Council of Europe) estabeleceu a Convenção Europeia sobre Crimes Cibernéticos, com o propósito de padronizar a legislação europeia em relação à política criminal de crimes cibernéticos. Nesse período, o tópico ganha força na legislação brasileira, com a primeira lei n° 9883 sendo promulgada no ano 2000, tratando de cibercrimes em aspectos gerais. A temática já havia sido abordada nos anos 1987 e 1990, mas com caráter econômico e não cibernético.

2. TIPOS E CLASSIFICAÇÕES DOS CRIMES CIBERNÉTICOS

2.1 Crimes Cibernéticos mais Comuns

Como os mais comuns tipos de crimes cibernéticos, pode-se citar, clonagem de número e WhatsApp, produção de boletos falsos, fraudes bancárias, comércios virtuais ilegais, leilões e empréstimos falsos, crimes contra a honra (difamação, exibição de fotos íntimas), roubo e sequestro de dados, etc.

2.2 Principal Classificação dos Crimes Cibernéticos

A Principal classificação dos Crimes Cibernético os divide em: **Crime Cibernético Próprio** e **Crime Cibernético Impróprio**. A primeira classificação trata-se dos crimes que só podem ser praticados no mundo digital, como o ataque de vírus e malware, ou seja, não causam danos diretos ao mundo real. Já a segunda classificação, corresponde à quando se são utilizados recursos informáticos para auxiliar o autor ao cometimento dos delitos, no entanto não depende somente deste meio para a efetivação do crime cometido. Mesmo assim, pode ocasionar até em um crime de homicídio, quando, por exemplo, através de dados de informações sobre medicação, um agente de forma ilícita acessa uma rede de informática de determinado

estabelecimento hospitalar, induzindo os profissionais de saúde a medicarem o paciente com uma dosagem elevada, levando o mesmo ao óbito.

2.3 **Outras Classificações Possíveis dos Crimes Cibernéticos**

Outro tipo de classificação possível de ser realizada entre os Crimes Cibernéticos é a divisão entre **Crime Cibernético Comum, Puro ou Misto**. Os Crimes Cibernéticos Comuns são crimes que utilizam a internet como instrumento para realizar um delito que enquadra no Código Penal, como a distribuição de conteúdo pornográfico infantil.

Já os Crimes Cibernéticos Puros são similares aos próprios, pois trata-se de condutas ilícitas que atingem o hardware e/ou software de um computador, sem danos diretos ao mundo real. Por fim, os Crimes Cibernéticos Mistos são aqueles similares aos impróprios, são condutas ilícitas que utilizam a internet para um objetivo diferente do crime virtual puro, como o furto eletrônico a contas bancárias online, assim, profere danos ao mundo externo às telas.

3. **LEGISLAÇÃO BRASILEIRA ACERCA DOS CRIMES CIBERNÉTICOS**

3.1 Lei Carolina DieckMann (Lei 12.737/2012)

A lei n° 12.737/2012 foi o principal marco inicial na tutela jurisdicional dos crimes cibernéticos. Ela inovou o ordenamento jurídico à medida em que tipificou novos delitos em seu texto, ampliando a legislação sobre crimes virtuais.

Antes da promulgação dessa lei, muitas práticas ilícitas no meio virtual, como invasão de dispositivos, a divulgação não autorizada de dados pessoais, entre outros crimes, ficava à margem da legislação penal tradicional, que não estava suficientemente preparada para lidar com os desafios impostos pela internet.

A norma pioneira é nomeada em homenagem a atriz brasileira Carolina DieckMann, que teve seu computador pessoal invadido e diversas fotos íntimas foram divulgadas em redes sociais após a artista não ceder à extorsão dos criminosos.

A lei teve o mérito de chamar a atenção para a vulnerabilidade das pessoas frente a crimes digitais, demonstrando a necessidade urgente de regulamentação específica para o ambiente online. O incidente envolvendo a atriz foi apenas um dos muitos casos que expuseram a fragilidade das vítimas diante da disseminação de imagens e informações pessoais sem

consentimento, o que gerou um movimento de conscientização e mobilização pela criação de normas mais rigorosas.

3.2 Marco Civil da Internet (Lei 12.965/2014)

O "Marco Civil da Internet" surgiu da fusão de diversos projetos semelhantes, que ganharam relevância principalmente devido às revelações de espionagem do Governo dos Estados Unidos contra o Brasil e outros países. Portanto, em 23 de abril de 2014, a presidente Dilma Rousseff sancionou a Lei número 12.695/2014, que define princípios, garantias, obrigações e direitos para os usuários da internet.

Essa lei possui cinco capítulos, sendo os dois primeiros os mais pertinentes ao presente debate. O primeiro capítulo da referida lei estabelece conceitos, princípios, direitos e responsabilidades para o uso da internet em todo o território nacional, além de estabelecer orientações para a atuação do governo no assunto. No segundo capítulo, trata-se dos direitos e garantias dos usuários, garantindo a proteção da sua privacidade e vida privada. Além disso, garante-lhes o direito a informações claras e exatas sobre as políticas de utilização dos sites, provedores e redes sociais.

3.3 Lei Geral de Proteção de Dados (Lei 13.709/2018)

Em face do aumento da ameaça de delitos cibernéticos, a Lei Geral de Proteção de Dados (LGPD) estabeleceu regras e orientações cruciais para a coleta, guarda e utilização apropriada dos dados pessoais do povo brasileiro. Os propósitos centrais da LGPD são aprimorar a transparência, a segurança e a privacidade no processamento de dados pessoais, além de fornecer orientações para a identificação dos autores de delitos digitais.

Através dessa legislação, podemos implementar medidas de proteção relacionadas à privacidade e informações confidenciais, com o objetivo de reprimir delitos cibernéticos e o uso impróprio de informações confidenciais. A legislação define normas para a proteção de dados pessoais, proporcionando um maior controle a respeito da infraestrutura e dos processos de segurança. Isso implica que as organizações devem cumprir a lei para prevenir danos éticos, jurídicos e financeiros.

3.4 Lei 14.155/2021

A Lei 14.155 de 2021, promulgada em 28 de maio de 2021, alterou e incorporou alguns artigos do Código Penal e do Código de Processo Penal, introduzindo mudanças nos delitos

de invasão de dispositivos informáticos, furto através de fraude eletrônica, estelionato através de fraude eletrônica, entre outros tópicos pertinentes.

3.5 Lei 14.132/2021

A Lei 14.132, promulgada em 31 de março de 2021, introduziu um novo artigo no Código Penal. 147-A, também conhecido como "crime de perseguição". A instituição deste tipo penal visa proteger a liberdade pessoal contra crimes praticados na internet, com o objetivo de constranger a vítima através da violação de sua privacidade.

4. GUERRA CIBERNÉTICA

A guerra cibernética é uma nova e intrincada faceta dos conflitos globais, que envolve a utilização de ataques cibernéticos contra sistemas vitais para debilitar e desestabilizar uma nação. Esta modalidade de conflito utiliza a interconexão e a crescente dependência de tecnologias de informação e comunicação para prejudicar a infraestrutura de nações, corporações e até indivíduos. Ao contrário da guerra convencional, a guerra cibernética pode acontecer sem a intervenção física de forças militares, empregando ferramentas tecnológicas como malware, vírus, ataques de negação de serviço (DDoS) e hacking para alcançar seus propósitos. Na guerra cibernética, frequentemente a motivação é de caráter político e estratégico, podendo converter ataques cibernéticos em um meio silencioso e potente de intimidação e subversão.

Diante do aumento dessas ameaças, o Brasil tem se esforçado para se preparar para uma eventual guerra cibernética, mesmo enfrentando desafios consideráveis para assegurar a proteção de suas infraestruturas vitais. Conforme o Livro Branco de Defesa Nacional e a Estratégia Nacional de Defesa, a área cibernética é uma das três bases estratégicas de defesa do país, juntamente com os setores aeroespacial e nuclear. Com o objetivo de fortalecer essa estratégia, o Brasil estabeleceu o Sistema Militar de Defesa Cibernética (SMDC), sob a coordenação do Exército e em colaboração com o Centro de Defesa Cibernética (CDCiber). O CDCiber executa ações preventivas, defensivas e de resposta a incidentes, sendo encarregado de salvaguardar as infraestruturas vitais do país, abrangendo áreas como energia, água, telecomunicações, finanças e transporte.

Adicionalmente a essas ações, o Brasil estabeleceu a Escola Nacional de Defesa Cibernética (ENaDCiber), destinada a capacitar profissionais, tanto militares quanto civis, para trabalhar na defesa cibernética e em atividades de segurança da informação. A formação da ENaDCiber demonstra o empenho do país em formar profissionais capacitados para enfrentar ameaças cibernéticas, algo crucial considerando a complexidade técnica envolvida. A instituição oferece formação em análise e gerenciamento de riscos, proteção de infraestruturas vitais, resiliência operacional e reação a ataques cibernéticos, fomentando uma cultura de defesa cibernética no Brasil. Além disso, o Brasil tem buscado alianças internacionais e regionais para reforçar sua segurança digital, cooperando com outras nações na partilha de informações e práticas de segurança.

Contudo, a infraestrutura brasileira de defesa cibernética continua a lidar com desafios consideráveis. A ausência de normas internacionais precisas e a complexidade em identificar e atribuir ataques cibernéticos fazem da defesa cibernética uma área extremamente complexa. A falta de limites físicos no ciberespaço torna difícil a identificação exata dos perpetradores de ataques, o que complica a implementação de ações legais ou de retaliação. Este desafio, denominado problema de atribuição, representa um dos maiores obstáculos para a segurança cibernética global, e o Brasil também se depara com esse desafio. Ademais, o elevado custo para a implementação e manutenção de tecnologias de defesa, juntamente com a constante demanda por atualização e inovação, constituem obstáculos para uma nação em crescimento, como o Brasil, que lida com restrições financeiras e estruturais.

Os efeitos de uma guerra cibernética na sociedade podem ser devastadores. Ataques a infraestruturas vitais, tais como redes elétricas, sistemas de fornecimento de água e sistemas de telecomunicações, poderiam levar a interrupções em grande escala, falta de água e suspensão dos serviços de comunicação, provocando pânico e caos na sociedade. Ademais, incidentes no setor financeiro poderiam prejudicar bancos e sistemas de pagamento, provocando instabilidade econômica e impactando o dia a dia de milhões de indivíduos. Um outro perigo relevante é a possibilidade de ataques a sistemas de saúde e segurança, tais como hospitais e serviços de emergência, o que poderia comprometer a saúde e a segurança da população.

Alguns exemplos de conflitos cibernéticos globais incluem o ataque Stuxnet em 2010, amplamente visto como um divisor de águas na guerra cibernética contemporânea. Este ataque, direcionado às centrífugas nucleares iranianas, empregou um malware avançado para prejudicar o programa nuclear do país. O Stuxnet é frequentemente mencionado como a primeira

referência de uma arma cibernética desenvolvida para provocar danos físicos, evidenciando a capacidade devastadora da guerra cibernética. Um exemplo similar é a invasão à Estônia em 2007, que resultou na interrupção de vários sistemas públicos e privados, como bancos, mídia e governo, através de um ataque coordenado de negação de serviço (DDoS). Estes ataques, supostamente realizados por grupos associados ao governo russo, ocorreram após um conflito diplomático e são vistos como um dos primeiros exemplos de guerra cibernética contemporânea.

Em 2015 e 2016, na Ucrânia, ocorreram ataques cibernéticos atribuídos à Rússia que impactaram a rede elétrica nacional, provocando interrupções que impactaram milhares de pessoas. Estes ataques evidenciaram o uso do ciberespaço para desestabilizar a infraestrutura de uma nação e diminuir sua habilidade de reação em situações de conflito. Estes exemplos destacam a fragilidade das infraestruturas vitais e a habilidade de uma guerra cibernética de provocar danos consideráveis a um país sem a exigência de invasões físicas.

Portanto, a área da guerra cibernética constitui um desafio estratégico tanto para o Brasil quanto para o mundo. A preparação do Brasil está avançando, porém encontra barreiras relacionadas a investimentos, normas e recursos humanos. Frente à possibilidade de uma guerra cibernética, é crucial que a nação continue aperfeiçoando suas habilidades de defesa e estabelecendo uma política de segurança cibernética sólida, além de fomentar a colaboração global para enfrentar as ameaças globais no ciberespaço.

5. CASOS ESPECÍFICOS DE ATAQUES CIBERNÉTICOS

5.1 **Burn, Baby, Burn**

Nos anos 1980, os EUA realizaram uma operação de contraespionagem, implantando um cavalo de Troia em um software de controle de gasoduto, que foi roubado pela União Soviética. Segundo Thomas Reed em seu livro At The Abyss, o software sabotado causou uma explosão massiva no gasoduto transiberiano em junho de 1982, quando alterou a pressão durante um teste, resultando em uma das maiores explosões não nucleares já vistas.

O plano foi idealizado por Gus Weiss, do Conselho de Segurança Nacional dos EUA. A explosão não causou vítimas, mas gerou grande confusão em Moscou e Washington, inicialmente suspeitando de um possível teste nuclear. Além dos danos econômicos ao

interromper o fornecimento de gás, a operação teve um impacto psicológico devastador nos soviéticos, que passaram a desconfiar de toda sua tecnologia importada. Isso afetou gravemente a indústria soviética, que dependia de equipamentos ocidentais.

5.2 **Implosão Nuclear**

Stuxnet foi um worm de computador altamente sofisticado, desenvolvido em 1982, com a colaboração dos governos dos Estados Unidos e de Israel. Seu principal objetivo era sabotar o programa nuclear do Irã, especificamente as centrífugas usadas no enriquecimento de urânio na instalação de Natanz. O ataque foi projetado para atrasar a capacidade do Irã de desenvolver armas nucleares, sem a necessidade de um conflito militar direto.

O vírus causou danos significativos ao danificar aproximadamente 1.000 das 5.000 centrífugas em operação em Natanz, uma instalação crucial para o programa nuclear iraniano. Esse ataque cibernético foi extremamente eficaz, resultando em um atraso no progresso do programa nuclear do Irã de pelo menos dois anos, ou mais. Além disso, o Stuxnet estabeleceu um precedente histórico, sendo o primeiro ataque cibernético documentado a causar danos físicos a uma infraestrutura crítica, marcando o início do uso de ciberarmas em conflitos internacionais.

Dessa forma, o ataque de 1982 aos sistemas do Irã não apenas demonstrou a vulnerabilidade das infraestruturas tecnológicas de países com programas nucleares, mas também marcou um novo estágio na guerra cibernética, onde o uso de ferramentas digitais tornou-se uma estratégia eficaz e de alto risco nas relações internacionais.

5.3 **The Interview (A Entrevista)**

Em 2014, hackers chamados "Guardiões da Paz" invadiram a rede da Sony Pictures, roubando 100 terabytes de dados. Utilizando um malware indetectável, os criminosos vazaram e-mails internos, dados de funcionários e filmes inéditos. Acredita-se que o ataque foi uma retaliação ao filme "A Entrevista", que satirizava o regime norte-coreano. Como consequência, a Sony cancelou a estreia do filme após ameaças contra cinemas. O prejuízo estimado foi de US$ 100 milhões.

Anteriormente, em 2011, a Sony também foi alvo de um ataque pelo grupo Anonymous, que invadiu a rede do PlayStation, derrubando-a por mais de 20 dias e comprometendo 77 milhões de contas, gerando um prejuízo de US$ 171 milhões.

5.4 **Black Energy**

Antes da guerra na Ucrânia, o país já era alvo de sofisticados ataques cibernéticos, especialmente após a anexação da Crimeia pela Rússia. Em 2015, o cibercrime "BlackEnergy" causou um apagão em Ivano-Frankivsk, na Ucrânia, afetando cerca de 225 mil pessoas. O ataque, realizado por hackers russos, usou malware escondido em arquivos do Microsoft Office, ativado por engenharia social. Com o malware, os invasores desativaram sistemas de TI e apagaram arquivos essenciais da rede elétrica.

Em 2016, a Ucrânia sofreu outro ataque, desta vez com o malware "Industroyer", que causou um apagão em Kiev, deixando milhares de casas sem energia por uma hora.

6. MANIPULAÇÃO GOVERNAMENTAL NO DIREITO INTERNACIONAL

Em primeira análise, a interferência do governo no direito internacional acontece quando as nações criam normas e entidades internacionais de acordo com seus interesses, prejudicando a neutralidade do sistema. Este fenômeno se apresenta de diversas maneiras, como na aplicação seletiva de penalidades. Países influentes impõem penalidades a adversários por infrações aos direitos humanos ou agressão territorial, contudo, muitas vezes atenuam ou desconsideram comportamentos semelhantes de seus aliados.

Essa atitude cria a impressão de que o direito internacional é adaptável e prioriza os interesses das potências, em detrimento da justiça e da paz mundiais. Assim, outro ponto importante é a utilização do discurso dos direitos humanos para legitimar ações militares ou econômicas. Numerosos países usam essa retórica para ocultar interesses econômicos ou geopolíticos, usando o pretexto de "salvaguarda dos civis" ou "incentivo à democracia" para justificar intervenções que, na realidade, visam manter ou ampliar sua influência em áreas estratégicas.

Este tipo de medida debilita o princípio da autodeterminação dos povos e estabelece um sistema em que as intervenções são seletivas, favorecendo os interesses das potências em prejuízo do bem-estar das comunidades impactadas. Dessa forma, a organização das entidades internacionais também contribui para essa manipulação. Por exemplo, o sistema de veto do Conselho de Segurança da ONU possibilita que os membros permanentes impeçam resoluções que não correspondam aos seus interesses. Isso restringe a habilidade dessas entidades de agir de forma imparcial e eficaz, favorecendo a aplicação desigual das regras e fortalecendo a influência das nações dominantes.

O recurso ao veto tem sido frequentemente empregado para salvaguardar aliados ou prevenir ações que possam colocar em risco os interesses estratégicos dos membros permanentes, prejudicando um sistema verdadeiramente multilateral e equitativo. Assim na esfera econômica, os acordos internacionais muitas vezes estabelecem condições desfavoráveis para as nações em desenvolvimento, limitando suas habilidades de controlar seu próprio mercado e salvaguardar setores vitais. A adoção de cláusulas que privilegiam investidores internacionais em vez da legislação local prejudica a independência dos Estados menores, forçando-os a aceitar termos que salvaguardam principalmente os interesses de grandes corporações e nações avançadas.

Isso demonstra que as regras econômicas globais geralmente são estabelecidas para favorecer os países que possuem maior influência na elaboração desses tratados. Nesse contexto no Brasil, a Constituição de 1988 estabelece a primazia dos direitos humanos e o respeito à autodeterminação dos povos. Por outro lado, a legislação sobre investimentos internacionais tem como objetivo assegurar que os fundos externos contribuam para o progresso do país, porém no contexto global, vários países negligenciam esses princípios em prol de políticas protecionistas ou intervencionistas, gerando uma contradição entre a implementação desses princípios no âmbito doméstico e as práticas internacionais.

Por fim esta interferência governamental demonstra um desequilíbrio estrutural que prejudica a legitimidade do direito internacional. A aplicação seletiva de normas debilita o sistema e transforma o direito internacional numa ferramenta que, frequentemente, atende aos interesses das potências, ao invés de fomentar a justiça e a equidade. A persistência deste desequilíbrio restringe a capacidade do direito internacional de estabelecer uma ordem mundial mais equitativa e colaborativa, transformando-o em um espelho das disparidades de poder que deveria combater.

REFERÊNCIAS

AGÊNCIA BRASIL. Estudo aponta manipulação política pela internet em 70 países em 2019. Agência Brasil, 25 set. 2019. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/estudo-apontamanipulacao-politica-pela-internet-em-70-paises-em-2019. Acesso em: 8 nov. 2024.

ALMEIDA, Jessica. Crimes Cibernéticos. Sergipe, 2015. Disponível em: <https://periodicos.grupotiradentes.com/cadernohumanas/article/view/2013> Acesso em: 04 de novembro de 2024.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília, DF, 3 out 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto--lei/del3689.htm>. Acesso em: 04 de novembro de 2024.

COMPUGRAF. As Principais Guerras Cibernéticas ao Longo da História. Publicado em 03 de agosto de 2020. Disponível em: Guerras Cibernéticas ao Longo da História

COSTA, Emanuely Silva. **SILVA**, Raíla da Cunha. Revista Eletrônica do Ministério Público do Estado do Piauí. 2 Ed; Dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf

DERECO. 1982: O Ciberataque da CIA que desmantelou a economia Soviética. Publicado em 28 de fevereiro de 2024. Disponível em: 1982 : O Cibertaque da CIA que desmantelou a economia Soviética

FASTHELP. Os ataques cibernéticos que entraram para a história. Publicado em 11 de outubro de 2023. Disponível em: Conheça os ataques cibernéticos que entraram para a história!

INDEX LAW. Manipulação política: desafios legais e sociais. Revista Direito e Democracia, v. 10, n. 2, p. 95-110, 1997. Disponível em: https://www.indexlaw.org/index.php/rdb/article/download/5301/5119/1997. Acesso em: 8 nov. 2024.

LE MONDE DIPLOMATIQUE. Entre a independência e a manipulação política. Le Monde Diplomatique Brasil, 10 nov. 2020. Disponível em: https://diplomatique.org.br/entre-a-independencia-e-a-manipulacaopolitica/. Acesso em: 8 nov. 2024.

MINISTÉRIO DA DEFESA DO BRASIL. Livro Branco de Defesa Nacional. Brasília, 2012. Disponível em: https://www.gov.br/defesa/pt-br

MINISTÉRIO DA DEFESA DO BRASIL. Estratégia Nacional de Defesa (END). Brasília, 2012. Disponível em: https://www.gov.br/defesa/pt-br

MUNDO CRÍTICO. Manipulação política: como as fake news influenciam a política global. Mundo Crítico, 15 mar. 2021. Disponível em: https://mundocritico.org/revista/manipulacao-politica/. Acesso em: 8 nov. 2024.

OLIVEIRA, Jessica Santos de. Classificação dos Crimes Cibernéticos. Jusbrasil. Disponível em: https://www.jusbrasil.com.br/artigos/classificacao-dos-crimes-ciberneticos/2104333712

PINHEIRO, Bruno Victor de Arruda. As Novas Disposições sobre os Crimes Cibernéticos. Jusbrasil, 2022. Disponível em: <https://jusbrasil.com.br/artigos/as-novas-disposicoes-sobre-os-crimes-ciberneticos/1518500029> Acesso em: 04 de novembro de 2024.

ROMANI, Bruno. 6 casos de ataque hacker. Publicado em 8 junho 2015. Disponível em: : 6 casos de ataque hacker | Super

SANTOS, Jefferson. Crimes Virtuais no Contexto Histórico. Rio de Janeiro, 2015. Disponível em: <https://repositorio.ivc.br/handle/123456789/480> Acesso em: 04 de novembro de 2024.

SILVA, Ronaldo; NOVAIS, Thyara. A Lei Geral de Proteção de Dados e sua Aplicação no Combate aos Crimes Cibernéticos: Desafios e Perspectivas. Revista Ibero-Americana de Humanidades, Ciências e Educação. São Paulo, 2023. Acesso em: 04 de novembro de 2024.

TEIXEIRA JÚNIOR, Augusto W. M., et al. (2017). "As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica." *Carta Internacional*, 12(3), 30-53. Disponível em: https://www.scielo.br/j/rbpi/a/zDC3D9BWxQvBxk56CmLdckJ/?lang=en