Crimes CIBERNÉTICOS

Apresentação da Disciplina PROGRAMAÇÃO E DIREITO – IBMEC Centro 2024.2

Professor: EDUARDO MANGELI

Tópicos Abordados

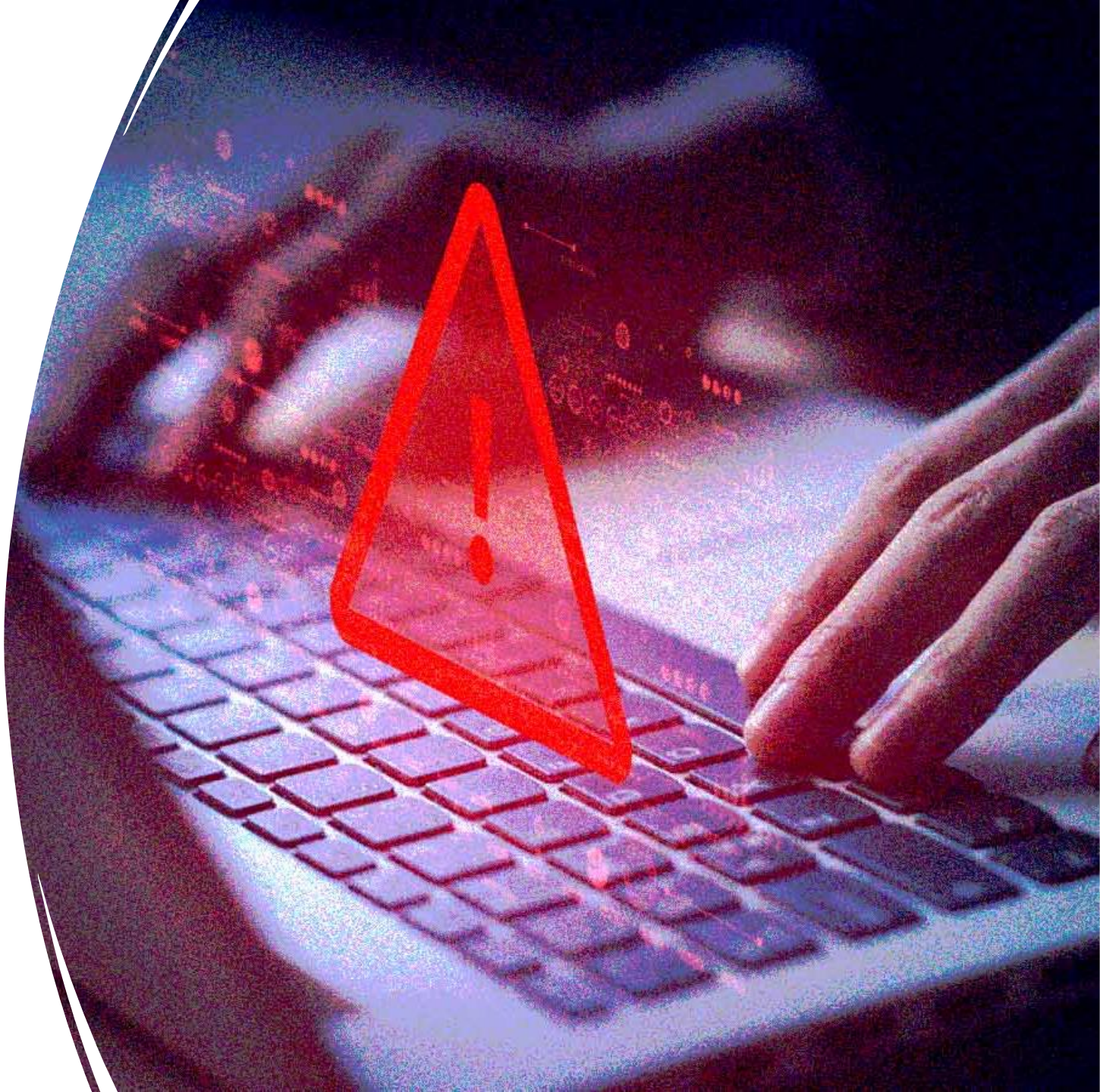
1. O que são Crimes Cibernéticos e qual sua Origem.
2. Tipos e Classificações.
3. Leis Brasileiras: Lei Carolina Dieckmann (Lei 12.737/2012), Marco Civil da Internet (Lei 12.965/2014), (Lei Geral de Proteção de Dados (Lei 13.709/18), Lei 14.155/2021 e Lei 14.132/2021.
4. Guerra Cibernética.
5. Casos Específicos.
6. Manipulação Governamental no Direito Internacional.

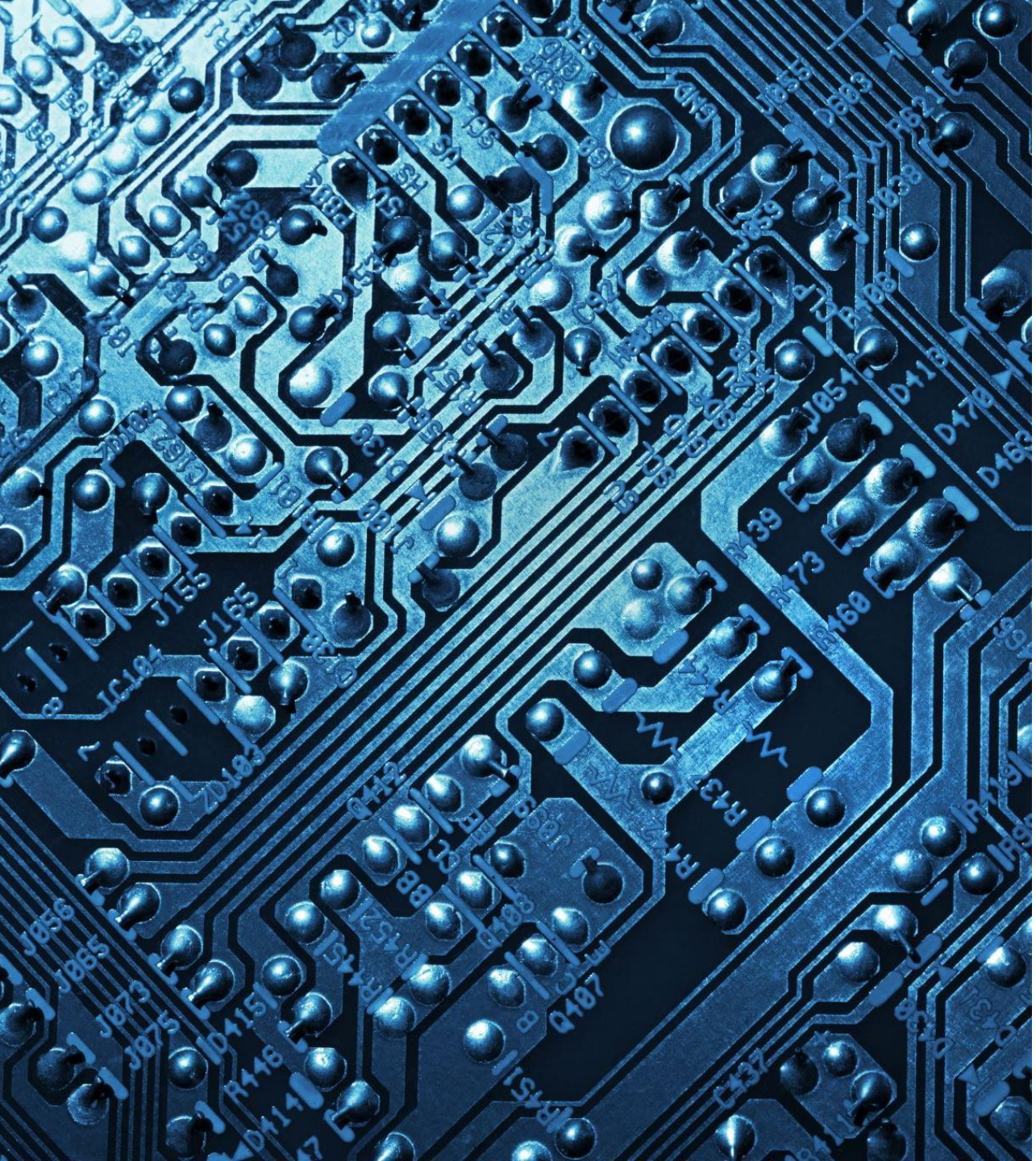
O que são Crimes Cibernéticos?

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**.

O que são Crimes Cibernéticos?

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.





Contexto Histórico

A prática dos crimes cibernéticos **evoluiu ao longo do tempo**, começando com a atuação de indivíduos altamente especializados na década de **1960**, mas se expandindo para pessoas comuns à medida que o acesso à tecnologia aumentou. Nos primeiros anos, os crimes se restringiam a **manipulação, sabotagem e espionagem de sistemas**. Na década de **1980**, com o crescimento do **uso de computadores** e redes, surgiram crimes como **manipulação de caixas eletrônicos, abusos de telecomunicações, pirataria de software e pornografia infantil.**

Contexto Histórico

Esse **aumento nos delitos cibernéticos levou à criação das primeiras legislações sobre o tema**, como o "Crime Control Act" (1984) e o "Computer Fraud and Abuse Act" (1986) nos Estados Unidos, a "Computer Kriminalitat" na Alemanha (1986), a Lei Godfraud na França (1988) e a inclusão de crimes informáticos no Código Penal espanhol em 1995. O conceito de "cibercrime" foi formalizado em 1997, durante um encontro do G8 em Lyon, França, e se referia a crimes cometidos via internet e outras redes de telecomunicações.

Contexto Histórico

Em 2001, o Conselho da Europa adotou a **Convenção Europeia sobre Crimes Cibernéticos** para padronizar a legislação sobre o tema. No Brasil, a legislação sobre cibercrimes começou a ganhar força com a promulgação da **Lei nº 9.883 em 2000**, que abordava aspectos gerais dos crimes cibernéticos, embora o assunto já tivesse sido tratado de forma econômica nas décadas de 1980 e 1990.

Tipos Mais Comuns

Entre os crimes cibernéticos mais comuns, destacam-se a clonagem de números de WhatsApp, a criação de boletos falsos, fraudes bancárias, comércios virtuais ilegais, leilões fraudulentos, empréstimos fictícios, crimes contra a honra (como difamação e divulgação não autorizada de fotos íntimas), além do roubo e sequestro de dados, entre outros.

Classificações Principais dos Crimes Cibernéticos

- **Crime Cibernético Impróprio**: É quando se utiliza 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 medicar o paciente com uma dosagem elevada, levando o mesmo ao óbito.
- **Crime Cibernético Próprio:** São 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.

Outras Classificações Possíveis

01

Crime Cibernético Comum: São crimes que utilizam a internet como instrumento para realizar um delito que enquadra no Código Penal, como a distribuição de conteúdo pornográfico infantil.

02

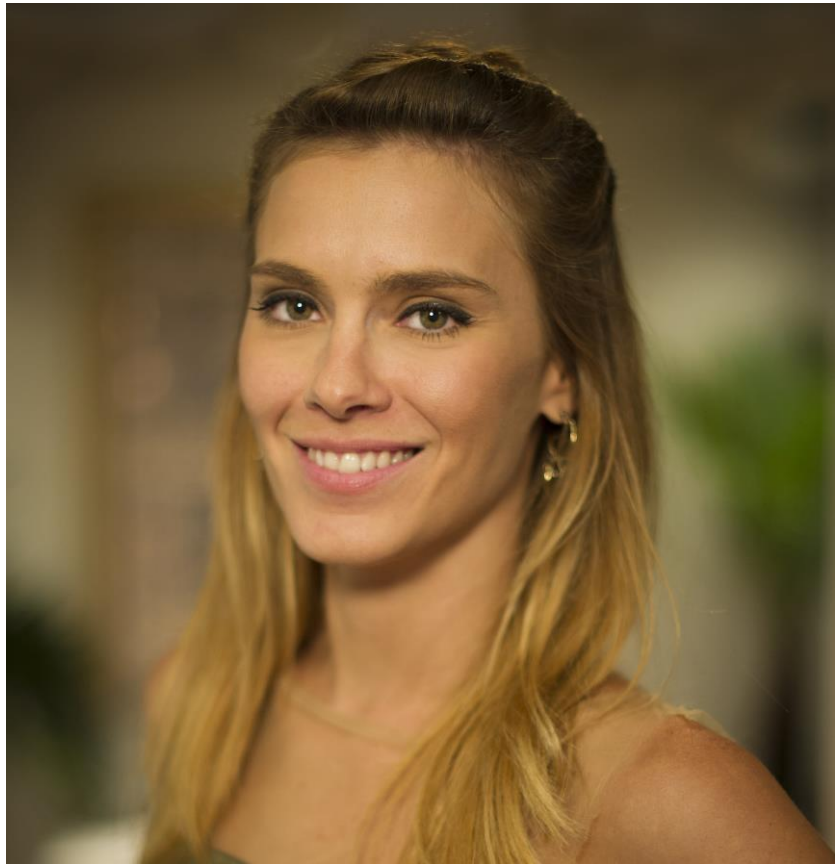
Crime Cibernético Puro: Similares aos próprios, são condutas ilícitas que atingem o hardware e/ou software de um computador, sem danos diretos ao mundo real.

03

Crime Cibernético Misto: 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.

Lei Carolina Dieckmann
Lei 12.737/2012

A Lei nº 12.737/2012, conhecida como **Lei Carolina Dieckmann**, foi um marco no combate **aos crimes cibernéticos** no Brasil, ao tipificar novos delitos no ambiente digital, como a invasão de dispositivos e a divulgação não autorizada de dados pessoais. Antes de sua promulgação, essas práticas eram difíceis de punir com a legislação penal tradicional, inadequada para os desafios da internet. A lei foi nomeada em homenagem à atriz Carolina Dieckmann, que teve seu computador invadido e fotos íntimas divulgadas após se recusar a ceder à extorsão. O caso destacou a vulnerabilidade das pessoas aos crimes digitais e gerou uma mobilização por uma regulamentação mais rígida para proteger a privacidade e a segurança online.



Marco Civil da Internet
Lei 12.965/2014

O "Marco Civil da Internet" (Lei nº 12.695/2014) foi sancionado pela presidente Dilma Rousseff em 23 de abril de 2014, após a fusão de diversos projetos e impulsionado pelas revelações de espionagem do governo dos Estados Unidos. A lei define **princípios, direitos e deveres para os usuários da internet no Brasil**. Seus dois primeiros capítulos são os mais relevantes: o primeiro estabelece conceitos, princípios e responsabilidades para o uso da internet, além de orientar a atuação do governo; o segundo garante direitos aos usuários, como a proteção da privacidade e a transparência nas políticas de uso de sites, provedores e redes sociais.

Lei Geral de Proteção de Dados
Lei 13.709/18

A Lei Geral de Proteção de Dados (LGPD) foi criada para enfrentar a crescente ameaça de delitos cibernéticos, estabelecendo regras para a **coleta, armazenamento e uso de dados pessoais no Brasil**. Seu principal objetivo é aumentar a **transparência, segurança e privacidade no processamento de dados**, além de fornecer meios para identificar responsáveis por crimes digitais. A LGPD exige que organizações adotem medidas de proteção de dados pessoais, promovendo maior controle sobre a segurança da informação e prevenindo danos éticos, jurídicos e financeiros decorrentes de seu uso inadequado.

Lei 14.155/2021 e Lei 14.132/2021

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.

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.

Guerra Cibernética

A guerra cibernética é uma **nova e complexa forma de conflito** que envolve **ataques cibernéticos contra sistemas essenciais** de nações, empresas e indivíduos, visando desestabilizar infraestruturas vitais. Ao contrário da guerra convencional, esses **ataques não necessitam de intervenção militar física**, sendo realizados por meio de ferramentas tecnológicas como malware, vírus e ataques de negação de serviço (DDoS). A **motivação é frequentemente política e estratégica**, com o ciberespaço tornando-se um meio silencioso de intimidação e subversão.

Guerra Cibernética

Diante dessas crescentes ameaças, o **Brasil** tem se esforçado para **se preparar** para uma eventual guerra cibernética, incorporando a **segurança digital** como uma das três bases estratégicas de defesa do país, ao lado dos setores aeroespacial e nuclear. O **Sistema Militar de Defesa Cibernética (SMDC),** coordenado pelo Exército, e o Centro de Defesa Cibernética (CDCiber) têm a missão de proteger as infraestruturas críticas do Brasil, incluindo áreas como energia, água, telecomunicações e finanças. O país também criou a **Escola Nacional de Defesa Cibernética (ENaDCiber)**, que capacita profissionais especializados para enfrentar essas ameaças.

Guerra Cibernética

No entanto, o Brasil enfrenta vários **desafios para fortalecer sua defesa cibernética**. A **ausência de normas internacionais** claras e a dificuldade de atribuir ataques cibernéticos a culpados, conhecidos como "problema de atribuição", tornam a **segurança digital uma área complexa e cheia de obstáculos**. Além disso, a constante **evolução das ameaças** exige grandes investimentos em tecnologias de defesa, algo que é um desafio para o Brasil devido **a restrições financeiras e estruturais**. A atualização contínua dessas defesas é essencial para enfrentar as ameaças em constante mudança.

Guerra Cibernética

Os **impactos** de uma guerra cibernética podem ser **devastadores**, afetando a sociedade de diversas maneiras, como a **interrupção de redes elétricas, sistemas de água e telecomunicações**, o que pode causar pânico e caos. Também há o risco de **ataques a sistemas financeiros, impactando a economia, e a sistemas de saúde, comprometendo a segurança da população**. Exemplos de conflitos cibernéticos globais, como o **Stuxnet** (2010), a **invasão à Estônia** (2007) e os ataques à **Ucrânia** (2015-2016), demonstram como ataques cibernéticos podem **desestabilizar infraestruturas vitais sem a necessidade de invasões físicas**, destacando a fragilidade de sistemas em um mundo cada vez mais dependente da tecnologia

Casos Reais – Burn, Baby, Burn

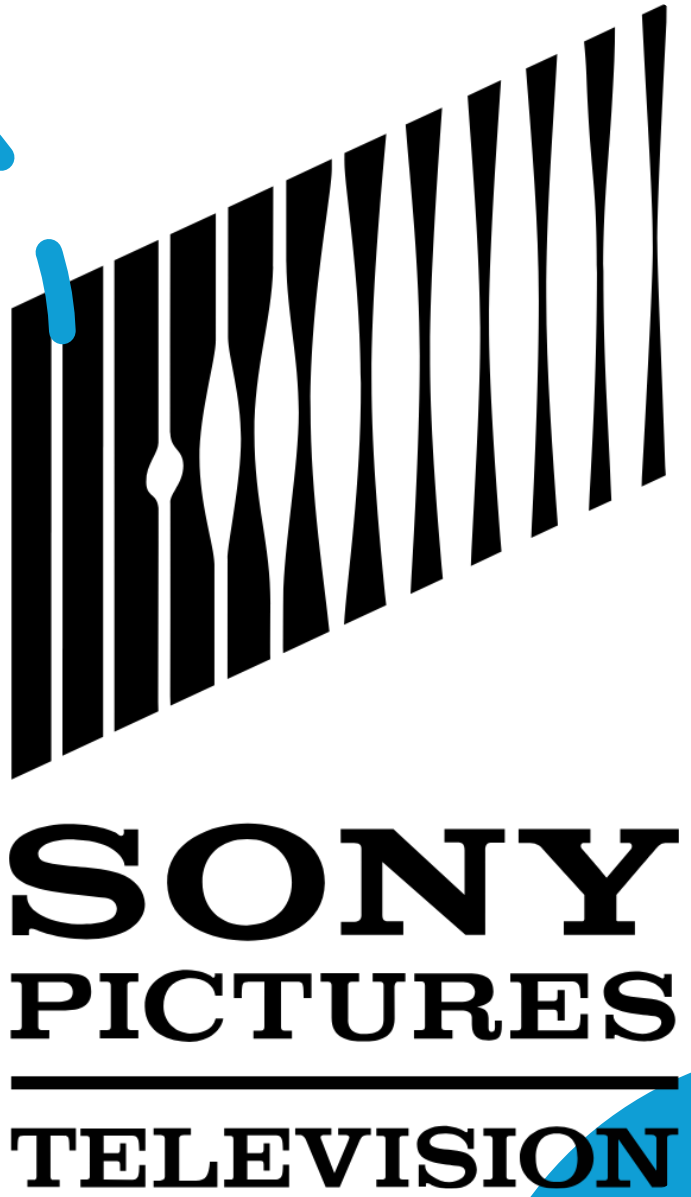
Nos anos **1980**, os **EUA** realizaram uma operação de contraespionagem, implantando um **cavalo de Troia em um software** de controle de gasoduto roubado pela **União Soviética**. Em junho de 1982, o software sabotado causou uma enorme explosão no gasoduto transiberiano, alterando a pressão durante um teste e provocando uma das maiores explosões não nucleares já registradas. A operação, idealizada por Gus Weiss do **Conselho de Segurança Nacional dos EUA**, gerou confusão em Moscou e Washington, com suspeitas iniciais de um teste nuclear. Embora não tenha causado vítimas, o ataque causou danos econômicos ao interromper o fornecimento de gás e teve um impacto psicológico significativo nos soviéticos, que passaram a **desconfiar de toda sua tecnologia importada**, prejudicando a indústria soviética que dependia de equipamentos ocidentais.

Casos Reais – Implosão Nuclear

Stuxnet foi um worm de computador altamente sofisticado, desenvolvido pelos governos dos **EUA e de Israel**, com o objetivo de sabotar as centrífugas de enriquecimento de urânio do **Irã** na instalação de Natanz. O ataque, que **destruiu cerca de 1.000 centrífugas**, visava atrasar o programa nuclear iraniano sem recorrer a ação militar direta. Esse ciberataque causou danos significativos à infraestrutura nuclear do Irã e atrasou seu progresso em até dois anos. Além disso, Stuxnet foi o **primeiro ataque cibernético documentado a causar danos físicos a uma infraestrutura crítica**, marcando o início do uso de ciberarmas em conflitos internacionais.

Casos Reais - The Interview (A Entrevista)

Em 2014, o grupo de hackers **"Guardiões da Paz"** invadiu a rede da **Sony Pictures**, roubando cerca de 100 terabytes de dados, incluindo e-mails internos, informações de funcionários e filmes inéditos. O ataque, realizado com um malware indetectável, foi amplamente considerado uma retaliação ao filme **"A Entrevista"**, que satirizava o regime norte-coreano. Em resposta, a Sony cancelou a estreia do filme após ameaças de violência contra cinemas. O prejuízo estimado foi de US$ 100 milhões. Este não foi o primeiro ataque à Sony: em 2011, o grupo **Anonymous** já havia invadido a rede do PlayStation, derrubando-a por mais de 20 dias e comprometendo 77 milhões de contas, resultando em perdas de US$ 171 milhões.



Casos Reais – BlackEnergy

Antes da guerra na **Ucrânia**, o país já enfrentava ataques cibernéticos sofisticados, especialmente após a anexação da Crimeia pela **Rússia**. Em 2015, o cibercrime "**BlackEnergy**" provocou um apagão em Ivano-Frankivsk, afetando cerca de 225 mil pessoas, quando hackers russos utilizaram malware oculto em arquivos do Microsoft Office, ativado por engenharia social, para desativar sistemas de TI e apagar arquivos essenciais da rede elétrica. Em 2016, a Ucrânia sofreu outro ataque cibernético, desta vez com o malware "Industroyer", que causou um **apagão em Kiev**, deixando milhares de casas sem energia por uma hora.

Manipulação Governamental no Direito Internacional

A **interferência dos governos** no direito internacional ocorre quando as nações **criam normas e instituições internacionais que atendem a seus próprios interesses**, prejudicando a imparcialidade do sistema global. Isso se manifesta na aplicação seletiva de penalidades: **países poderosos impõem sanções a adversários**, mas ignoram comportamentos semelhantes de seus aliados, dando a impressão de que o direito internacional favorece as potências em vez de buscar justiça e paz.

Manipulação Governamental no Direito Internacional

Outro aspecto é o uso do **discurso dos direitos humanos** para justificar ações militares ou econômicas, frequentemente disfarçando interesses geopolíticos e econômicos. Ao utilizar o pretexto de proteger civis ou promover a democracia, países intervêm em **áreas estratégicas**, o que enfraquece o princípio da autodeterminação dos povos e estabelece um sistema de **intervenções seletivas que favorecem as potências**, prejudicando as populações afetadas.

Manipulação Governamental no Direito Internacional

Além disso, o sistema de veto no **Conselho de Segurança da ONU** permite que os membros permanentes **bloqueiem resoluções contrárias aos seus interesses**, restringindo a capacidade da organização de agir de forma eficaz e imparcial. Essa dinâmica de poder também se reflete nos acordos econômicos internacionais, que muitas vezes impõem **condições desfavoráveis a países em desenvolvimento**, limitando sua autonomia econômica e favorecendo investidores internacionais e potências dominantes.

Manipulação Governamental no Direito Internacional

No Brasil, embora a **Constituição de 1988** garanta a primazia dos direitos humanos e o respeito à autodeterminação, na prática, o país muitas vezes adota **políticas externas que contradizem esses princípios**, em nome de interesses econômicos e políticos globais. Esse desequilíbrio estrutural enfraquece o direito internacional, transformando-o em uma ferramenta que frequentemente atende aos interesses das potências, em vez de promover uma ordem mundial mais justa e equitativa.

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.

Referências

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

Obrigado!

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