<< CIBERSEGURANÇA EM FOCO: DESAFIOS E INTERVENÇÕES PARA PROTEGER A SOBERANIA DIGITAL BRASILEIRA >>

Renato Laterza Franceschini

Jairo Oliveira De Castro (Orientador)

José Aparecido Santos Junior (Co-Orientador)

Brazilian International School

Resumo

O mundo globalizado contemporâneo está passando por um intenso processo de digitalização. O setor econômico mundial, bem como as nossas atividades cotidianas estão centradas no ciberespaço. De forma análoga, atividades criminosas nesse meio, como os ataques cibernéticos, vem crescendo e se nossa população e sistemas da informação não estiverem preparados para retalia-las com eficácia, poderemos enfrentar graves consequências.

Esse trabalho visa conceituar o termo cibersegurança, explorar sua crescente importância e juntamente analisar as diferentes formas como ela é ameaçada. Dessa forma, construindo uma base sólida para a discussão de seu principal objetivo: analisar a segurança cibernética brasileira, e a partir do estudo de um ataque cibernético específico, problematizá-la. Para que ao fim, uma adequada proposta de intervenção seja elaborada, visando proteger a soberania digital brasileira.

Palavras-chave: Ataques Cibernéticos. Cibersegurança. Dados Digitais. Segurança Cibernética. Soberania Digital

Introdução

De acordo com uma pesquisa conduzida pelo Instituto de Tecnologia de Massachusetts (MIT), nomeada "MIT Technology Review Insights Cyber Defense Index 2022/23", entre os 20 países avaliados no quesito cibersegurança, o Brasil estava localizado na posição Nº18, apenas atrás da Turquia e Indonésia. Levando em consideração o panorama global do espaço digital, que demonstra a crescente importância da segurança cibernética, essa posição coloca o Brasil em um cenário preocupante em termos de proteção dos seus sistemas de informação.

O advento da internet revolucionou a forma como nos comunicamos, trabalhamos e interagimos socialmente. No entanto, esse ambiente digital também trouxe consigo desafios significativos, sendo um deles o aumento dos casos de ataques cibernéticos. Esses ataques representam uma ameaça não apenas para a segurança de indivíduos e organizações, mas também para a estabilidade de uma nação como um todo.

Os ataques cibernéticos podem ter consequências devastadoras em diversos aspectos da sociedade. Eles podem comprometer a integridade e a confidencialidade dos dados, afetando empresas, instituições governamentais e até mesmo infraestruturas críticas, como sistemas de energia, transporte e comunicação. Além disso, esses ataques podem causar danos econômicos significativos, resultando em perdas financeiras e interrupções nas atividades comerciais.

Dessa forma, torna-se indispensável que o Brasil priorize a segurança cibernética como um pilar fundamental de sua agenda estratégica. Para tanto, é fundamental desenvolver uma proposta de intervenção abrangente e adaptada à realidade brasileira. Essa proposta deve ser embasada em casos de ataques cibernéticos reais e contemporâneos, como o caso específico a ser estudado neste trabalho. Ao analisar as vulnerabilidades identificadas nesse caso e compreender as razões por trás do vazamento e suas consequências para os usuários, será possível problematizar a segurança cibernética no Brasil e apontar direções para a melhoria da proteção dos sistemas de informação.

Somente por meio de um esforço conjunto e coordenado, envolvendo todos os atores relevantes, será possível enfrentar os desafios cada vez mais complexos do cenário

cibernético, assim protegendo a soberania digital brasileira e garantindo a segurança de nossos sistemas de informação. A segurança cibernética é um imperativo para o desenvolvimento sustentável, a proteção dos direitos individuais e a preservação da integridade de nossa nação no mundo digital, essas sendo questões que não podem ser negligenciadas.

Objetivo

OBJETIVO GERAL

Considera-se como objetivo geral deste trabalho: compreender a área da cibersegurança de forma generalista, assimilar as lacunas na segurança cibernética brasileira e desenvolver uma proposta de intervenção que vise proteger a soberania digital brasileira e impedir que soframos mais consequências provenientes da defasagem nacional na área da segurança cibernética.

OBJETIVOS ESPECÍFICOS

- Definir precisamente o termo "cibersegurança", a fim de que ela possa ser abordada de uma forma multidisciplinar;
- Abordar a crescente importância da cibersegurança no cenário global contemporâneo;
- Realizar uma análise tipológica dos ataques cibernéticos mais comuns;
- Compreender as estatísticas a respeito da cibersegurança brasileira;
- Produzir uma análise aprofundada de um ataque cibernético específico ocorrido no Brasil;
- Identificar padrões dentre os ataques cibernéticos ao espaço digital brasileiro;
- Elaborar uma proposta de intervenção para o aprimoramento do desempenho brasileiro nessa área, e dessa forma, protegendo a soberania digital brasileira e impedindo que soframos mais consequências provenientes de ataques cibernéticos.

Metodologia

O presente estudo é de natureza aplicada, visando fornecer uma compreensão aprofundada dos desafios e das lacunas na segurança cibernética no Brasil, analisando casos reais de ataques cibernéticos e propondo intervenções concretas para melhorar a segurança cibernética no país. A pesquisa foi conduzida de acordo com a metodologia exploratória e uma abordagem quali-quantitativa. Ademais, essa pesquisa é baseada na leitura e citação de dezenas de artigos científicos disponíveis na Internet.

Desenvolvimento

1. RETRATO DA SEGURANÇA CIBERNÉTICA

1.1. CONCEITUANDO A SEGURANÇA CIBERNÉTICA

Como demonstram Craigen, Diakun-Thibault e Purse (2014), a cibersegurança é um termo que possui definições altamente variáveis e muitas vezes subjetivas, fato que impediria o desenvolvimento dessa área. Entretanto, justamente com o objetivo de enriquecer a sua abordagem acadêmica, industrial, governamental e não governamental, foi elaborada uma nova definição, que englobaria a sua total multidisciplinaridade e não só em seu aspecto técnico.

Segundo os mesmos autores, a cibersegurança pode ser definida como a implementação de medidas e a adoção de estratégias destinadas a proteger o ciberespaço e os sistemas conectados contra situações que possam afetar a relação entre os direitos de propriedade estabelecidos por lei e aqueles que são efetivamente praticados.

Essa definição introduz um novo conceito: a ideia do ciberespaço (também denominado espaço cibernético). Diversos autores buscaram definir esse conceito, mas de forma generalista ele pode ser visto como "O espaço criado pela conexão de todas as bases de dados, formado pelas redes de computadores e de telecomunicações"; essa sendo uma interpretação de Cascais (2001 apud VIEIRA, SILVIA e RODRIGUES, 2014). Isso significa que toda informação produzida, armazenada, analisada e disseminada no espaço digital faz parte do espaço cibernético.

Por conseguinte, entende-se que segundo os autores previamente supracitados, os *meios* utilizados para proteger esse ciberespaço, tanto de jure (de acordo com a lei) quanto de facto (na prática) são denominados cibersegurança.

1.2. A CRESCENTE IMPORTÂNCIA DOS DADOS E DA SEGURANÇA CIBERNÉTICA

De acordo com a Organização das Nações Unidas 5,3 bilhões de pessoas no mundo são usuárias da internet, e esse número vem apenas crescendo diariamente (dados publicados em Setembro de 2022). Essa estatística pode ser explicada por um estudo produzido por Reinsel, Gantz e Rydning (2018), onde é descrito que estamos passando por um processo extensivo de "Digitalização do Mundo". O mundo globalizado contemporâneo vem se moldando de uma forma que tornou intrínseco que a população faça o uso das ferramentas disponíveis na Internet e dos sistemas de comunicação para a realização de até mesmo suas mais mundanas tarefas diárias. Assim fazendo com que nos dias de hoje, nossas vidas e o mundo virtual se *entrelacem.*

Consequentemente, o setor econômico mundial, também foi tomado pelo ciberespaço. Hoje, compras e transações financeiras podem ser realizadas de maneira instantânea e totalmente digitalizada, englobando desde simples usuários a grandes negociadores; serviços podem ser realizados de maneira digital, até mesmo a indústria do entretenimento estabelecendo-se no ciberespaço, com os serviços de streaming, por exemplo; a comunicação se tornou digital, com o avanço das redes sociais e plataformas de mensagem instantâneas; e entre outros exemplos.

De uma perspectiva mais superficial, centrada na experiência dos consumidores e na visão estratégica de crescimento das empresas, essas novas tendências tecnológicas apenas contribuíram para a velocidade e a qualidade dos diversos setores econômicos mundiais. Entretanto, é fundamental observar o outro lado dessa moeda: quais serão os riscos dessa transformação? A chave para essa resposta está centrada no estudo dos dados:

Segundo Reinsel, Gantz e Rydning (2018) uma parcela significativa da economia contemporânea está profundamente interligada com o uso de dados, e essa interdependência é esperada para se intensificar no futuro. Esse aumento na dependência ocorrerá à medida que as empresas incorporarem em cada etapa de suas cadeias de suprimentos a prática de adquirir, organizar e rentabilizar dados. Além disso, as empresas coletarão volumes substanciais de informações dos clientes, visando proporcionar níveis mais elevados de personalização. Ao mesmo tempo, os consumidores integrarão em suas rotinas diárias elementos como mídias sociais, entretenimento, armazenamento em nuvem e serviços personalizados em tempo real.

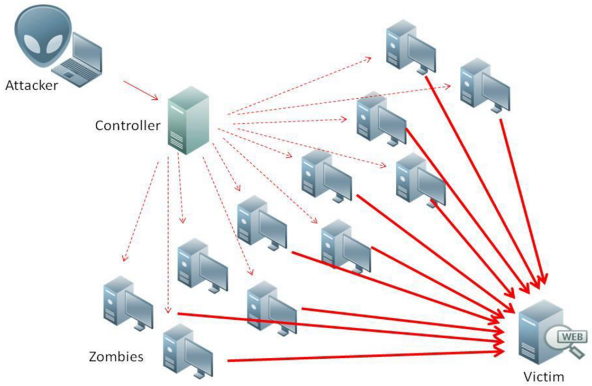
Essa passagem explica de maneira brilhante a relação entre a expansão do mundo digital e a crescente importância dos dados. Ao passo que todas as informações sobre nossas vidas pessoais, sistemas financeiros e governamentais concentram-se no ciberespaço em forma de dados digitais, surge um questionamento: o que poderia ocorrer caso esses dados fossem de alguma maneira corrompidos? Roubados? Modificados sem autorização? Quais serão então os prejuízos para a sociedade?

E é por esse motivo que a cibersegurança vem se destacando cada vez mais nos setores tecnológicos durante os últimos anos. Os dados digitais são valiosos, e sem a devida proteção dessas informações, há margem para que toda a estabilidade de nossos sistemas digitais, e consequentemente de nossas vidas, seja afetada.

1.3. BREVE ANÁLISE TIPOLÓGICA DAS AMEAÇAS À SEGURANÇA CIBERNÉTICA

A última etapa para compreender o verdadeiro retrato da segurança cibernética será analisar os tipos de ameaças que podem comprometer a integridade, confidencialidade e disponibilidade das informações e sistemas no ciberespaço. É importante ressaltar que devido à natureza complexa e em constante evolução do ciberespaço, é praticamente impossível analisar todas as possíveis variações e formas de ameaças à segurança cibernética. Entretanto, o objetivo principal é obter uma contextualização sólida das ameaças mais relevantes. Essa abordagem permite uma compreensão mais profunda do cenário de segurança cibernética, auxiliando no desenvolvimento de estratégias e soluções adaptáveis para enfrentar os desafios que surgem nesse ambiente complexo:

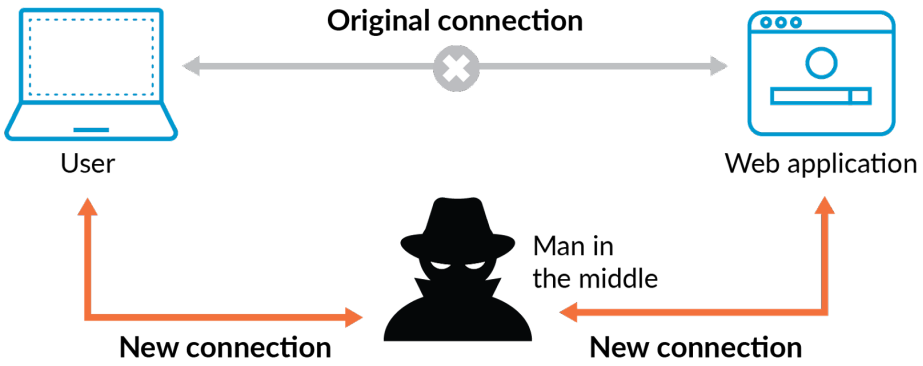
Ataque de negação de serviço: Também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service, é um termo utilizado para descrever um tipo de ataque realizado com o objetivo de tornar um serviço indisponível para os usuários legítimos.



Ele ocorre quando um grande volume de tráfego ou solicitações (induzido por uma série de dispositivos (zombies) comandados por um só computador (dispositivo mestre) é direcionado a um

alvo específico (em um curto espaço de tempo). Dessa forma sobrecarregando seus recursos e tornando-o incapaz de responder adequadamente às solicitações legítimas.
Devido à capacidade limitada dos servidores web em lidar com um número simultâneo de usuários, conhecido como slots, ele se torna sobrecarregado, incapaz de processar novas solicitações. Essa sobrecarga pode levar a uma degradação significativa no desempenho do sistema ou até mesmo à sua completa indisponibilidade.

Ataque man-in-the-middle (MitM): Os ataques MIIDM são uma forma sofisticada de ataque cibernético, caracterizados pela interceptação e manipulação de comunicações entre dois participantes legítimos, sem que eles tenham conhecimento disso. Esse tipo de ataque envolve a presença de um atacante intermediário que se posiciona entre as partes envolvidas na comunicação, podendo monitorar e até mesmo alterar os dados transmitidos.



Uma das principais preocupações com os ataques MIIDM é a sua capacidade de comprometer a integridade e a confidencialidade das informações transmitidas. Ao se inserir no fluxo de comunicação, o atacante pode acessar dados sensíveis, como informações pessoais, senhas e dados financeiros. Além disso, eles podem manipular os dados transmitidos, causando danos significativos às partes envolvidas.

Ataque de Injeção de SQL: Para compreender o Ataque de Injeção de SQL será necessário explorar o contexto em que ele ocorre. Bancos de dados são componentes essenciais de muitos sistemas, armazenando informações confidenciais e críticas para o funcionamento de empresas e organizações. A linguagem SQL (Structured Query Language) é amplamente utilizada para consultar e manipular dados em bancos de dados.

O Ataque de Injeção de SQL ocorre quando um invasor explora uma vulnerabilidade em um

sistema que não realiza uma validação adequada dos dados inseridos pelo usuário. O atacante insere código SQL malicioso em campos de entrada de dados, como formulários de login ou caixas de pesquisa, com o objetivo de enganar o sistema e executar comandos não autorizados no banco de dados.
Uma das principais preocupações com esse tipo de ataque é a possibilidade de comprometer a integridade dos dados armazenados e, em alguns casos, obter acesso a informações confidenciais. O invasor pode realizar ações como roubo, modificação ou exclusão de dados sensíveis, causando danos significativos à organização afetada.

Ataque de ransomware: Os ataques de ransomware são um tipo específico de ciberataque que tem se destacado pela sua natureza prejudicial e impactos significativos nas organizações. Esse tipo de ataque envolve a infecção de sistemas e redes com um software malicioso projetado para criptografar os arquivos e dados do alvo, tornando-os inacessíveis.

Quando o software malicioso é ativado, ele começa a criptografar os arquivos e exibe uma mensagem exigindo um resgate (geralmente em criptomoedas) em troca da chave de descriptografia. Entretanto, sua característica mais preocupante é o seu potencial de causar interrupções graves nas operações de negócios, instituições governamentais e até mesmo serviços essenciais, como saúde e infraestrutura crítica. Os atacantes exploram o valor crítico dos dados e a dependência das organizações por eles, tornando o pagamento do resgate uma opção tentadora para recuperar o acesso aos arquivos.

Ataque de engenharia social: Por fim, será realizada a análise de um dos ataques cibernéticos mais comuns, a Engenharia Social. Esse tipo de ataque se tornou amplamente difundido devido à sua eficácia em explorar as vulnerabilidades humanas e obter acesso não autorizado a informações confidenciais. A engenharia social se baseia na compreensão dos aspectos psicológicos e sociais das interações humanas, manipulando emoções, confiança e ingenuidade para enganar as vítimas. Entre os diversos tipos de ataques de engenharia social, se destacam:

Phishing: Nesse tipo de ataque, os invasores enviam e-mails, mensagens ou links falsos que se assemelham a comunicações legítimas de empresas ou instituições conhecidas. Os usuários são induzidos a clicar em links maliciosos ou fornecer informações confidenciais, como senhas ou números de cartão de crédito. A mensagem geralmente apela para a urgência, medo

ou benefícios financeiros, levando a vítima a agir impulsivamente.

Pretexting: No pretexting, os invasores se fazem passar por pessoas confiáveis ou autoridades para obter informações sensíveis. Eles podem criar uma narrativa convincente, como se estivessem ligando de um departamento de suporte técnico ou de uma empresa parceira, e solicitar dados pessoais ou credenciais de acesso. O objetivo é explorar a tendência natural das pessoas de seguir instruções de figuras de autoridade e confiar em solicitações aparentemente legítimas.

Tailgating: O tailgating ocorre quando um invasor ganha acesso não autorizado a um local físico aproveitando a cortesia ou a confiança dos funcionários. O invasor pode se passar por um colega de trabalho ou se aproveitar de uma situação em que uma pessoa autorizada está entrando em um prédio ou área restrita. Ao se infiltrar junto com a pessoa autorizada, o invasor evita os controles de segurança e obtém acesso indevido às instalações.

Quid pro quo: No ataque quid pro quo, os invasores oferecem algo em troca de informações ou acesso não autorizado. Por exemplo, podem se passar por especialistas em TI e ligar para os usuários, oferecendo ajuda imediata em troca de suas credenciais de login ou de outras informações confidenciais. Ao explorar o desejo de resolver problemas rapidamente ou obter benefícios, os invasores conseguem acesso aos sistemas ou informações desejadas.

Em suma, os ataques cibernéticos exploram tanto as fraquezas inerentes à natureza humana quanto às vulnerabilidades mais profundas dos sistemas de TI. Enquanto os ataques de engenharia social demonstram a necessidade de educar os usuários e desenvolver estratégias de conscientização para detectar e evitar essas táticas enganosas; os ataques que exploram as vulnerabilidades dos sistemas de TI destacam a importância da implementação de medidas mais robustas de segurança cibernética.

Resultados e Discussões

2. SOLUÇÃO DOS PROBLEMAS CONTEMPORÂNEOS DA CIBERSEGURANÇA BRASILEIRA

2.1. VISÃO GERAL DOS ATAQUES CIBERNÉTICOS OCORRIDOS NO BRASIL

De acordo com uma pesquisa realizada em 2022 pelo MIT Technology Review Insights, nomeada "MIT Technology Review Insights Cyber Defense Index 2022/23", entre os 20 países avaliados no quesito cibersegurança, o Brasil estava localizado na posição Nº18, apenas atrás da Turquia e Indonésia. Mais especificamente, o critério de avaliação definido foi "o quão bem sucedido vem sendo o desenvolvimento de políticas visando o aprimoramento da cibersegurança". O Brasil foi indicado como tendo possuído "progresso lento ou irregular em relação à criação de um ambiente de cibersegurança".

Figure 1: All Cyber Defense Index country rankings, 2022-2023

The leaders	The 5 countries making the greatest progress and commitment toward creating a cyber defense environment.	1	Australia	7.83
		2	Netherlands	7.61
		3	South Korea	7.41
		4	United States	7.13
		5	Canada	6.94
The challengers	The 10 countries making progress or commitment toward creating a cyber defense enviroment.	6	Poland	6.91
		7	United Kingdom	6.79
		8	France	6.78
		9	Japan	6.71
		10	Switzerland	6.45
		11	Italy	6.37
		12	China	6.27
		13	Germany	6.24
		14	Spain	6.13
		15	Saudi Arabia	5.55
Strivers	The 5 countries making slow and uneven progress or commitment toward creating a cyber defense environment.	16	Mexico	5.31
		17	India	4.87
		18	Brazil	4.75
		19	Turkey	4.26
		20	Indonesia	3.46

Source: MIT Technology Review Insights, 2022

Compreender os motivos pelos quais o Brasil ocupa essa posição de fragilidade é fundamental para que possamos desenvolver novas estratégias e abordagens para fortalecer a cibersegurança no país. Nesta seção serão realizadas análises de dados, casos, estatísticas e legislações a respeito da segurança cibernética no país e no mundo, a fim de que possamos compreender nossas severas lacunas nesse setor.

Elaboração do Marco Civil da Internet (Lei n° 12 965, de 23 de abril 2014):

O Marco Civil da Internet, oficialmente conhecido como Lei nº 12.965/2014, e sancionado pela então presidente Dilma Rousseff, é uma legislação brasileira que estabelece princípios, direitos e deveres para o uso da Internet no país. Essa lei desempenha um papel fundamental na promoção da segurança cibernética e na proteção dos direitos dos usuários no ambiente digital. (Assis, 2016)

O Marco Civil da Internet foi criado com o objetivo de estabelecer uma estrutura legal que garantisse a liberdade de expressão, a privacidade, a neutralidade de rede e a responsabilidade dos diferentes atores envolvidos no ecossistema da Internet. Essa legislação reflete a necessidade de estabelecer um equilíbrio entre a proteção dos direitos individuais e a promoção da segurança cibernética no Brasil.

No contexto da cibersegurança, o Marco Civil da Internet desempenha um papel crucial ao estabelecer diretrizes claras para a proteção dos dados pessoais e da privacidade dos usuários. A legislação exige que as empresas que coletam e processam dados pessoais cumpram requisitos rigorosos, garantindo a segurança dessas informações e a transparência no tratamento dos dados.

Ademais, a responsabilidade dos provedores de serviços de Internet em relação à segurança cibernética também é estabelecida. Eles devem adotar medidas técnicas e organizacionais adequadas para proteger os dados dos usuários e prevenir ataques cibernéticos. Dessa forma, dando os primeiros passos para a consolidação de técnicas eficazes de segurança cibernética para nosso território.

Ataques cibernéticos ocorridos no Brasil durante a pandemia (COVID-19):

A pandemia da COVID-19 teve um impacto significativo na dinâmica digital global, impulsionando uma maior dependência da tecnologia e do mundo digital para manter as atividades cotidianas. Essa transição acelerada para o ambiente digital resultou em mudanças no cenário da cibersegurança e contribuiu para um aumento nos ataques cibernéticos.

Durante a pandemia, com o aumento do trabalho remoto, ensino a distância e o aumento do

comércio eletrônico, os cibercriminosos encontraram novas oportunidades para explorar vulnerabilidades e realizar ataques cibernéticos. A dependência cada vez maior de plataformas online e a rápida adaptação das organizações e indivíduos ao ambiente digital proporcionaram um terreno fértil para atividades maliciosas.

De acordo com uma análise realizada pelo inside CyberTech Report, ocorreram diversos ataques cibernéticos a grandes corporações brasileiras, incluindo: o Grupo Fleury (com um ataque via ransomware, exigindo um pagamento US$ 5 milhões por meio da criptomoeda monero (XMR) para a recuperação de seus bancos de dados; e a multinacional brasileira JBS S.A (que também sofreu um ataque de ransomware, teve suas operações paradas por quatro dias por conta do ataque e optou por pagar o resgate de US$ 11 milhões em bitcoin para que pudesse retomar suas atividades).

O Superior Tribunal de Justiça e o Tribunal de Justiça do Rio Grande do Sul (TJRS) também foram alvos de ataques cibernéticos, ambos via ransomware, em que os criminosos sequestraram os dados contidos em seus sistemas e exigiram o pagamento em criptomoeda para o resgate dos dados e a retomada das atividades).

Panorama atual e futuro para a cibersegurança no Brasil:

Segundo um estudo realizado pela Checkpoint Software, o terceiro trimestre de 2022 testemunhou um aumento significativo de 37% nos ciberataques registrados no Brasil. Esses dados, combinados com os fatores supracitados, sugerem uma tendência alarmante e preocupante.

Apenas em 2022: a Localiza, Magazine Luiza, Americanas, Mercado Livre, e entre outras empresas brasileiras foram afetadas. O cenário atual é claro: se não forem realizadas intervenções efetivas e abrangentes, é provável que os ataques cibernéticos apenas continuem a aumentar no Brasil. E suas consequências podem se tornar ainda mais graves, incluindo: a interrupção de serviços essenciais, como energia, saúde, transporte e infraestrutura; prejuízos financeiros trilionários (De acordo com os dados levantados Inside REPORT • CYBERTECH, os prejuízos por ataques cibernéticos beiravam a marca de 1 trilhão de dólares em 2020, valor que representava mais de 1% do PIB mundial); e por fim, consequências para a segurança nacional).

2.2. UMA PROPOSTA DE INTERVENÇÃO PARA OS ATAQUES CIBERNÉTICOS OCORRIDOS NO BRASIL

- Essa presente seção ainda está em fase de elaboração. Nesta etapa, será desenvolvida a tese final do projeto, determinando a maneira como as diversas entidades da sociedade brasileira devem se posicionar e se comportar a fim de restaurar a soberania digital brasileira e impedir que novos ataques cibernéticos venham afetar o desenvolvimento e andamento dos sistemas do nosso país. Sua conclusão ocorrerá antes do período estipulado para a entrega final do projeto.

Considerações Finais

A seção de conclusão dessa pesquisa científica está em fase de elaboração e será finalizada antes do período estipulado para a entrega do projeto.

Referências Bibliográficas

CHELLY, M. et al. **The Cyber Defense Index**. Disponível em: <https://mittrinsights.s3.amazonaws.com/CDIreport.pdf>. Acesso em: 15 set. 2023.

Crescimento da internet desacelera e 2,7 bilhões ficam fora da rede. Disponível em: <https://news.un.org/pt/story/2022/09/1801381>. Acesso em: 15 set. 2023.

DA SILVA MENDONÇA, C. **GUERRA CIBERNÉTICA: Desafios de uma Nova Fronteira**. Disponível em: <https://pantheon.ufrj.br/bitstream/11422/3340/1/CMendon%C3%A7a.pdf>. Acesso em: 15 set. 2023.

DAN CRAIGEN, NADIA DIAKUN-THIBAULT, AND RANDY PURSE. **Defining Cybersecurity.** Disponível em: <https://www.researchgate.net/publication/326309769_Defining_Cybersecurity>. Acesso em: 15 set. 2023.

DAVID REINSEL, JOHN GANTZ, JOHN RYDNING. **The digitization of the world from edge to core**. Disponível em: <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-white paper.pdf>. Acesso em: 15 set. 2023.

DE ARAUJO, F. C.; ROSSI, J. M. **A EVOLUÇÃO DOS ATAQUES CIBERNÉTICOS**. Disponível em: <https://ric.cps.sp.gov.br/bitstream/123456789/5272/1/1S2020_Franciele%20Cassimiro%20de%20Ara%C3%BAjo_OD0878.pdf>. Acesso em: 15 set. 2023.

DO NASCIMENTO, N. L. **CRIMES CIBERNÉTICOS**. Disponível em: <https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf>. Acesso em: 15 set. 2023.

MIRANDA, JULIAN & C., VIKRANTH & DHAWAN, PARAG & CHURI, PRATHAMESH. **Exploratory data analysis for cybersecurity**. Disponível em: <https://www.researchgate.net/publication/349407966_Exploratory_data_analysis_for_cybersecurity>. Acesso em: 15 set. 2023.

MONTEIRO, S. D. **O Ciberespaço: o termo, a definição e o conceito**. Disponível em: <https://www.brapci.inf.br/_repositorio/2010/01/pdf_31a590c998_0007547.pdf>. Acesso em: 15 set. 2023.

MUNIZ, L. M. **ESTUDO E PREVISÃO DO CRIME CIBERNÉTICO**. Disponível em: <https://www.ufpe.br/documents/39362/3468937/TCC+-+Estudo+e+Previs%C3%A3o+do+Crime+Cibern%C3%A9tico+-+Lais+Muniz.pdf/26b31608-f3c3-414b-8ffa-ab5e77e6a0ba>. Acesso em: 15 set. 2023.

TEIXEIRA, C. F. **A. SEGURANÇA CIBERNÉTICA EM REDES MODERNAS: COMO PROTEGER E MITIGAR ATAQUES CIBERNÉTICOS**. Disponível em: <https://monografias.ufop.br/bitstream/35400000/3567/1/MONOGRAFIA_Seguran%C3%A7aCibern%C3%A9ticaRedes.pdf>. Acesso em: 15 set. 2023.

WILLIAM, V. et al. **O Papel da Defesa Nacional em Casos de Ataques Cibernéticos: Uma Análise sobre a Necessidade de Protocolo(s) de Prevençção e Atuaççã**o. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/oa_papela_daa_defesaa_nacionala_ema_casosa_dea_ataquesa_ciberneticosa_umaa_analisea_sobrea_aa_necessidadea_dea_protocolos.pdf>. Acesso em: 15 set. 2023.