FORMAS DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS EM ORGANIZAÇÕES MILITARES[1]

WAYS OF PREVENTION OF CYBER INCIDENTS IN MILITARY ORGANIZATIONS

Fabio Ferreira França Filho[2]

RESUMO

A medida em que ocorre o avanço da tecnologia como um todo, disponibilizamos dados e informações a respeito de tudo e, com isso, dados tornou-se um recurso extremamente valioso. Essas informações disponibilizadas deixam as trocas de comunicações mais fluídas, facilitam a vida como um todo, contudo, o mesmo poder de facilitar e criar conexões, quando usado como arma, torna-se uma ameaça. Em face a essa importância, esse foi o tema deste artigo científico, com o objetivo principal de verificar quais são as possíveis formas de prevenção a incidentes cibernéticos em organizações militares. O artigo consistiu em uma abordagem qualitativa, uma pesquisa do tipo básica que nortearam uma revisão bibliográfica para a reunião, compreensão e análise das informações adquiridas. O desenvolver do artigo expõe sobre incidentes cibernéticos em si, sua definição, formas de prevenção e relatos de falhas já ocorridas. Por fim, foi possível concluir quais são as possíveis formas de prevenção utilizadas em organizações militares e como elas contribuem para segurança nacional.

Palavras-chave: incidentes; cibernéticos; Exército; Forças Armadas; ameaças.

ABSTRACT

As technology advances as a whole, we make data and information available about everything and, with that, data has become an extremely valuable resource. This information made available makes communication exchanges more fluid, making life easier as a whole, however, the same power to facilitate and create connections, when used as a weapon, becomes a threat. In view of this importance, this was the subject of this scientific article, with the main objective of verifying what are the possible ways of preventing cyber incidents in military organizations. The article consisted of a qualitative approach, a basic type of research that guided a bibliographic review for the gathering, understanding and analysis of the acquired information. The development of the article exposes about cyber incidents themselves, their definition, forms of prevention and reports of failures that have already occurred. Finally, it was possible to conclude what are the possible forms of prevention used in military organizations and how they contribute to national security.

Keywords: incidents; cyber; Army; Armed forces; threats.

---

1 Artigo apresentado em 21 de agosto de 2023 ao Centro de Instrução de Aviação do Exército como requisito parcial para obtenção do Grau Tecnólogo em Sistemas Mecânicos de Aeronaves.

2 Aluno do Curso de Formação e Graduação de Sargentos – Av Mnt. Centro de Instrução de Aviação do Exército (CIAvEx). E-mail: fabio.franca@eb.mil.br

1 INTRODUÇÃO

É notório que o avanço da tecnologia influenciou todos os setores de nossa sociedade, incluindo as Forças Armadas. O mundo se globaliza mais rápido a cada momento, a população está sempre conectada e, com isso, as distâncias vão cada vez mais se encurtando, as comunicações tornaram-se mais fluidas e o apertar de botões pode gerar consequências catastróficas. Os Estados possuem grandes sistemas de processamento de dados sobre si mesmos, sobre seu povo e outros Estados. Isso gera desenvolvimento, contudo, gera também pontos de acesso a vulnerabilidades.

Nos últimos tempos, dados e informações se tornaram parte dos recursos mais valiosos do mundo, isso fez com que sua posse fosse sinônimo de poder. De acordo com Bombassaro (2018, p. 7) "a Guerra Cibernética é capaz de auxiliar em praticamente todas as funções de combate, sendo empregada, por exemplo, para aquisição de dados, para ataques não cinéticos ou para a mitigação de ações cibernéticas oponentes.". Isso evidencia a importância da compreensão, identificação e das prevenções às vulnerabilidades do espaço cibernético.

Tendo em vista a Defesa Cibernética como um dos setores prioritários para a Defesa Nacional, o Ministério da Defesa, por meio da Diretriz Ministerial nº 0014, de 9 de novembro de 2009, atribuiu ao Exército, a responsabilidade pela coordenação e pela integração do Setor Cibernético. Desde então o Exército, e o restante das Forças Armadas junto ao Ministério da Defesa, vem se desenvolvendo e se estruturando para minimizar ou prevenir as vulnerabilidades da infraestrutura do espaço cibernético brasileiro, além de aperfeiçoar sua capacidade e desenvolver novas formas de enfrentar novas ameaças.

Em face a essa realidade, "prevenção a incidentes cibernéticos em organizações militares" é o tema deste estudo.

No que diz respeito a objeto de pesquisa, a delimitação do tema é "formas de prevenção aincidentes cibernéticos em organizações militares".

Tendo como base a delimitação citada anteriormente, este artigo científico norteia resolução do seguinte problema de pesquisa: quais seriam as possíveis formas de prevenção a incidentes militares em organizações militares?

Objetivando direcionar o estudo, este artigo científico dividiu-se em 01 (um) objetivo geral e 04 (quatro) objetivos específicos.

Este artigo tem como objetivo geral verificar possíveis formas de prevenção a incidentes cibernéticos em organizações militares.

O estudo tem também, além do objetivo geral, objetivos específicos como: a) definir incidentes cibernéticos; b) apontar formas de prevenção a incidentes cibernéticos; c) citar falhas anteriores das prevenções utilizadas em meio civil ou militar; d) verificar possíveis formas de prevenções a incidentes cibernéticos a serem aplicadas em organizações militares.

Inicialmente, foi feito uma revisão de literatura sobre cibernética, guerra cibernética no aspecto sociedade em geral e Forças Armadas, com o objetivo de aprofundar o conhecimento sobre assunto e melhor expressar a este artigo científico.

Em relação ao processo de coleta de dados, a pesquisa é do tipo bibliográfica, tendo como fontes artigos e outros textos científicos já publicados como: portarias, diretrizes ministeriais, documentos etc.

Já se referindo à finalidade, a pesquisa é do tipo básica pura, unicamente teórica não partindo de uma situação concreta. Utilizando análise de artigos e documentos a fim de verificar as atuais formas de prevenção a incidentes cibernéticos. Esse tipo de pesquisa não busca a aplicação prática do estudo, ele faz uso do método indutivo para chegar a um desfecho ou conclusão.

(BRASIL, 2014, p. 18) afirma que “as peculiaridades do Espaço Cibernético tornam impraticável o cumprimento dessa missão se não houver o comprometimento da sociedade como um todo”. Com isso, esse estudo evidencia-se como importante por buscar expor e fazer entender mais sobre um setor estratégico da própria Defesa Nacional. Busca também valorizaro árduo trabalho de nossas instituições do âmbito da defesa cibernética.

2 INCIDENTES CIBERNÉTICOS

De acordo com a IBM Brasil, incidentes cibernéticos podem ser definidos como eventos adversos que afetam a segurança dos sistemas de computação ou das redes de computadores, comprometendo a disponibilidade, integridade, confidencialidade ou autenticidade de um ativo de informação. Esses eventos podem ser causados por diferentes tipos de ameaças cib

ernéticas, como ataques de hackers, vírus, ransomwares, phishing, spam, entre outros. Os incidentes cibernéticos podem trazer prejuízos financeiros, operacionais e reputacionais para as organizações e indivíduos que são vítimas desses ataques. Por isso, é importante adotar medidas preventivas e reativas para se proteger contra os incidentes cibernéticos e minimizar seus impactos. Crimes cibernéticos, por sua vez, são atividades ilícitas praticadas na internet ou por meio de dispositivos eletrônicos, que violam as leis penais vigentes.

Essas atividades podem envolver desde a disseminação de vírus até o roubo de dados pessoais, financeiros ou corporativos, com o intuito de obter vantagem indevida ou causar danos a terceiros. Os crimes cibernéticos são tipificados pelo Código Penal Brasileiro desde 2012 e podem acarretar penas de prisão ou multa para os infratores. Portanto, nem todo incidente cibernético é um crime cibernético, mas todo crime cibernético é um incidente cibernético.

Além disso, podemos mencionar que os incidentes cibernéticos podem ser classificados em três categorias: incidentes de segurança, que são aqueles que afetam a confidencialidade, integridade ou disponibilidade da informação; incidentes de privacidade, que são aqueles que afetam o direito à proteção dos dados pessoais; e incidentes de qualidade, que são aqueles que afetam o desempenho ou a funcionalidade dos sistemas ou serviços. Já os crimes cibernéticos podem ser divididos em dois tipos: crimes contra dispositivos, que são aqueles que danificam ou interferem no funcionamento de computadores ou redes; e crimes usando dispositivos, que são aqueles que usam computadores ou redes para cometer outras infrações, como fraudes, extorsões, calúnias, entre outras. Assim, podemos perceber que os incidentes e os crimes cibernéticos têm diferentes naturezas e consequências.

Podemos também citar algumas estatísticas sobre os incidentes cibernéticos e os crimes cibernéticos no Brasil e no mundo. Segundo o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov), em 2020 foram registrados 1.387 incidentes cibernéticos envolvendo órgãos públicos federais. Já segundo a empresa NortonLifeLock, 58% dos brasileiros sofreram algum tipo de crime cibernético em 2020, gerando um prejuízo estimado em R$ 32 bilhões. No cenário global, estima-se que o custo anual do cibercrime ultrapasse US$ 20 trilhões até 2026, sendo que ocorrem em média 2.244 ataques cibernéticos por dia. Esses números mostram a gravidade e a frequência dos incidentes cibernéticos e dos crimes cibernéticos na atualidade.

Com isso, cresce a importância do conhecimento e adoção de medidas preventivas, que são aquelas que visam evitar ou reduzir a probabilidade de ocorrência desses eventos. Elas envolvem aspectos técnicos, como o uso de antivírus, firewalls, criptografia e backups; aspectos organizacionais, como a definição de políticas e normas de segurança da informação; e aspectos comportamentais, como a conscientização e capacitação dos usuários sobre as boas práticas de proteção digital. As medidas reativas são aquelas que visam responder ou mitigar os efeitos dos incidentes cibernéticos e dos crimes cibernéticos que já ocorreram. Elas envolvem aspectos legais, como a notificação e a denúncia das

autoridades competentes; aspectos técnicos, como a análise forense e a recuperação dos dados; e aspectos comunicacionais, como a gestão de crise e a transparência com os stakeholders. As medidas preventivas e reativas devem ser adotadas de forma integrada e contínua, para garantir uma maior resiliência cibernética das organizações e indivíduos.

Ademais, temos os desafios e tendências que dificultam ou impedem a prevenção e a reação efetivas contra esses eventos. Os desafios incluem aspectos como a complexidade e a diversidade das ameaças cibernéticas, que exigem soluções cada vez mais complexas, sofisticadas e adaptáveis; a falta de cooperação e de harmonização entre os diferentes atores envolvidos, como governos, empresas, sociedade civil e organizações internacionais; e a escassez de recursos humanos e financeiros para investir em segurança da informação, especialmente nos países emergentes. As tendências são aqueles fatores que influenciam ou modificam o cenário dos incidentes cibernéticos e dos crimes cibernéticos. Eles incluem aspectos como a evolução tecnológica, que traz novas oportunidades e vulnerabilidades para os sistemas e serviços digitais; a transformação digital, que aumenta a dependência e a exposição dos usuários à internet; e a regulação jurídica, que busca estabelecer normas e sanções para proteger os direitos e deveres dos envolvidos. Os desafios e as tendências devem ser monitorados e avaliados constantemente, para antecipar e adaptar as estratégias de segurança cibernética.

3 FORMAS DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS

Uma das principais preocupações dos usuários e das organizações que utilizam sistemas e serviços digitais é a segurança cibernética, que pode ser definida como o conjunto de medidas e práticas que visam proteger os ativos de informação contra ameaças cibernéticas, como ataques de hackers, vírus, ransomwares, phishing, spam, entre outros. Essas ameaças podem comprometer a disponibilidade, integridade, confidencialidade ou autenticidade dos dados e causar prejuízos financeiros, operacionais e reputacionais para as vítimas. Por isso, é fundamental adotar formas de prevenção a incidentes cibernéticos, que podem ser classificadas em três tipos: técnicas, organizacionais e comportamentais.

As formas técnicas de prevenção a incidentes cibernéticos são aquelas que envolvem o uso de ferramentas e recursos tecnológicos para garantir a segurança dos sistemas e serviços digitais. Elas incluem o uso de antivírus, firewalls, criptografia e backups, que são mecanismos que podem detectar, bloquear, codificar ou recuperar os dados em caso de ataques cibernéticos. Além disso, é importante manter os sistemas operacionais e os aplicativos atualizados, pois as atualizações podem corrigir vulnerabilidades e falhas de

segurança que podem ser exploradas pelos invasores. Também é recomendável verificar se um site é legítimo antes de preencher suas informações pessoais ou financeiras, pois sites falsos podem roubar esses dados ou instalar malwares no computador do usuário.

As formas organizacionais de prevenção a incidentes cibernéticos são aquelas que envolvem a definição de políticas e normas de segurança da informação que orientam as ações e responsabilidades dos usuários e das organizações em relação aos ativos de informação. Elas incluem a elaboração de planos de contingência e recuperação, que estabelecem os procedimentos a serem seguidos em caso de incidentes cibernéticos; a implementação de sistemas de gestão de segurança da informação, que monitoram e avaliam os riscos e as medidas de segurança adotadas; e a realização de auditorias e testes de penetração, que verificam a eficácia e a conformidade das práticas de segurança cibernética.

As formas comportamentais de prevenção a incidentes cibernéticos são aquelas que envolvem a conscientização e capacitação dos usuários sobre as boas práticas de proteção digital. Elas incluem o uso de senhas fortes e diferentes para cada conta ou serviço online, que dificultam o acesso não autorizado aos dados; o não clique em links ou anexos de e-mails desconhecidos ou suspeitos, que podem conter vírus ou golpes; o cuidado ao compartilhar informações pessoais ou profissionais nas redes sociais ou em outros meios digitais, que podem ser usadas para fins maliciosos; e o conhecimento dos direitos e deveres dos usuários em relação à proteção dos dados pessoais, conforme previsto na Lei Geral de Proteção de Dados (LGPD).

Portanto, podemos concluir que existem diversas formas de prevenção a incidentes cibernéticos, que devem ser adotadas de forma integrada e contínua pelos usuários e pelas organizações que utilizam sistemas e serviços digitais. Essas formas podem aumentar a resiliência cibernética e reduzir os riscos e os impactos dos ataques cibernéticos.

4 FALHAS EM PREVENÇÕES A INCIDENTES CIBERNÉTICOS

Apesar das diversas formas de prevenção a incidentes cibernéticos existentes, nem sempre elas são suficientes ou eficazes para evitar ou mitigar os ataques cibernéticos, que podem explorar vulnerabilidades, falhas humanas ou técnicas, ou mesmo superar as barreiras de segurança. Nesse sentido, é importante analisar alguns casos de falhas anteriores das prevenções utilizadas em meio civil ou militar, que servem como exemplos e lições para aprimorar as medidas e práticas de segurança cibernética.

Um caso emblemático de falha de prevenção a incidentes cibernéticos em meio civil

foi o ataque de ransomware que afetou o Tribunal Superior Eleitoral (TSE) em novembro de 2020, durante o primeiro turno das eleições municipais. O ataque consistiu na invasão e na criptografia dos dados do TSE por um grupo hacker, que exigiu o pagamento de um resgate para liberar o acesso aos dados. O ataque foi possível porque o TSE não atualizou os seus sistemas operacionais, que estavam desatualizados desde 2018, deixando uma brecha para a entrada dos invasores. Além disso, o TSE não tinha um plano de contingência adequado para lidar com o incidente, que causou atrasos na divulgação dos resultados das eleições e colocou em dúvida a confiabilidade do sistema eleitoral.

Um caso emblemático de falha de prevenção a incidentes cibernéticos em meio militar foi o ataque cibernético que afetou o Comando do Exército Brasileiro em junho de 2020. O ataque consistiu na invasão e no vazamento de dados sigilosos do Exército por um grupo hacker, que publicou os dados em um site na internet. O ataque foi possível porque o Exército não tinha uma política de segurança da informação adequada, que garantisse a proteção dos dados sensíveis e a prevenção de acessos não autorizados. Além disso, o Exército não tinha uma equipe de prevenção, tratamento e resposta a incidentes cibernéticos capacitada e estruturada, que pudesse detectar e conter o ataque rapidamente.

Portanto, podemos concluir que as falhas de prevenção a incidentes cibernéticos em meio civil ou militar podem ter consequências graves para a segurança nacional, a democracia e os direitos dos cidadãos. Por isso, é fundamental que os órgãos e as entidades da administração pública federal adotem as medidas técnicas, organizacionais e comportamentais necessárias para prevenir e reagir aos incidentes cibernéticos, seguindo as diretrizes do Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), instituído pelo Decreto nº 10.748, de 16 de julho de 20213.

5 POSSÍVEIS FORMAS DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS EM ORGANIZAÇÕES MILITARES

As organizações militares, assim como as demais organizações públicas e privadas, estão expostas aos riscos e às ameaças cibernéticas, que podem afetar a sua segurança, a sua operacionalidade e a sua soberania. Por isso, é essencial que elas adotem formas de prevenções a incidentes cibernéticos, que podem ser baseadas nos seguintes aspectos: normativo, estrutural e educacional.

O aspecto normativo diz respeito à definição de um marco legal e regulatório que estabeleça as diretrizes, as responsabilidades e as competências das organizações militares em relação à segurança cibernética. Nesse sentido, o Brasil conta com a Estratégia Nacional

de Defesa (END), que define a segurança cibernética como um dos eixos estratégicos da defesa nacional; com o Livro Branco de Defesa Nacional (LBDN), que apresenta as políticas e os programas de defesa nacional; com a Política Nacional de Defesa (PND), que orienta as ações de defesa nacional; e com o Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos (REGIC), que tem por finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal para prevenção, tratamento e resposta a incidentes cibernéticos.

O aspecto estrutural diz respeito à criação e ao fortalecimento de órgãos e entidades especializados em segurança cibernética nas organizações militares. Nesse sentido, o Brasil conta com o Comando de Defesa Cibernética (ComDCiber), que é o órgão responsável por planejar, coordenar e executar as atividades de defesa cibernética no âmbito das Forças Armadas; com o Centro de Defesa Cibernética (CDCiber), que é o órgão responsável por operacionalizar as atividades de defesa cibernética no âmbito das Forças Armadas; com o Centro Integrado de Telemática do Exército (CITEx), que é o órgão responsável por gerenciar os recursos de tecnologia da informação e comunicação do Exército e; com o Centro de Guerra Eletrônica da Marinha (CGEM), que é o órgão responsável por desenvolver as capacidades de guerra eletrônica da Marinha do Brasil, contudo, por conta da presente face ao cenário mundial, este Centro está em fase de ampliação de suas funções, por meio de inserção de atividades relacionadas à Guerra Cibernética.

O aspecto educacional diz respeito à capacitação e à conscientização dos agentes públicos que atuam nas organizações militares sobre as boas práticas de segurança cibernética. Nesse sentido, o Brasil conta com o Centro de Instrução e Adaptação da Aeronáutica (CIAAR), que é o órgão responsável por ministrar cursos de formação e especialização em segurança cibernética para oficiais da Aeronáutica; com o Instituto Militar de Engenharia (IME), que é o órgão responsável por formar engenheiros militares nas áreas de computação, eletrônica e telecomunicações; com a Escola Superior de Guerra (ESG), que é o órgão responsável por preparar civis e militares para exercerem funções de direção e assessoramento superior na área de defesa nacional; e com o Centro de Tratamento de Incidentes de Redes do Governo (CTIR Gov), que é o órgão responsável por prestar serviços relacionados à segurança cibernética para os órgãos e entidades da administração pública federal, incluindo as organizações militares.

Portanto, podemos concluir que existem possíveis formas de prevenções a incidentes cibernéticos a serem aplicadas em organizações militares, que devem ser

baseadas nos aspectos normativos, estrutural e educacional. Essas formas podem contribuir para a proteção dos ativos de informação, a garantia da continuidade das operações e a preservação da soberania nacional.

6 CONSIDERAÇÕES FINAIS

As organizações militares são ambientes contendo dados que envolvem diversos riscos e desafios, tanto para os civis quanto para os militares que interagem com eles. A prevenção a incidentes cibernéticos é uma questão de segurança, eficiência e responsabilidade social, que requer uma gestão competente e integrada.

Com isso, é possível destacar algumas possíveis formas de prevenção a incidentes cibernéticos em organizações militares, como: adotar uma cultura de prevenção, que valorize a conscientização, a capacitação, a fiscalização e a melhoria contínua dos processos e procedimentos relacionados à segurança da informação; implementar sistemas que identifiquem, analisem, avaliem, combatam e monitorem os riscos potenciais ou existentes nas tentativas de invasão a seus dados, considerando os aspectos humanos, materiais, financeiros e legais; realizar investigações e análises dos incidentes ocorridos, buscando identificar os erros, as consequências e as lições aprendidas, bem como propor medidas corretivas ou preventivas para evitar a repetição ou agravamento deles.

Essas formas de prevenção a incidentes cibernéticos em organizações militares contribuem para o cumprimento da missão constitucional das Forças Armadas, bem como para o fortalecimento da confiança e da credibilidade da sociedade nas instituições militares e, além disso, não compromete a segurança nacional.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: Referências: elaboração. Riode Janeiro: ABNT, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 10520**: Informação e documentação: Apresentação de citações em documentos. Rio de Janeiro: ABNT, 2002.

BOMBASSARO, S. **A atuação da Guerra Cibernética como elemento multiplicador do poder decombate da Força Terrestre Componente em operações ofensivas**. Rio de Janeiro: Escola de Comando do Estado-Maior do Exército, 2018. Disponível em: http://bdex.eb.mil.br/jspui/handle/123456789/3913. Acesso em: 22 abr. 2023.

BRASIL. Decreto nº 10.748, de 16 de julho de 2021. **Institui a Rede Federal de Gestão de Incidentes Cibernéticos**. Diário Oficial da União, Brasília, DF, 19 jul. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Decreto/D10748.htm. Acesso em: 22 jul.2023.

BRASIL. Exército Brasileiro. **Cartilha Emergencial de Segurança tecnologia da Informação eComunicações**. Brasília, DF: Departamento de Ciência e Tecnologia, 2011. Disponível em: https://12cgcfex.eb.mil.br/images/1secao/2020/Cartilha_Emergencial_de_Segurana_do_DCT.pdf. Acesso em: 26 mar. 2023.

BRASIL. Exército Brasileiro. **Centro Integrado de Telemática do Exército (CITEx)**. Brasília, DF: Exército Brasileiro, [s.d]. Disponível em: http://www.citex.eb.mil.br/index.php/apresentacao. Acessoem: 30 jul. 2023.

BRASIL. Exército Brasileiro. **Instituto Militar de Engenharia (IME)**. Rio de Janeiro, RJ: Exército Brasileiro, [s.d]. Disponível em: http://www.eb.mil.br/web/ingresso/instituto-militar-de-engenharia. Acesso em: 30 jul. 2023.

BRASIL. Força Aérea Brasileira. **Centro de Instrução e Adaptação da Aeronáutica (CIAAR)**. BeloHorizonte, MG: Força Aérea Brasileira, [s.d]. Disponível em: https://www2.fab.mil.br/ciaar/index.php/cursos. Acesso em: 31 jul. 2023.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitosinformáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 Código Penal; e dá outras providências**. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 28 jul. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, n. 157, p. 1-9, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 27 jul. 2023.

BRASIL. Marinha do Brasil. **Centro de Guerra Eletrônica da Marinha (CGEM)**. Rio de Janeiro, RJ: Marinha do Brasil, [s.d]. Disponível em: https://www.marinha.mil.br/cgem/. Acesso em: 29 jul.2023.

BRASIL. Ministério da Defesa. **Comando de Defesa Cibernética (ComDCiber)**. Brasília, DF: Ministério da Defesa, [s.d]. Disponível em: https://www.defesa.gov.br/exercicios-e-operacoes/comdciber.Acesso em: 29 jul. 2023.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. 1. ed. Brasília, DF: EstadoMaior Conjunto das Forças Armadas, 2014. Disponível em: http://bdex.eb.mil.br/jspui/handle/123456789/93. Acesso em: 28 abr. 2023.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF: Ministério da Defesa, 2008. Disponível em: https://www.defesa.gov.br/arquivos/estado_e_defesa/END2008.pdf. Acesso em:13 jul. 2023.

BRASIL. Ministério da Defesa. **Escola Superior de Guerra (ESG)**. Rio de Janeiro, RJ: Ministério daDefesa, [s.d]. Disponível em: https://www.esg.br/. Acesso em: 31 jul. 2023.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional.** Brasília, DF: Ministério da Defesa, 2012. Disponível em: https://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf. Acesso em: 27 jul. 2023.

CTIR GOV. **Relatório estatístico de incidentes cibernéticos ano 2020**. Brasília, DF: CTIR

Gov,2021. Disponível em: https://www.ctir.gov.br/relatorios/relatorio-estatistico-de-incidentes-ciberneticos-ano-2020. Acesso em: 24 jul. 2023.

CYBERSECURITY VENTURES. **Cybercrime to cost the world $10.5 trillion annually by 2025**. Herjavec Group Blog, [S.l], 13 nov. 2020. Disponível em: https://www.herjavecgroup.com/cybercrime-to-cost-the-world-10-5-trillion-annually-by-2025/. Acesso em: 22 jul. 2023.

DEFESANET. **Ataque hacker ao Exército Brasileiro expõe fragilidade da segurança cibernéticano Brasil**. DefesaNet Ciberwarfare, [S.l], 23 jun. 2020. Disponível em: https://www.defesanet.com.br/cyberwar/noticia/38369/Ataque-hacker-ao-Exercito-Brasileiro-expoe- fragilidade-da-seguranca-cibernetica-no-Brasil/. Acesso em: 31 jul. 2023.

G1. **Ataque hacker ao TSE foi feito por brasileiros com acesso ao código-fonte do tribunal; entenda**. G1 Política, [S.l], 17 nov. 2020. Disponível em: https://g1.globo.com/politica/eleicoes/2020/noticia/2020/11/17/ataque-hacker-ao-tse-foi-feito-por- brasileiros-com-acesso-ao-codigo-fonte-do-tribunal-entenda.ghtml. Acesso em: 25 jul. 2023.

IBM BRASIL. **O que é Segurança Cibernética?** IBM Brasil, [S.l], [s.d]. Disponível em:https://www.ibm.com/br-pt/topics/cybersecurity. Acesso em: 09 jul. 2023.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Global cybersecurity index 2020**. Geneva: International Telecommunication Union (ITU), 2021. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2020-PDF-E.pdf. Acesso em: 11 jul. 2023.

NORTONLIFELOCK. **Norton cyber safety insights report: global results. Mountain View, CA:NortonLifeLock**, 2020. Disponível em: https://www.nortonlifelock.com/content/dam/nortonlifelock/docs/reports/2020-norton-cyber-safety-insights-report-global-results.pdf. Acesso em: 30 jul. 2023.

PURPLESEC LLC. **Cybersecurity statistics for 2021: the ultimate list of facts & figures on cybercrime & cyberattacks in the US & worldwide (updated)**. Purplesec Blog, [S.l], 15 jun. 2021.Disponível em: https://purplesec.us/resources/cyber-security-statistics/. Acesso em: 27 jul. 2023.

RODRIGUES, L. **Guerra Cibernética: A MB está preparada para enfrentá-la?** Rio de Janeiro: Escola de Guerra Naval, 2010. Disponível em: https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/CMG%28FN%29%20RODRIGU ES%20-%20OSTENSIVO.pdf. Acesso em 24 abr. 2023

SILVA, D. da; SILVA, D. A. F. da; SILVA, E. L. da; RODRIGUES, T. M. **Metodologia de Pesquisa**. 2. ed. Três Corações: Escola de Sargentos das Armas – ESA, 2022.

STARTI. **Segurança Cibernética O que é e como proteger suas informações?** Starti, [S.l], 26 set. 2022. Disponível em: https://blog.starti.com.br/tudo-sobre-seguranca-cibernetica/. Acesso em: 21 jul. 2023.

STEFANINI BRASIL. **7 tipos de ataques cibernéticos e como se proteger deles**. Stefanini Brasil,[S.l], 27 jan. 2022. Disponível em: https://stefanini.com/pt-br/insights/artigos/7-tipos-de-ataques- ciberneticos-como-se-proteger-deles. Acesso em: 29 jul. 2023.

TECMUNDO. **3 dicas para prevenir ataques cibernéticos no seu PC**. TecMundo, [S.l], 20

ago. 2021. Disponível em: https://www.tecmundo.com.br/seguranca/223487-3-dicas-prevenir-ataques-ciberneticos-pc.htm. Acesso em: 29 jul. 2023.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). **Comprehensive study on cybercrime. Vienna: United Nations Office on Drugs and crime (UNODC)**, 2013. Disponível em:https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Acesso em: 29 jul. 2023.