# Constituição de uma base de competência técnica em defesa e segurança cibernética no âmbito acadêmico

*Diogo Bezerra Borges[1], Sônia Marise Salles Carvalho[2], Helton Alanderson Viana[3], Paula Meyer Soares[4]*

**Resumo**

O presente artigo aborda alguns aspectos relevantes que dizem respeito à constituição de uma base de competência técnica nas universidades para tratar das questões de *defesa cibernética* e *segurança cibernética*. Para tanto, os autores optaram por realizar uma pesquisa aplicada ao grupo de estudantes do curso de Engenharia de Redes de Comunicação da Universidade de Brasília (UnB), com o propósito de verificar a percepção deles em relação ao tema, suas perspectivas de cooperação tecnológica e atuação profissional. Ao final do trabalho, foi possível dispor de informações importantes que evidenciaram as possibilidades de cooperação entre a Universidade de Brasília

**Abstract**

*This article addresses some relevant aspects that concern the constitution of a technical competence base in universities to deal with the issues of cyber defense and cybersecurity. For this purpose, the authors chose to conduct a survey applied to a group of students of the Communication Networks Engineering course at the University of Brasilia (UnB), to verify their perception concerning the theme, their perspectives of technological cooperation, and professional performance. At the end of the work, important information that highlighted the possibilities of cooperation between the University of Brasilia (UnB) and the Cyber Defense Command (ComDCiber) was obtained. The goal of this*

1 Mestrado em Administração pela Universidade do Estado de Santa Catarina (Udesc). Analista em Ciência e Tecnologia do Ministério da Ciência, Tecnologia e Inovações (MCTI).

2 Doutorado em Sociologia pela Universidade de Brasília (UnB). Professora associada da Universidade Federal do Amazonas (UFAM) e, atualmente, em exercício provisório no Centro de Apoio ao Desenvolvimento Tecnológico (CDT/UnB).

3 Especialização em Direito Público pela Faculdade Casa Branca, no município de Casa Branca, em São Paulo. Advogado e ex-assessor jurídico do Departamento de Gestão Estratégica do Comando de Defesa Cibernética.

4 Bacharel em Ciências Econômicas pela Universidade de Fortaleza (Unifor) (1990), mestre e doutora em Economia pela Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas (FGV-Eaesp). Professora da Faculdade UnB Gama (FGA) e do Programa de Pós-graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação (Profnit) da UnB.

(UNB) e o Comando de Defesa Cibernético (ComDCiber), com o objetivo de prover ações que permitam despertar, nos universitários, o interesse pela carreira no campo cibernético, assim como identificar talentos que futuramente possam compor a base de competência técnica no País.

**Palavras-chave:** Defesa cibernética. Segurança cibernética. Cooperação tecnológica. Formação de pessoal. Perspectiva profissional.

*cooperation is to provide actions that stimulate college students to work in the cyber field, as well as identify talents that in the future may compose the technical competence base in the country.*

***Keywords:*** *Cyber defense. Cyber security. Technological cooperation. Staff training. Professional perspective.*

# 1. Introdução

## 1.1. Setor de defesa e mobilização do ecossistema de inovação

O contexto histórico tem demonstrado a importância do ecossistema de inovação e do empreendedorismo tecnológico como um dos fatores essenciais para o desenvolvimento econômico regional e/ou nacional. A formação do Vale do Silício, na Califórnia, Estados Unidos (EUA), se apresenta como um claro exemplo no qual a ciência, a tecnologia, a inovação e o empreendedorismo tecnológico tiveram papel fundamental na constituição de um polo tecnológico bem-sucedido. A origem desta iniciativa remete a 1957, quando um grupo de oito cientistas e engenheiros resolveu criar uma empresa fabricante de transistores, denominada *Fairchild Semiconductors*. A empresa formada por esse grupo obteve, inicialmente, o aporte de recursos por parte de um capitalista de risco, além de o seu comprometimento em auxiliá-los nos primeiros contratos de venda à IBM. Esse relacionamento comercial inicial proporcionou à nova empresa de semicondutores um ganho de credibilidade que lhe permitiu assegurar um prestigioso contrato de fornecimento de componentes eletrônicos para um programa de mísseis intercontinentais do governo americano (ENDEAVOR BRASIL, 2014).

No contexto da Guerra Fria, as encomendas tecnológicas realizadas pelo Departamento de Defesa Americano exerceram importância significativa para o sucesso e o crescimento do Vale do Silício. O surgimento de diversas empresas ocorreu num período em que a sociedade americana buscava a supremacia tecnológica perante a União das Repúblicas Socialistas Soviéticas (URSS) (CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS - CGEE, 2013). Segundo Dosi (1984), o Vale do Silício se consolidou como um subproduto dos gastos em Pesquisa e Desenvolvimento (P&D)

do setor militar. Entre as décadas de 1960 e 1970, mais de 90% da demanda de semicondutores produzidos naquela região tinha como origem as compras governamentais derivadas do complexo militar (DOSI, 1984). As respectivas demandas garantiram a lucratividade empresarial nos campos mais incipientes e a consequente difusão do conhecimento tecnológico nos diferentes setores da indústria do país. Além disso, o Departamento de Defesa Americano exerceu um papel relevante no apoio às pesquisas, por meio do financiamento de diversos departamentos de ciência da computação em universidades dos EUA, incluindo um laboratório ligado à Universidade da Carolina do Sul, fundamental para a fabricação de *chips* (CGEE, 2013).

Nesse contexto, Mazzucato (2011) destaca a importância estratégica do Estado no desenvolvimento de grandes avanços tecnológicos. Como argumentos, a autora cita que o surgimento de determinadas tecnologias não ocorreu por uma visão puramente estratégica do setor privado, mas pela insistência do governo no seu desenvolvimento. A tecnologia em rede (ARPANET)[5] (WIKIPÉDIA) é citada como um dos projetos decorrentes do esforço da pesquisa tecnológica no período da Guerra Fria e que, posteriormente, deu origem à internet (MAZZUCATO, 2011). As primeiras transmissões em *wireless* também contariam com o apoio central do *Defense Advanced Research Projects Agency* (DARPA). A respectiva agência foi a principal financiadora no desenvolvimento dos computadores pessoais, algo vital para a difusão da tecnologia e para o estímulo do desenvolvimento de *software* (CGEE, 2013). Além do financiamento dos projetos, a agência se destaca na criação de empresas de tecnologia, tais como: Sun Microsystems, Apple, Silicon Graphics, Inc., Cisco Systems, Fore, IBM, Compaq, NCR, Cray Research, Hewlett Packard, Intel, Motorola, Analog Devices, Cisco, Bay Networks, Precept, Intel, IBM (DEFENSE ADVANCED RESEARCH PROJECTS AGENCY – DARPA, 2008).

Uma das razões que colocaram os EUA na vanguarda tecnológica foi justamente o êxito na aproximação entre a esfera produtiva e os centros de pesquisa públicos/universidades (CGEE, 2013). No caso brasileiro, também é possível verificar casos exitosos no desenvolvimento de tecnologias, que envolveram a conjugação de esforços entre as instituições de pesquisa e o setor industrial. Tem-se como exemplo o plano *Smith-Montenegro*, que visava, no longo prazo, ao alcance da capacidade produtiva aeronáutica no País. Esse plano foi responsável pela criação das primeiras instituições de ensino e pesquisa com competência tecnológica no setor aeroespacial (RODENGEN, 2009), como o Centro Tecnológico da Aeronáutica (CTA), no qual teve origem a primeira escola de engenharia aeronáutica, denominada Instituto Tecnológico de Aeronáutica

5 A Advanced Research Projects Agency Network (Arpanet) [em português: Rede da Agência para Projetos de Pesquisa Avançada] foi uma rede de comutação de pacotes e a primeira rede a implementar o conjunto de protocolos TCP/IP. Ambas as tecnologias se tornaram a base técnica da Internet. A Arpanet foi inicialmente financiada pela Agência de Projetos de Pesquisa Avançada (Arpa) do Departamento de Defesa dos Estados Unidos (WIKIPÉDIA).

(ITA). Em 1954 foi criado o Instituto de Pesquisa e Desenvolvimento (IPD), de onde vieram, posteriormente, os primeiros produtos da Embraer (FONSECA, 2012). A aproximação com universidades foi um dos facilitadores que contribuíram para que essa empresa ingressasse no seleto grupo de companhias aeroespaciais e de defesa do mundo. Isso foi possível graças à combinação entre a engenharia criativa do brasileiro e a excelência educacional na formação de engenheiros aeronáuticos (EMBRAER, 2019).

Cabe destacar que, pelos exemplos apresentados, os projetos estratégicos militares brasileiros e americanos envolveram o esforço de desenvolvimento tecnológico e de formação de pessoal por parte das universidades e dos institutos de pesquisa. Nesse sentido, considera-se primordial a realização de estudos que permitam subsidiar as instituições governamentais civis ou militares na formação de uma base de competência técnica nas universidades, com capacidade para atender às necessidades tecnológicas dos programas estratégicos inseridos nas políticas de defesa. No contexto deste trabalho, optou-se pela escolha do tema *defesa cibernética* diante da relevância que vem ganhando ao longo dos anos. Para tanto, a pesquisa aqui apresentada teve o propósito de verificar a percepção dos alunos em relação ao tema, suas perspectivas de cooperação tecnológica e profissionais. No que diz respeito à metodologia, optou-se por uma pesquisa exploratória e descritiva, na qual se adotou o grupo focal como técnica de coleta e de análise de dados.

## 2. Referencial teórico

### 2.1. Guerra cibernética: relevância nos conflitos internacionais e vulnerabilidades no território nacional

Percebe-se, cada vez mais, que o avanço tecnológico tem estimulado uma reflexão nas táticas de guerra atuais. Certamente, a guerra do futuro fará uso intensivo de informações do campo de batalha em tempo real. Do mesmo modo, será crescente o uso de: armas dirigidas ou remotamente tripuladas; mísseis de cruzeiro guiados por satélite/GPS e drones; sistemas de vigilância e análise de múltiplos alvos; e *software* embarcado. Será evidente, ainda, o uso intenso de emissões eletromagnéticas, além da guerra cibernética nas operações militares (GAMA NETO, 2017). Os autores ressaltam que não apenas a China, mas várias outras nações vêm se preparando para o campo de batalha cibernético, por meio de "bombas lógicas" e "*backdoors*" (CLARKE; KNAKE, 2010). Recente reportagem, publicada pela *Bloomberg*, noticiou um possível caso de espionagem

que envolveu um pequeno *chip* inserido em placas-mães. Esse componente eletrônico permitiu aos chineses o acesso a dados sigilosos de instituições governamentais, incluindo o Departamento de Defesa Nacional e a Agência de Inteligência Americana (ROBERTSON; RILEY, 2018).

Em relação ao Brasil, a imprensa noticiou alguns casos de ataques cibernéticos e até mesmo ações de espionagem direcionadas às instituições governamentais. Um caso nacionalmente conhecido diz respeito à divulgação de informações advindas de ações de espionagens direcionadas à então presidente da república, Dilma Rousseff, e seus assessores. Após conhecimento do respectivo episódio, autoridades brasileiras determinaram a criação da Comissão Parlamentar de Inquérito (CPI), com o propósito de apurar as denúncias de espionagem estrangeira. O relatório final da Comissão constatou a vulnerabilidade do Brasil diante de ações de espionagem. Documentos apontaram que o País foi um dos alvos preferenciais do serviço de inteligência norte-americano (BRASIL, 2014). Duas outras ocorrências demonstraram a vulnerabilidade do Brasil no que diz respeito à proteção de sistemas das instituições governamentais. Um deles ocorreu em 2014, quando *hackers* direcionaram seus ataques ao sistema do Ministério das Relações Exteriores (MRE) (NETO; BENTES, 2014). Outro caso de ataque cibernético foi registrado em 2015 e teve como alvo os sistemas do Exército Brasileiro (GLOBO.COM, 2015).

Diante desse cenário, compreende-se a necessidade do empreendimento esforços no desenvolvimento de tecnologias nacionais que permitam conter o risco de *software* e *hardware* importados e códigos maliciosos capazes de expor os sistemas nacionais à invasão inimiga. É de fundamental importância, ainda, reduzir as importações e produzir o máximo de componentes, *hardware* e *software* voltados para a transmissão de dados, além de dispositivos para prover a segurança da informação. Para isso, serão essenciais os investimentos na indústria de defesa e os incentivos apoiados pelo governo federal (MOREIRA; CORDEIRO, 2014). Na esfera nacional, a temática *Cibernética* encontra-se inserida no âmbito de políticas e estratégias, por meio das seguintes abordagens: (1) Política de Defesa; (2) Estratégia Nacional de Defesa; e (3) Estratégia Nacional de Ciência, Tecnologia e Inovação (ENCTI).

## 2.2. A inserção da temática *Cibernética* na política e na estratégia de defesa nacionais

A Política Nacional de Defesa (PND) é o documento condicionante de mais alto nível do planejamento de ações coordenadas pelo Ministério da Defesa. Nele, são estabelecidos objetivos e orientações para o preparo e o emprego dos setores (militar e civil) em prol da defesa nacional. O documento reforça a importância do setor cibernético como estratégico para o País. A Estratégia

Nacional de Defesa trata de questões políticas e institucionais decisivas para a defesa do País. Dentre as prioridades, encontram-se a capacitação, o preparo e o emprego dos poderes cibernéticos em prol das operações conjuntas e da proteção das infraestruturas estratégicas. (BRASIL, 2012).

O Ministério da Defesa atribuiu ao Comando de Defesa Cibernética (ComDCiber) a responsabilidade pela coordenação e integração das atividades do setor. Por sua vez, criou o Programa da Defesa Cibernética, com a finalidade de incrementar as atividades de capacitação, doutrina, ciência, tecnologia e inovação (CT&I), inteligência e operações. Dentre as ações do Programa, é relevante citar a criação da Escola Nacional de Defesa Cibernética (ENaDCiber). Essa instituição tem como propósito capacitar recursos humanos, civis e militares, de modo a proporcionar a pronta resposta às ameaças cibernéticas. (BRASIL, 2019b).

A Estratégia Nacional de Ciência, Tecnologia e Inovação (ENCTI 2016-2022) (BRASIL, 2018) converge com a Política de Defesa e a Estratégia Nacional de Defesa, por ressaltar que as facilidades proporcionadas pelo rápido avanço das tecnologias e as crescentes preocupações com a segurança cibernética colocaram a temática *cibernética* como prioritária nas políticas de CT&I. Nessa perspectiva, a ENCTI 2016-2022 reforça o comprometimento do Ministério da Ciência, Tecnologia e Inovações (MCTI) no apoio ao programa de defesa cibernética, por meio da pesquisa em segurança de sistemas e aplicações voltadas para comércio eletrônico, transações bancárias e análise de *malware*. Nesse sentido, será de fundamental importância, por parte das universidades, a formação de pessoal com perfil inovador, capaz de contribuir para o desenvolvimento econômico e social do País (BRASIL, 2018).

## 2.3. Constituição da base de competência técnica: mobilização, estratégias de atração e perspectiva profissional

Para Klimburg (2011), países do Ocidente, com destaque para os Estados Unidos, têm sido relativamente lentos na mobilização da base de competência técnica em defesa cibernética. Diferentemente, países como a Rússia e a China se encontram bem avançados na constituição de uma base de competência técnica apta a realizar ataques cibernéticos e defender suas infraestruturas críticas. No âmbito do programa de Reserva da China, muitos estudantes da área de tecnologia da informação e comunicação são automaticamente considerados como parte da organização de defesa nacional. O país detém mais de 25 milhões de estudantes em universidades públicas, não incluindo aqueles em treinamento privado ou programas técnicos especializados. No que diz respeito à Rússia, o autor também cita a responsabilidade daquela nação por uma série de ataques. Como estratégia de mobilização, os serviços de segurança

russos buscam cooptar ou recrutar criminosos cibernéticos e patriotas *hackers*, para que muitos deles operem contra as forças antirrussas (KLIMBURG, 2011).

Apesar do posicionamento crítico do autor em relação à morosidade do governo americano no que se refere à mobilização da sociedade civil, percebe-se, no atual contexto, a realização de algumas ações nesse sentido por parte dos EUA. Alguns congressistas apresentaram uma proposta de criação do sistema de reserva nacional de segurança cibernética. Para um dos deputados que defende a proposta, a constituição da respectiva reserva ajudaria no fortalecimento da segurança nacional. Diversos especialistas da área de segurança cibernética têm manifestado opiniões contrárias ou favoráveis. Como argumento favorável, justifica-se que muitos patriotas poderiam atuar na defesa nacional quando necessário (KOROLOV, 2017).

Um dos desafios relativos ao recrutamento corresponde à falta de conhecimento dos jovens a respeito do serviço militar e das oportunidades de atuação no âmbito do governo americano. Segundo Westermeyer (2008), existem algumas iniciativas para amenizar essa escassez de informações por parte da população desta faixa etária em relação ao papel das forças armadas. Como exemplo, o Departamento de Defesa criou um programa denominado "*Why You Serve*?", por meio do qual os veteranos são convidados a compartilharem os motivos que os levaram a ingressar nas forças armadas, além de relatarem suas experiências vivenciadas no exterior. De forma similar, o "*Eisenhower Series College Program*" é um programa de extensão estabelecido pelo Exército com o propósito de encorajar a discussão no tocante à segurança nacional. Para Westermeyer (2008), um programa semelhante, por parte do Comando do Ciberespaço Americano, seria relevante para contribuir nos esforços de divulgação de suas ações. Outra frente de atuação proposta pelo autor diz respeito à necessidade de as instituições militares expandirem suas capacidades de recrutamento via internet, por meio de mensagens *on-line*, utilização de *podcasting*, participação em redes sociais e preparação de vídeos com dicas de carreiras para divulgação na *web*, além de produção e disponibilização de *games* relacionados à Guerra Cibernética (WESTERMEYER, 2008).

Outra forma importante de contribuição para o sucesso no recrutamento da nova geração ocorreria com o apoio de familiares. Os esforços de sensibilização mencionados também poderiam ser realizados em: fóruns frequentados por pais, avós e professores de jovens; feiras de ensino médio e universitário; eventos comunitários, festivais e reuniões nas cidades. Nessas oportunidades, poderiam ser destacados fatores relevantes como os dizem respeito aos inúmeros benefícios educacionais disponibilizados aos jovens que venham a ingressar na Força Aérea. Um diploma universitário é comumente aceito como o caminho para o sucesso na América, contudo, as despesas são relativamente elevadas. A promoção dos mencionados benefícios

educacionais e de treinamentos teria um forte apelo entre a *geração do milênio*, além de ser um forte argumento no processo de convencimento dos familiares. Outra vantagem no campo da educação corresponde ao programa federal de reembolso de empréstimos estudantis. Um estudo de 2005, do "*Office of Personnel Management*", constatou que mais de três quartos das agências que usam o programa relataram seu impacto positivo. A Força Aérea deveria maximizar o uso desse programa para atrair recém-formados. (WESTERMEYER, 2008).

No que se refere à formação de pessoal, Starr (2009) declara haver uma insatisfação por parte do setor empresarial dos EUA em relação à qualidade e quantidade de especialistas em segurança de computadores. Além disso, há uma desconexão entre o ensino realizado nas universidades e as demandas do governo e do setor privado. Para o autor, existe uma grande base de talentos com potencial e não aproveitada no campo cibernético. Como forma de superar essas deficiências, ele recomenda a realização de competições nacionais entre estudantes. Isso permitiria identificar talentos, além de contribuir para a formação de especialistas em segurança cibernética. Indica, também, a implementação de instrumentos de apoio, tal como a concessão de bolsas destinadas aos alunos e professores, além da criação de outros tipos de incentivos. O estabelecimento de programas de intercâmbio entre governo e setor privado é igualmente uma ação recomendada por parte do autor. Isso contribuiria para desmistificar os desafios relacionados à segurança cibernética (STARR, 2009).

## 3. Metodologia de pesquisa

A necessidade de consolidar uma base de competência técnica na área cibernética envolve a realização de estudos que permitam subsidiar as instituições governamentais, civis ou militares, envolvidas com políticas públicas de apoio à segurança e/ou defesa cibernética. A presente pesquisa teve como foco o ambiente universitário, onde foi possível realizar uma análise da percepção dos alunos do curso de Engenharia de Redes de Comunicação em relação ao tema, suas perspectivas de cooperação tecnológica e atuação profissional após a conclusão do curso. Optou-se pela utilização de uma pesquisa exploratória e descritiva, na qual o grupo focal foi adotado como técnica de coleta e de análise de dados. A escolha da abordagem qualitativa baseia-se na indicação de Backes *et al*., (2011). Segundo os autores, tal abordagem é constituída de diversas possibilidades metodológicas que permitem um processo dinâmico de aderência a novas formas de coleta e de análise de dados. A opção pelo grupo focal se justifica pela possibilidade de inserção dos participantes da pesquisa no contexto das discussões de análise e de síntese. Tendo em vista que a presente pesquisa aborda um tema emergente e de complexo entendimento, as discussões em sala de aula podem se tornar um ambiente interativo e apropriado para os alunos

compartilharem as suas percepções e perspectivas. A discussão em grupo estimula o debate entre os participantes, permitindo que os temas abordados sejam mais problematizados do que numa entrevista individual. Os participantes, de modo geral, ouvem o posicionamento dos outros antes de formarem as suas próprias opiniões. Além disso, constantemente, mudam de posição ou fundamentam melhor sua opinião inicial quando estão envolvidos numa discussão em grupo (BACKES *et al*., 2011).

No que diz respeito à justificativa da amostra escolhida, buscou-se identificar um curso superior cuja proposta de ensino apresentasse afinidade com a temática *segurança ou defesa cibernética*. Conforme informações obtidas no site da Universidade de Brasília (UnB), o estudante do curso de Engenharia de Redes de Comunicação recebe uma formação interdisciplinar sólida em áreas da Engenharia Elétrica, das Telecomunicações e da Computação, o que o prepara para atuar numa realidade de contínua evolução tecnológica. Além disso, são aplicados exercícios práticos em laboratórios de sistemas digitais; eletrônica; arquitetura de computadores; redes ópticas e sem fio; segurança da informação; e gerência de redes; dentre outros temas. Atividades extracurriculares também fazem parte do projeto pedagógico, tais como: projetos de iniciação científica; e atividades de pesquisa, desenvolvimento e inovação, em parceria com grandes empresas públicas e privadas, a saber: Dell, Ericsson, Intel, Petrobrás, HP e Banco do Brasil (UNIVERSIDADE DE BRASÍLIA - UNB, 2019).

No tocante às atividades extracurriculares, fica evidente que a proposta do curso apresenta preocupação com a inserção do aluno em projetos relevantes, por meio de parcerias com instituições privadas. Compreende-se que esse tipo de iniciativa facilita a formação prática dos alunos e a sua inserção no mercado de trabalho. Quanto às oportunidades no campo da *segurança ou defesa cibernética*, a literatura acadêmica destaca que a área de atuação profissional poderá ser tanto na esfera militar quanto na civil. Isso reforçou a importância de se inserir, no âmbito da pesquisa focal, a realização de uma apresentação sobre: as ações do ComDCiber; os programas de apoio ao empreendedorismo tecnológico; e as possibilidades de atuação no quadro das Forças Armadas. Após tais exposições em sala de aula, foram iniciadas as atividades de coleta e de análise de dados. Para isso, foram definidas três categorias de análise: (1) Percepção em relação ao tema; (2) Cooperações tecnológicas; (3) Perspectivas profissionais.

## 3.1. Limitações da Pesquisa

Embora se compreenda que os resultados da pesquisa tenham sido relevantes, considera-se necessária a realização de novos estudos complementares, que permitam superar as limitações da presente pesquisa, tais como:

- Pequena amostragem: verificou-se o reduzido grupo de alunos participantes da pesquisa. Estiveram presentes apenas 12 alunos do curso de Engenharia de Redes de Comunicação;

- Limitada abrangência da pesquisa: caso houvesse maior tempo delimitado para tal tarefa, compreende-se que a pesquisa poderia ter sido ampliada para outros cursos das ciências exatas oferecidos pela universidade, especificamente Ciência da Computação e Engenharia da Computação;

- Reduzido nível de profundidade dos temas apresentados: compreende-se que não foi possível aprofundar em temas importantes que pudessem enriquecer as discussões em sala de aula, como a carreira nas Forças Armadas e até mesmo a experiência profissional de empreendedores brasileiros que atuam no campo cibernético.

# 4. Análise dos resultados

Os estudantes envolvidos na pesquisa acompanharam, em sala de aula, uma apresentação realizada por um oficial da Força Aérea Brasileira, referente a ações e demandas do Comando de Defesa Cibernético (ComDCiber). Na sequência, foi iniciado o processo de coleta de dados, por meio das informações reveladas durante as discussões sobre: o interesse dos alunos pelo tema; suas perspectivas profissionais; e o interesse deles em realizar projetos cooperativos com ComDCiber. Procurou-se analisar tais informações por um ponto de vista crítico, valendo-se do que foi identificado na literatura acadêmica e do posicionamento dos autores em relação ao tema. Posteriormente, foram apresentadas as propostas de ações e considerações finais.

## 4.1. Interesse no tema e conhecimento dos projetos estratégicos

### 4.1.1. Informações coletadas

Um desses estudantes conhecia um pouco das ações realizadas por essa organização militar, em razão de ter participado de um processo seletivo para ingresso no Núcleo Preparatório de Oficiais da Reserva (NPOR). À época, o referido aluno desistiu de ingressar no quadro, pois já atuava na EngNet Consultoria, a empresa júnior do curso de Engenharia de Redes de Comunicação da UnB. No período da coleta de dados, porém, este aluno se declarou arrependido da decisão. Outro estudante também inserido no mesmo processo seletivo destacou que, por meio das apresentações realizadas, foi possível conhecer algumas ações do ComDCiber e a relevância do

tema para a segurança do País. Contudo, disse ainda restar dúvidas em relação à atuação da referida organização militar. Por fim, este segundo estudante sugeriu uma apresentação com informações mais detalhadas sobre o programa, considerando o seu apreço pela área militar. Ele informou que o pai foi da Polícia Militar e o incentivou, quando ainda mais jovem, a ingressar na carreira militar.

### 4.1.2. Análise crítica

Com base nos depoimentos, foi possível verificar que apenas um aluno revelou ter familiaridade com os projetos estratégicos militares apresentados em sala de aula. Isso evidencia o pouco conhecimento pertinente à atuação do ComDCiber. Esse fato converge com as dificuldades apresentadas por Westermeyer (2008). Segundo o autor, um dos desafios no processo de recrutamento diz respeito à carência de informações por parte dos jovens em relação às atividades do serviço militar (WESTERMEYER, 2008). Considera-se que o NPOR seja uma experiência profissional relevante para os universitários que pretendem trabalhar com *defesa cibernética*. Essa forma de ingresso, mesmo que temporária, permite ao jovem o acesso ao posto de oficial, sem a exigência de qualquer experiência profissional ou conclusão do curso superior. Contudo, questiona-se o conhecimento técnico do futuro oficial, tendo em vista que a idade de ingresso (entre 19 e 20 anos) ocorre nos períodos iniciais do seu curso de bacharelado. Nessa fase, os alunos ainda não concluíram as disciplinas especializadas, que servem de base teórica para a atuação no campo cibernético, como Segurança de Redes; e Telecomunicações, entre outras que são ministradas até o final do curso. A título de comparação, a Universidade de Brasília somente libera universitários para a realização de estágios a partir do 5° semestre da graduação (UNB, 2019). A empresa Google, por exemplo, só admite em seu programa de estágio os universitários que estejam em fase final de conclusão do curso (CORREIOWEB, 2019).

## 4.2. Realização de apresentações institucionais em sala de aula

### 4.2.1. Informações coletadas

No que diz respeito à realização de apresentações institucionais por um representante do ComdCiber, todos os alunos concordaram que essas atividades deveriam ocorrer com frequência na universidade. Um dos alunos enfatizou como positiva a aproximação entre o ComDCiber e o curso de Engenharia de Redes de Comunicação. Contudo, ressaltou que a simples realização de apresentações sem perspectivas de cooperação poderia causar frustação nos alunos. Seria preciso estabelecer parcerias que permitissem a maior interação entre o Comando e a universidade. A apresentação das demandas tecnológicas do ComDCiber seria um escopo inicial

para se identificar oportunidades de cooperação tecnológica. Outra possibilidade de interação poderia ocorrer por meio do compartilhamento de disciplinas entre a Escola Nacional de Defesa Cibernética (ENaDCiber) e o curso de Engenharia de Redes de Comunicação da UnB. Muitos alunos manifestaram o interesse em conhecer a matriz curricular da ENaDCiber e, talvez, cursar algumas disciplinas ofertadas pela respectiva instituição de ensino.

### 4.2.2. Análise crítica

Com base nos relatos em sala de aula, foi possível perceber o grande interesse dos alunos em relação aos temas apresentados. Essas são evidências valorosas num contexto estratégico em que se busca despertar a relevância da temática *defesa cibernética* no ambiente acadêmico. Isso reforça a importância e a necessidade da elaboração de ações governamentais que venham a permitir, de forma estruturada e permanente, a aproximação entre o Comando e as universidades. Esses tipos de ações já são realizadas pelo Exército Americano, a exemplo do "*Eisenhower Series College Program*", no qual é incentivado o diálogo, pertinente ao tema *Segurança Nacional* e a outras questões relacionadas a políticas públicas, entre funcionários e estudantes da *US Army War College* e o público civil, com ênfase em estudantes e professores das instituições acadêmicas nos Estados Unidos. No campo educacional, é interessante destacar que esses tipos de iniciativas convergem com as novas *Diretrizes Curriculares Nacionais do Cursos de Graduação em Engenharia*, conforme instituído pela Resolução n.º 2, de 24 de abril de 2019, da Câmara de Educação Superior do Conselho Nacional de Educação. Nesse sentido, torna-se relevante citar as recomendações contidas no Artigo 6º, em seu inciso VIII, § 10:

> Art. 6º O curso de graduação em Engenharia deve possuir Projeto Pedagógico do Curso (PPC) que contemple o conjunto das atividades de aprendizagem e assegure o desenvolvimento das competências, estabelecidas no perfil do egresso. Os projetos pedagógicos dos cursos de graduação em Engenharia devem especificar e descrever claramente:
>
> [...]
>
> VIII - o processo de autoavaliação e gestão de aprendizagem do curso que contemple os instrumentos de avaliação das competências desenvolvidas, e respectivos conteúdos, o processo de diagnóstico e a elaboração dos planos de ação para a melhoria da aprendizagem, especificando as responsabilidades e a governança do processo;
>
> [...]

> § 10 Recomenda-se a promoção frequente de fóruns com a participação de profissionais, empresas e outras organizações públicas e privadas, a fim de que contribuam nos debates sobre as demandas sociais, humanas e tecnológicas para acompanhar a evolução constante da Engenharia, para melhor definição e atualização do perfil do egresso (BRASIL, 2019a, p.43).

## 4.3. Realização de visitas técnicas, cooperações tecnológicas e estágios em organizações (civis ou militares)

### 4.3.1. Informações coletadas

Por unanimidade, os alunos pesquisados - incluindo a contribuição do professor - manifestaram interesse na realização de estágios, participação em cooperações tecnológicas e até mesmo em operações de simulação de guerra cibernética com os militares. Foi solicitada também a apresentação de *cases* que pudessem ser divulgados e levados como exemplos para clarificar o papel exercido pelo ComDCiber, num contexto de ataque cibernético, tal como o do episódio da proliferação do vírus *Wanna Cry*. A necessidade de compreender os mecanismos de intercâmbio de informações entre as instituições internacionais, para se evitar a proliferação do ataque entre as nações, foi outra curiosidade apresentada por parte dos alunos. Por fim, eles citaram como relevante o apoio, por meio de incentivos como bolsas, para a realização de pesquisa e desenvolvimento de tecnologias que sejam de interesse do Comando.

### 4.3.2. Análise crítica

Conforme relatado, verificou-se o grande interesse dos alunos na participação em estágios e simulações de operações de guerra cibernética. Essas são evidências importantes num contexto estratégico em que se pretende iniciar a construção de uma base de competência técnica a partir da formação acadêmica. Considera-se que as competições por meio de *hackatons* e de outras atividades práticas poderiam ser realizadas com o propósito de esclarecer o *modus operandi* de um episódio de ataque e defesa cibernética. Esses tipos de atividades serviriam para complementar as ações de promoção e divulgação anteriormente propostas. Tais atividades práticas permitiriam aos alunos uma melhor compreensão dos conhecimentos necessários e das habilidades exigidas de um especialista em segurança cibernética, além de desmistificar os tipos de atividades realizadas no âmbito do ComDCiber. Outro aspecto positivo, advindo dessas ações, refere-se à identificação de potenciais talentos que futuramente venham a suprir as necessidades de pessoal de instituições civis ou militares. A implementação de um programa de apoio ao desenvolvimento tecnológico por meio de bolsas também seria uma ação relevante para viabilizar a formação de pessoal, permitindo, inclusive, a realização de cooperações

tecnológicas. Essas propostas de ações convergem com o posicionamento de Starr (2009). Para o autor, há uma desconexão entre o ensino realizado nas universidades e as demandas do governo e do setor privado. Existe uma grande base de talentos com potencial não aproveitada no campo cibernético. Como forma de superar essas deficiências, ele recomenda a realização de competições nacionais entre estudantes. No que diz respeito às cooperações tecnológicas, cabe destacar que o departamento do curso já as realiza com instituições que demandam: tecnologias de segurança cibernética; construção de algoritmos para reconhecimento facial; *blockchain*; criptografia; e inteligência artificial, entre outras aplicações (UNB, 2019). Essas parcerias podem ser potencializadas com a aproximação e o apoio do ComDCiber.

Por fim, cabe destacar que todas essas ações propostas também convergem com as novas diretrizes curriculares definidas para os cursos de engenharia por meio da Resolução n.º 2, de 24 de abril de 2019. Ainda no Artigo 6º do referido normativo, em seu inciso VIII, os parágrafos 8º e 9º defendem o estímulo da iniciação científica, a realização de competições acadêmicas, visitas técnicas, desenvolvimento de protótipos e atividades empreendedoras, entre outras ações. Na sequência, outra análise do parágrafo 10º revela a recomendação para a promoção de fóruns com a participação de empresas e outras organizações públicas e privadas que contribuam para os debates referentes às demandas sociais, humanas e tecnológicas, tal como destacado abaixo:

> Art. 6º [...]
>
> VIII – [...]
>
> § 8º Devem ser estimuladas as atividades acadêmicas, tais como trabalhos de iniciação científica, competições acadêmicas, projetos interdisciplinares e transdisciplinares, projetos de extensão, atividades de voluntariado, visitas técnicas, trabalhos em equipe, desenvolvimento de protótipos, monitorias, participação em empresas júniores, incubadoras e outras atividades empreendedoras.
>
> § 9º É recomendável que as atividades sejam organizadas de modo que aproxime os estudantes do ambiente profissional, criando formas de interação entre a instituição e o campo de atuação dos egressos.
>
> § 10º Recomenda-se a promoção frequente de fóruns com a participação de profissionais, empresas e outras organizações públicas e privadas, a fim de que contribuam nos debates sobre as demandas sociais, humanas e tecnológicas para acompanhar a evolução constante da Engenharia, para melhor definição e atualização do perfil do egresso (BRASIL, 2019a, p.43).

## 4.4. Perspectiva profissional (Ingresso na carreira militar/ Empreendedorismo tecnológico)

### 4.4.1. Informações coletadas

No âmbito das discussões, não foi possível verificar o posicionamento claro por parte dos alunos em relação às perspectivas profissionais. A atuação nas Forças Armadas não foi descartada, assim como o empreendedorismo tecnológico. Em relação ao último ponto, não foram realizados questionamentos dos alunos em relação aos programas e instrumentos de apoio ao empreendedorismo tecnológico, apenas breves perguntas em relação à carreira militar nas Forças Armadas. Deve-se ressaltar que alguns alunos presentes já estiveram na Empresa Júnior do curso de Engenharia de Redes de Comunicação UnB. Consequentemente, exerceram alguma atividade prática ou tiveram contato com alguma tecnologia de interesse do mercado. Como informação complementar, o depoimento de um professor presente em sala de aula reforçou a importância da interação do curso com o mercado, porém, reclamou da passividade da indústria em relação ao desenvolvimento tecnológico em parceria com as universidades. Conforme seu relato, a indústria ainda tem como preferência a aquisição de tecnologias do exterior. No que se refere ao empreendedorismo tecnológico, o professor destacou a sua participação na criação de três empresas de tecnologia que, posteriormente, foram gerenciadas pelos próprios alunos do curso.

### 4.4.2. Análise crítica

Em relação às expectativas profissionais, percebeu-se que nenhum aluno apresentou um posicionamento consistente. Verificou-se que os alunos se encontram numa situação de passividade à espera do surgimento de oportunidades, seja na iniciativa privada, no governo ou mesmo por meio do empreendedorismo tecnológico. O professor presente em sala de aula comentou o apreço dos alunos pelo concurso público. Historicamente, as perspectivas profissionais advindas da administração pública sempre foram significativamente relevantes em Brasília, atraindo inclusive profissionais das ciências exatas. Porém, numa conjuntura de baixo crescimento econômico, em que o governo tende à redução do número de concursos públicos e o setor privado paralisa as contratações, salvo exceção aquelas em que existe grande escassez de profissionais capacitados no mercado, o empreendedorismo tecnológico surge como uma opção relevante. Nesse aspecto, o professor relatou suas experiências na criação de empresas de base tecnológica na própria universidade, porém, sem que exercesse as atividades de gestão. Nesses casos, as empresas foram gerenciadas pelos próprios alunos do curso. Esse depoimento demonstra o relevante papel do professor, como indutor no processo de criação de empresas de tecnologia no ambiente universitário. Essas são evidências importantes num contexto estratégico em que se pretende consolidar a base de competência técnica pela via do empreendedorismo tecnológico, durante ou após a formação acadêmica. Nessa perspectiva, propõe-se a divulgação

dos programas de apoio ao empreendedorismo tecnológico e a apresentação de *cases* de empreendedores tecnológicos e de professores que tiveram participação significativa na criação de empresas no ambiente acadêmico.

## 5. Considerações finais

O contexto histórico tem demonstrado a relevante participação do setor acadêmico no apoio à pesquisa e ao desenvolvimento tecnológico de projetos militares estratégicos. A capacidade de articulação e o desenvolvimento de ações conjuntas entre institutos de pesquisa e a esfera produtiva foram algumas das razões que colocaram os Estados Unidos na vanguarda tecnológica (CGEE, 2013). No Brasil, verificaram-se também projetos estratégicos exitosos em que a participação das instituições de pesquisa foi fundamental, tal como na constituição da Empresa Brasileira de Aeronáutica (Embraer) (EMBRAER, 2019). Outros diversos casos retratados na literatura acadêmica reforçam a importância da atuação das instituições científicas e tecnológicas para as políticas de defesa nacional, sobretudo no que diz respeito à *defesa cibernética*. A presente pesquisa abordou alguns aspectos relevantes pertinentes à constituição de uma base de competência tecnológica nas universidades, no âmbito da respectiva temática estratégica. Para tanto, optou-se por realizar uma pesquisa aplicada ao grupo de estudantes do curso de Engenharia de Redes de Comunicação da Universidade de Brasília. Os resultados da pesquisa demonstraram que, apesar do pouco conhecimento referente ao tema e às ações do ComDCiber, todos os alunos demonstraram o interesse em participar de: estágios em instituições civis ou militares; simulações de guerra cibernética; cooperações tecnológicas; e outras atividades correlatas. Tais relatos reforçam as evidências do engajamento do corpo discente perante a uma cooperação entre a Universidade de Brasília e o ComDCiber. Para tanto, seria necessário consolidar um programa interinstitucional, que abarcasse: realização de novas apresentações institucionais; fomento à inovação (bolsas) para viabilizar as cooperações tecnológicas; formação de pessoal em parceria com EnadCiber; e estímulo ao empreendedorismo tecnológico. Todas essas iniciativas seriam essenciais para despertar, nos universitários, o interesse pela carreira no campo cibernético, além de identificar os talentos que futuramente poderiam compor a base de competência tecnológica no País.

## Referências

BACKES, D.S.; COLOMÉ, J.S.; ERDMANN, R.H.; LUNARDI, V.L. Grupo focal como técnica de coleta e análise de dados em pesquisas qualitativas. **O Mundo da Saúde**, v. 35, n.º 4, p.438-42. 2011. Disponível em: http://bvsms.saude.gov.br/bvs/artigos/grupo_focal_como_tecnica_coleta_analise_dados_pesquisa_qualitativa.pdf

BRASIL. Exército Brasileiro. Escritório de Projetos. **Programa da defesa cibernética na defesa nacional.** Disponível em: http://www.epex.eb.mil.br/index.php/defesa-cibernetica. Acesso em: 16 jun. 2019.

BRASIL. Ministério da Ciência, Tecnologia e Inovação - MCTI. **Estratégia Nacional de Ciência, Tecnologia e Inovação 2016-2022** - Balanço das Atividades Estruturantes. Brasília: MCTI, 2018. 136 p. Disponível em: http://www.finep.gov.br/images/a-finep/Politica/16_03_2018_Estrategia_Nacional_de_Ciencia_Tecnologia_e_Inovacao_2016_2022.pdf

BRASIL. Ministério da Defesa. **A Escola nacional de defesa cibernética é inaugurada em Brasília.** Disponível em: https://www.gov.br/defesa/pt-br/assuntos/noticias/ultimas-noticias/escola-nacional-de-defesa-cibernetica-e-inaugurada-em-brasilia#:~:text=Escola%20Nacional%20de%20Defesa%20Cibernética%20é%20inaugurada%20em%20Brasília,-Compartilhe%3A&text=Brasília%2C%2011%2F02%2F2019,Forte%20Marechal%20Rondon%2C%20em%20Brasília. Acesso em: 24 jun. 2019.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa – Estratégia Nacional de Defesa**. Brasília: MD, 2012. 41 p. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf

BRASIL. Ministério da Educação - ME. **Resolução nº 02, de 24 de abril de 2019. Institui as diretrizes curriculares nacionais do curso de graduação em engenharia**. Brasília, DF. Disponível em: https://www.in.gov.br/web/dou/-/resolu%C3%87%C3%830-n%C2%BA-2-de-24-de-abril-de-2019-85344528

BRASIL. Senado Federal. **CPI da espionagem. Relatório final. 301 p.** Disponível em: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco Acesso em: 15 jun. 2019.

CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS-CGEE. **Dimensões estratégicas do desenvolvimento brasileiro**: As fronteiras do conhecimento e da inovação: oportunidades, restrições e alternativas estratégicas para o Brasil. Brasília: 2013. v.2, 212 p. Disponível em: https://www.cgee.org.br/documents/10195/734063/CAEBS21_vII_Web_9520.pdf/e6d4d1c6-5e36-4fa8-a8d8-40d5e83da9f4?version=1.7

CLARKE, Richard A.; KNAKE, Robert K. **Cyberwar: the next threat to national security and what to do about it**. Nova Iorque: HarperCollins Publishers, 2010. 306 p.

CORREIOWEB. Eu, Estudante. **Google abre inscrições para programa de estágio**. 03 set. 2019. Disponível em: https://www.correiobraziliense.com.br/app/noticia/eu-estudante/trabalho-e-formacao/2019/09/03/interna-trabalhoeformacao-2019,780593/programa-de-estagio-do-google-abre-inscricoes.shtml. Acesso em: 03 jul. 2019

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY – DARPA. **50 Years of bridging the gap: revolutionizing the commercial marketplace.** Flórida: Faircount Llc, 2008. 180 p. (online). Disponível em: https://issuu.com/faircountmedia/docs/darpa50

DOSI, G. T**echnical change and industrial transformation**. Macmillan, 1984. 338 p. 10.1007/978-1-349-17521-5

EMBRAER S.A. **História da EMBRAER.** Disponível em: https://historicalcenter.embraer.com/br/pt/historia. Acesso em: 16 jun. 2019.

ENDEAVOR BRASIL. **Como o Vale do Silício se tornou o Vale do Silício? Três surpreendentes lições para outras cidades e regiões**. jul. 2014. 22 p. Disponível em: https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F6588%2F1425325397Como_o_Vale_do_Sil%C3%ADcio_se_tornou_o_Vale_do_Sil%C3%ADcio.pdf. Acesso em: 10 jun. 2019.

FONSECA, Paulus Vinícius da Rocha. Embraer: um caso de sucesso com o apoio do BNDES. **Revista do BNDES**, Rio de Janeiro, v. 37, p.39-66, jun. 2012. Disponível em: https://web.bndes.gov.br/bib/jspui/bitstream/1408/17642/1/PRArt213368_Embraer_Compl_P.pdf

GAMA NETO, Ricardo Borges. Guerra cibernética/guerra eletrônica – conceitos, desafios e espaços de interação. **Revista Política Hoje**, Recife - PE, v. 26, n.º 1, p.201-218, jun. 2017. Disponível em: https://periodicos.ufpe.br/revistas/politicahoje/article/download/9180/16123

GLOBO.COM. G1. **Hackers invadem servidores do Exército e vazam CPFs de militares. 2015.** Disponível em: http://g1.globo.com/tecnologia/noticia/2015/11/hackers-invadem-servidores-do-exercito-e-vazam-cpfs-de-militares.html. 09 nov. 2015. Acesso em: 10 jun. 2019

KLIMBURG, Alexander. Mobilising cyber power. **Survival**, **Global Politics and Strategy**. v. 53, n.º 1, p.41-60, 28 jan. 2011. http://dx.doi.org/10.1080/00396338.2011.555595 Acesso em: 10 jun. 2019

KOROLOV, Maria. **Experts divided on value of Cyber National Guard. 17 mar. 2017.** Disponível em: https://www.csoonline.com/article/3181840/experts-divided-on-value-of-cyber-national-guard.html. Acesso em: 16 jun. 2019

MAZZUCATO, M. O estado empreendedor: desmascarando o mito do setor público vs. setor privado. **Confins, Revista Franco-Brasileira de Geografia**, n.º 27, 2016. Disponível em: https://journals.openedition.org/confins/10951?lang=pt

MOREIRA, Alexandre Santana; CORDEIRO, Sandro Silva. O Spin-In na indústria de defesa brasileira voltada para o setor cibernético. **Revista da Escola Superior de Guerra**, v. 29, n.º 58, p. 100-116, jul. 2014. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/download/181/156/251. Acesso em: 04 out. 2019.

NETO, Vladimir; BENTES, Vianey. **Sistema de comunicação do Itamaraty é alvo de invasão hacker.** 27 mai. 2014. Disponível em: http://g1.globo.com/politica/noticia/2014/05/sistema-de-comunicacao-do-itamaraty-e-alvo-de-ataque-hacker.html. Acesso em: 15 jun. 2019.

ROBERTSON, Jordan; RILEY, Michal. Bloomberg Businewsweek. **The Big hack: how china used a tiny chip to infiltrate U.S. companies. 04 out. 2018.** Disponível em: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies. Acesso em: 16 jun. 2019

RODENGEN, J.L. **The History of Embraer.** Fort Lauderdale, Fl: Write Stuff Enterprises, 2009. 255 p.

SANTOS, Ricardo Henrique Correia dos. **O desenvolvimento da cadeia industrial aeronáutica sob o enfoque da competitividade.** 2018. 128 f. Dissertação (Mestrado) - Curso de Ciências Aeroespaciais, Universidade da Força Aérea, Rio de Janeiro, 2018.

STARR, Stuart H. Toward a preliminary theory of cyberpower. In: KUEHL, Dr Dan. **Cyberpower and National Security.** Virginia: Pootmac Books, 2009. p. 43-88. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-03.pdf?ver=2017-06-16-115054-677

UNIVERSIDADE DE BRASÍLIA – UNB. **Engenharia de redes de comunicação.** Disponível em: https://redes.unb.br/index.php/curso/ Acesso em: 10 jun. 2019

WESTERMEYER, Roger H. **Recruiting and retaining cyberwarriors.** 2008. 36 f. Dissertação (Mestrado) - Master of Strategic Studies Degree, U.s. Army War College, Philadelphia, 2008. Disponível em: https://apps.dtic.mil/dtic/tr/fulltext/u2/a478276.pdf

WIKIPÉDIA. **Advanced Research Projects Agency Network – ARPANET**. Disponível em: https://pt.wikipedia.org/wiki/ARPANET#cite_note-2. Acesso em 03 de fevereiro de 2021.