ERNANI LUSTOSA KUHN
LEANDRO NEVES DE OLIVEIRA BANDO

DESENVOLVIMENTO E PROTEÇÃO DAS INFRAESTRUTURAS CRÍTICAS DE COMUNICAÇÃO DA ADMINISTRAÇÃO PÚBLICA FEDERAL: UMA ANÁLISE

Trabalho de Conclusão de Curso apresentado à Escola Superior de Defesa, como exigência parcial para obtenção do título de Especialista em Altos Estudos em Defesa.

Orientador: CF RM1 MB Marco Aurélio Carvalho Leandro

Brasília
2023

Brasília, DF, 16 de novembro de 2023

ERNANI LUSTOSA KUHN
PESQUISADOR

LEANDRO NEVES DE OLIVEIRA BANDO
PESQUISADOR

ERNANI LUSTOSA KUHN
LEANDRO NEVES DE OLIVEIRA BANDO

DESENVOLVIMENTO E PROTEÇÃO DAS INFRAESTRUTURAS CRÍTICAS DE COMUNICAÇÃO DA ADMINISTRAÇÃO PÚBLICA FEDERAL: UMA ANÁLISE

Trabalho de Conclusão de Curso apresentado à Escola Superior de Defesa, como exigência parcial para obtenção do título de Especialista em Altos Estudos em Defesa.

Trabalho de Conclusão de Curso **APROVADO**:

Brasília, DF, 16 de novembro de 2023

MARCO AURÉLIO CARVALHO LEANDRO – CF RM1 (ESD)
Orientador

NÁDIA XAVIER MOREIRA – CF T MB (ESD)
Membro 1

DONALD GRAMKOW – Cel R1 FAB (ESD)
Membro 2

Desenvolvimento e Proteção das Infraestruturas Críticas de Comunicação da Administração Pública Federal: uma Análise

Ernani Lustosa Kuhn[*]
Leandro Neves de Oliveira Bando[**]

RESUMO

A proteção de dados e da comunicação de cidadãos e do governo pode ser alcançada com adoção de ações de cibersegurança e de segurança da infraestrutura crítica de comunicação. Neste contexto, a empresa Telecomunicações Brasileiras S/A – Telebras – é importante prestadora de serviços ao governo. Este estudo busca responder à questão "como os órgãos e as entidades da Administração apoiam e poderiam contribuir para ampliar a proteção de suas comunicações?". Tem como hipótese que se utiliza ou seria possível utilizar o ciclo integrado de inteligência e contrainteligência para aumentar o nível de proteção desta infraestrutura. O estudo utilizou-se de metodologia qualitativa, aplicada e exploratória, bem como de procedimentos de análise documental e bibliográfica. Adicionalmente foram realizadas entrevistas abertas para uma maior compreensão da definição e execução de políticas ou normas de cibersegurança. Foi possível identificar que o nível de cibersegurança e segurança das infraestruturas críticas tem evoluído nos últimos anos, porém, não foi possível identificar a adoção do ciclo integrado de inteligência e contrainteligência.
Palavras-chave: cibersegurança; infraestruturas críticas; comunicação; inteligência e contrainteligência.

Development and Protection of Critical Communication Infrastructures of the Federal Public Administration: an Analysis

ABSTRACT

Protecting of government and citizen data and communication can be achieved by adopting cybersecurity and security actions for the critical communications infrastructure. In this context, the company Telecomunicações Brasileiras S/A – Telebras – is an important service provider for the government. This study seeks to answer the question "how do Administration bodies and entities support and could contribute to expanding the protection of their communications?" The hypothesis is that the integrated cycle of intelligence and counterintelligence is used or could be used to increase the level of protection of this infrastructure. The study used qualitative, applied, and exploratory methodology, as well as document and bibliographic analysis procedures. Additionally, interviews and open interviews

[*] Especialista em Políticas Públicas e Gestão Governamental do Ministério das Comunicações. Graduado em Engenharia Civil pela Universidade Estadual de Campinas – Unicamp e Mestre em Economia do Setor Público pela Universidade de Brasília – UnB. Mestre em Administração Pública pela Hertie School of Governance. E-mail: ernani.kuhn@mcom.gov.br

[**] Especialista em Gestão de Telecomunicações. Telecomunicações Brasileiras S/A. Graduado em Administração de Empresas pela Universidade Federal de Goiás e em Análise e Desenvolvimento de Sistemas pela Universidade Católica de Brasília. E-mail: leandro.neves@telebras.com.br

were carried out to gain a greater understanding of the definition and execution of cybersecurity policies or standards. It was possible to identify that the level of cybersecurity and security of critical infrastructures has evolved in recent years, however, it was not possible to identify the adoption of the integrated intelligence and counterintelligence cycle.
***Keywords**: cybersecurity, critical infrastructure, communication, intelligence and counterintelligence.*

1. INTRODUÇÃO

A segurança, a defesa e o desenvolvimento do ciberespaço têm grande relevância para o Brasil. Desde a Estratégia Nacional de Defesa de 2008, o setor cibernético, em conjunto com o espacial e o nuclear, são considerados como setores de importância estratégica (Brasil, 2008). O cenário mundial de aumento na vulnerabilidade e o risco decorrente de acesso por terceiros não autorizados a informações sensíveis, torna o ciberespaço um tema de pesquisa de fundamental relevância. No atual contexto de ameaças híbridas, em que se utilizam de métodos danosos de ordem diversa da ação militar tradicional, o estudo e entendimento das políticas públicas existentes em prol da cibersegurança – ou de sua ausência – são essenciais para projetar os rumos para o desenvolvimento do tema no Brasil.

Dentre outros fatores e face a relevância das comunicações no setor cibernético, a Telecomunicações Brasileiras S/A – Telebras – foi reativada em 2010. Nos termos do decreto de sua reativação e para os fins deste estudo, destaca-se a atribuição da Companhia de "implementar a rede privativa de comunicação da administração pública federal" (Brasil, 2010). Conforme detalhado adiante neste trabalho, a infraestrutura de comunicação, assim como os sistemas de tecnologia da informação, são componentes do ciberespaço.

Outro exemplo da importância dos serviços prestados pela Telebras é o fato de que, em resposta à divulgação de informações sensíveis realizadas por Edward Snowden, em 2013, o Governo Federal publicou o Decreto nº 8.135. Este decreto estabeleceu que as comunicações de dados da administração pública federal direta, autárquica e fundacional deveriam ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal. Assim sendo, como única empresa estatal do setor, os serviços de telecomunicações deveriam ser fornecidos pela Telebras (Brasil, 2013).

Cabe destacar que a Telebras é uma empresa vinculada ao Ministério das Comunicações que presta serviços à sociedade brasileira há mais de 50 anos. Em sua fundação, a Companhia era empresa controladora das operadoras regionais de telefonia e tinha a atribuição de regulamentar do Sistema Brasileiro de Telecomunicações. No final dos anos 1.990 ocorreram mudanças no setor de telecomunicações com vistas a possibilitar a competição neste setor, tendo sido promulgada a Emenda Constitucional nº 8, de 15 de agosto de 1995 e a Lei Geral de Telecomunicações – LGT. Em linhas gerais, as atribuições de regulamentação do setor foram transferidas para a Agência Nacional de Telecomunicações – Anatel – e as operadoras

telefônicas regionais privatizadas, deixando a Telebras em processo para encerramento das atividades e liquidação (TELEBRAS, 2023a).

Não obstante, além da prestação de serviços de telecomunicação civis, a Telebras pauta sua atuação em sinergia com a área de Defesa. Em 2012, a Telebras passou a ser integrante do Grupo-Executivo do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC) – que possibilita a comunicação dual – civil e militar, respectivamente, em 100% do território nacional e em grande parte da América do Sul. Na consecução de seus objetivos, a Companhia opera mais de 30.000 Km de redes ópticas, distribuídas em todos os Estados do território nacional, além de operar o SGDC. As instalações físicas do Centro de Operações Espaciais Principal (COPE-P), principal componente do segmento solo do SGDC, possuem certificação "TIER IV", o que representa ter o mais alto nível de disponibilidade e confiabilidade para a infraestrutura de uma instalação, conhecida como "Fault Tolerant" (tolerante a falhas) (Telebras, 2023b).

Atualmente, as atividades da Telebras são orientadas pelas Políticas Públicas de Telecomunicações, que manteve a atribuição de implementar a rede privativa de comunicação da administração pública federal (Brasil, 2018b). Ademais, a alteração no decreto realizada em 2022, determinou que a rede privativa de comunicação da administração pública federal seja composta por segmentos de rede móvel e fixa, incluída rede satelital, com a condição de que a companhia provenha os serviços com "capacidade de rede adequada para o atendimento das demandas de órgãos e de entidades da administração pública federal e de órgãos de segurança pública e das forças armadas, com níveis de prioridade, segurança e criptografia adequados" (BRASIL, 2023).

Considerando o histórico acima apresentado, é possível constatar que, no setor de comunicações, a Telebras é ator relevante para prestação de serviços à Administração Pública, e consequentemente, à sociedade. A Telebras, com suas competências de implementar a rede privativa de comunicação da Administração Pública Federal, é um agente público atuante que encerra relevante relação com a presente discussão, na sua condição de ator e alvo potencial de ações invasivas. A proteção dessa rede é ação fundamental para garantir a segurança dos órgãos e entidades da Administração Pública que a utilizam.

Os problemas de pesquisa relacionados ao ciberespaço que merecem a atenção da comunidade acadêmica são inúmeros. Apenas para ilustrar alguns desses problemas, destacamos as questões relacionadas à liberdade de expressão versus a responsabilização; ao anonimato versus a atribuição de autoria; à inclusão versus a exclusão dos indivíduos no

ciberespaço; à tecnologia, à inovação e à obsolescência; à proteção, à defesa e à segurança frente a ataques cada vez mais sofisticados e frequentes. Todavia, impõe-se a necessidade de limitar o problema de pesquisa, mas de tal forma que possa ser utilizado por outros pesquisadores no desenvolvimento de novos estudos, ou ainda para que o resultado deste trabalho possa ser aplicado em organizações que atuam no ciberespaço.

Diante do dilema, da vastidão do assunto e da necessidade de objetividade, optou-se por estudar a cibersegurança, com foto na camada informacional da infraestrutura crítica que a suporta, com vistas a sua proteção. Neste sentido, este trabalho deve tentar responder ao seguinte problema:

Como os órgãos e as entidades da Administração apoiam e poderiam contribuir para ampliar a proteção de suas comunicações?

Com o desenvolvimento deste estudo, almeja-se conhecer o que já foi produzido academicamente sobre o tema e elencar opções para a sua implementação, com vistas ao aperfeiçoamento de arcabouços institucionais e de medidas de cibersegurança para salvaguardar rede privativa de comunicação da Administração Pública Federal, serviço de telecomunicação prestado pela Telebras. Assim, o objetivo geral do estudo será levantar informações sobre as principais ações empreendidas no âmbito da proteção de estruturas críticas no governo federal e identificar modos como os órgãos e as entidades da Administração Pública apoiam e poderiam contribuir para a proteção dos ativos da infraestrutura crítica do ciberespaço.

Para alcançar este objetivo geral, o trabalho tem os seguintes objetivos específicos: (i) identificar o arcabouço regulatório relacionado à segurança dos serviços de telecomunicações suportados pela infraestrutura da Telebras; (ii) identificar na literatura como as outras nações estão se organizando para garantir a cibersegurança de suas infraestruturas críticas de comunicações; (iii) avaliar a integração entre órgãos e entidades da Administração Pública Federal junto aos órgãos e entidades que suportam a cibersegurança no âmbito nacional; e, (iv) identificar na literatura métodos e propostas de aprimoramento que possibilitariam outros ganhos para a cibersegurança com foco na proteção das infraestruturas críticas de comunicação. Tem-se como hipótese deste estudo que as organizações estejam adotando de alguma forma o ciclo integrado de inteligência e contrainteligência, proposto por Nolan (2002) e detalhado adiante, orientado às questões de cibersegurança e da infraestrutura de telecomunicações.

O desenvolvimento do projeto de pesquisa justifica-se por três principais motivos. Em primeiro lugar, pela relevância de se garantir a segurança das comunicações da Administração.

Faz-se necessário aprofundar os estudos relacionados à obtenção de conhecimento sobre os ciberataques, as contramedidas de proteção que podem ser adotadas – em âmbito civil – para resguardar os interesses da sociedade brasileira.

Em segundo lugar, em uma concepção histórico-social, reconhece-se algum nível de exploração econômica, exercida pelos colonizadores e neocolonizadores face ao povo e à nação brasileira. Neste sentido, a aquisição indevida de informações – de posse do Estado, mas pertencentes ao cidadão – traduz-se por uma nova forma de exploração, doravante tecnológica. A utilização indevida das informações do público por outros atores, ainda que nacionais, também apresentam conotações perniciosas. Esse fator justifica ações para a proteção da infraestrutura do ciberespaço. E o desenvolvimento no setor cibernético, em tese, teria a condição de garantir a independência da nação, ponto preconizado pela Estratégia Nacional de Defesa já em 2008 (END, 2008).

Por fim, em uma concepção relacionada à área de estudos da ciência da computação, o trabalho justifica-se ao possibilitar a compreensão de modelos, métodos, processos, ferramentas, softwares que permitam identificar e responder aos eventuais ataques realizados contra a infraestrutura que suporta o ciberespaço.

1.1 – INTELIGÊNCIA E CONTRAINTELIGÊNCIA: CIBERESPAÇO

Cabe observar que desde a concepção do termo, o ciberespaço está mais e mais presente nas atividades sociais. Gibson, autor que utilizou o termo *cyberspace* pela primeira vez em 1982, definiu ciberespaço como um espaço imaginário criado por uma rede de computadores universal contendo os mais diversos tipos de informações (Monteiro, 2007). Levy (2000, p.92) define ciberespaço como “espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores”. No Brasil, o assunto tem grande relevância ao menos desde a publicação da Estratégia Nacional de Defesa de 2008. De acordo com o documento, o setor cibernético, em conjunto com o espacial e o nuclear, são setores de importância estratégica para a Segurança, Desenvolvimento e Defesa da País (Brasil, 2008).

Adicionalmente, o ciberespaço pode ter sua constituição analisada por meio de seus principais componentes. Para Viana e Fernandes (2015), o ciberespaço é constituído por redes de comunicação de dados e sistemas de informação automatizados para o provimento de informações a usuários, organizações e a sociedade. A Internet e as demais redes de comunicação são componentes importantes do ciberespaço, mas não os únicos. Dentre estes componentes devem ser também considerados os dispositivos conectados (*hardware*), os

sistemas informatizados (*software*), as pessoas e organizações que os utilizam, assim como o conjunto de interações e atividades realizadas no ambiente virtual. (ABNT, 2015; Vianna, Fernandes, 2015).

Além de sua composição, o ciberespaço, de acordo com Moresi (2013), pode ser descrito em três dimensões: cognitiva, informacional e física. O autor argumenta que a proteção da dimensão cognitiva, relacionada mais a aspectos comportamentais do que tecnológicos, não é simples. Todavia, seria possível proteger as dimensões física e informacional por meio de quatro objetivos: estabelecer proteção da infraestrutura de tecnologia da informação e da aplicação, visando permitir o uso das redes e sistemas de informação; detectar ataques, para associar contramedidas passivas de proteção; restaurar de forma rápida e eficiente os sistemas que foram comprometidos; resposta de ataque, associando contramedidas ativas (O'hara, 2004, apud Moresi, 2013).

Moresi (2013) afirma ainda que as organizações têm atuado fortemente na proteção da dimensão informacional aplicando contramedidas como firewall, *anti-spam*, controles de acesso etc. De outro modo, torna-se importante atuar ativamente na dimensão informacional, principal origem de vulnerabilidades. Assim o autor recomenda a adoção de procedimentos para a identificação preferencialmente automatizada de vulnerabilidades nas aplicações, e adicionalmente de serviços de certificação.

Quanto à compreensão de alguns termos, a atual legislação do Estado brasileiro é útil na compreensão dos termos "inteligência" e "contrainteligência". As definições a seguir foram extraídas da Lei 9.883/99 que instituiu o Sistema Brasileiro de Inteligência e criou a Agência Brasileira de Inteligência – ABIN. O marco legal definiu:

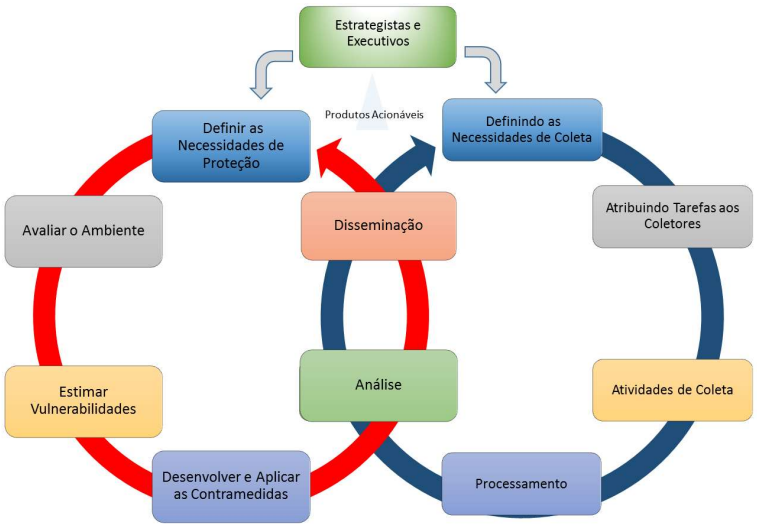
> Entende-se como a inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado. [...] Entende-se como contrainteligência a atividade que objetiva neutralizar a inteligência adversa (BRASIL, 1999).

Na literatura existem diversos trabalhos que descrevem ciclos (por vezes também denominados modelos ou processos) de inteligência e de contrainteligência, geralmente como disciplinas militares.

Duvenage e Von Solms (2012), propuseram um esboço conceitual para contrainteligência cibernética. Os autores definem contrainteligência como as atividades realizadas para identificar, avaliar, explorar, neutralizar e proteger contra ações de inteligência hostis que são prejudiciais ou potencialmente prejudiciais ao interesse de uma entidade. Para os autores as ações de contrainteligência apresentam-se em gradação entre passivas ou ativas e defensivas ou ofensivas. Em ações defensivas tem-se ações de negação, detecção e coleta. Em ações ofensivas, tem-se ações de coleta, perturbação, exploração e destruição.

Nolan (2002), propôs um ciclo integrado de inteligência e contrainteligência, originalmente orientado a negócios. A Figura 1 apresenta o modelo integrado de inteligência e contrainteligência.

FIGURA 1 - Modelo Integrado de Inteligência e Contrainteligência



Fonte: Adaptado de Nolan (2002, p. 239)

Nolan (2002) argumenta que o modelo integrado de inteligência se fundamenta na natureza cíclica dos modelos de coleta (inteligência) e de proteção da informação (contrainteligência) e que tal modelo traz os seguintes benefícios: aquisição e proteção de inteligência de maneira simultânea e organizada; diminuição do desperdício de recursos ou contramedidas desnecessárias; produção de inteligência de forma sinérgica; e, entendimento amplo e comum dos ambientes interno e externo da organização.

A adoção do ciclo integrado de inteligência e contrainteligência poderia, na análise dos autores, ser útil para aumentar a segurança e reduzir os ataques cibernéticos à infraestrutura crítica de comunicações, à medida que as informações enviadas por coletores – dispositivos de

segurança (como, por exemplo, *logs* de sistemas detecção ou prevenção à intrusão, *firewalls*, *honeypots,* antivírus, servidores de aplicação entre outros) – poderiam ser analisados de forma integrada, produzindo inteligência na forma de novas regras de segurança e, possibilitando o desenvolvimento de regras específicas a serem aplicadas, automaticamente ou não, aos dispositivos de segurança que compõe a infraestrutura de telecomunicações.

Com base nos ensinamentos de Gil (2008), este trabalho pode ser classificado em relação às dimensões de sua abordagem, de sua natureza, de seus objetivos e de seus procedimentos. O trabalho possui metodologia tipo qualitativa, quanto à sua abordagem, uma vez que busca compreender os fenômenos relacionados ao ciberespaço e à sua proteção e busca apresentar métodos que possibilitariam outros ganhos para a proteção cibernética da infraestrutura crítica de comunicação. Quanto à natureza, esta pesquisa é classificada como pesquisa aplicada, uma vez que busca criar conhecimentos para aplicação prática em relação ao seu problema de pesquisa. Em relação ao seu objetivo, esta pesquisa é classificada como exploratória, pois proporciona maior familiaridade junto ao tema de pesquisa. No que tange seus procedimentos, este trabalho é classificado como uma pesquisa documental, bibliográfica de levantamento de informações através de entrevistas abertas realizadas com atores relevantes na definição de políticas públicas e normas de cibersegurança para o setor de telecomunicações.

Para responder ao primeiro objetivo de pesquisa, foram analisados os artigos disponibilizados em periódicos acadêmicos em língua portuguesa ou inglesa relacionados à proteção da infraestrutura crítica com foco em comunicações e na cibersegurança publicados na Escola Superior de Defesa, na Escola Superior de Guerra e em outros repositórios, neste último caso com publicação a partir de 2020. Quando muitos resultados foram encontrados, foram analisados apenas os primeiros artigos em ordem de relevância da ferramenta relacionados ao tema deste estudo.

Quadro 1 – critérios para consulta de artigos científicos a serem analisados

Repositório	Critérios	Resultados encontrados
Scielo	(ti:(“critical infrastructure”)) e ano >= 2020	0
Scielo	(ti:(cybersecurity)) e ano >= 2020	41
Scielo	(ti:(“infraestrutura crítica”)) e ano >= 2020	2
Google Scholar	“infraestrutura crítica” e ano >= 2020	562
Google Scholar	"cybersecurity” e ano >= 2020	109.000
Google Scholar	“critical infrastructure” e ano >= 2020	31.200
Web of Science / Capes	“critical infrastructure” e ano >= 2020	3.777
Web of Science / Capes	“cybersecurity” e ano >= 2020	28.745
Web of Science / Capes	“infraestrutura crítica” e ano > 2020	13

Science Direct / Scopus	“critical infrastructure” e ano >= 2020	5.192
Science Direct / Scopus	“cybersecurity” e ano >= 2020	8.295
Science Direct /Scopus	“infraestrutura crítica” e ano >= 2020	-

Fonte: Elaborado pelos autores (2023).

Importa ressaltar que as bases acima relacionadas foram consultadas em relação aos termos “Política Nacional de Segurança de Infraestruturas Críticas”, “PNSic”, “Estratégia Nacional de Segurança de Infraestruturas Críticas”, “Ensic”, “Estratégia Nacional de Cibersegurança” e “E-Ciber”, todos relacionados às políticas brasileiras de cibersegurança e de proteção das infraestruturas críticas. Não foram encontrados resultados relacionados à estas pesquisas nas bases Scielo, Web of Science e Science Direct. Os resultados encontrados no Google Scholar e nos repositórios da Escola Superior de Defesa e da Escola Superior de Guerra estão apresentados no quadro 2. Todavia, destaca-se que nem todos resultados encontrados na ferramenta referem-se a artigos científicos, contendo outras informações não acadêmicas.

Quadro 2 – artigos relacionados às políticas brasileiras

Repositório	Critérios	Resultados encontrados
Google Scholar	“Política Nacional de Segurança de Infraestruturas Críticas” e ano >= 2020	35
Google Scholar	“Estratégia Nacional de Segurança de Infraestruturas Críticas” e ano >= 2020	17
Google Scholar	“Estratégia Nacional de Cibersegurança” e ano >= 2020	46
ESG / ESD	“Política Nacional de Segurança de Infraestruturas Críticas”	368
ESG / ESD	“Estratégia Nacional de Segurança de Infraestruturas Críticas”	370
ESG / ESD	“Estratégia Nacional de Cibersegurança”	22

Fonte: Elaborado pelos autores (2023).

Por último, foram realizadas entrevistas abertas com responsáveis sobre a definição e execução de políticas ou normas de cibersegurança do Ministério das Comunicações e da Agência Nacional de Telecomunicações (Anatel).

2. DESENVOLVIMENTO

Nesta seção iremos apresentar a síntese do arcabouço legal e normativo aplicável à cibersegurança e à proteção das infraestruturas críticas de telecomunicação, a literatura relevante, conforme proposto na metodologia, e o resumo com os principais temas tratados durante as entrevistas realizadas.

2.1 SÍNTESE DO ARCABOUÇO JURÍDICO-NORMATIVO APLICÁVEL

O arcabouço legal e normativo aplicável à proteção do ciberespaço e das infraestruturas críticas que compõe o ciberespaço tem crescido ao longo dos últimos anos.

Em 2015, a Associação Brasileira de Normas Técnicas (ABNT) publicou a 1ª versão da norma ISO/IEC 27032, denominada Tecnologia da Informação – Técnicas de segurança – Diretrizes para cibersegurança. Este documento não tem caráter impositivo para as organizações, mas é adotado como guia orientativo. Ele foi elaborado pelo Comitê Brasileiro de Computadores e Processamento de Dados e está de acordo com a norma internacional. Vale destacar que o documento trata da Cibersegurança e diferencia da Proteção da Infraestrutura Crítica de Informação. De acordo com a norma:

> a disponibilidade e a confiabilidade do ciberespaço, em muitos aspectos, dependem da disponibilidade e confiabilidade dos serviços de infraestrutura crítica relacionados, como a infraestrutura de rede de telecomunicações. A segurança do ciberespaço também está intimamente relacionada com a segurança da Internet, redes de empresas/lares e com a segurança da informação em geral. Convém notar que os domínios de segurança identificados [...] têm os seus próprios objetivos e escopo de foco. Lidar com questões de cibersegurança, portanto, requer comunicações e coordenação substanciais entre as diferentes entidades públicas e privadas de diferentes países e organizações. Serviços de infraestrutura crítica são considerados por alguns governos como serviços relacionados à segurança nacional e, portanto, podem não ser discutidos ou divulgados abertamente. Além disso, o conhecimento das fraquezas de infraestrutura crítica, se não for usado adequadamente, pode ter uma implicação direta na segurança nacional. Uma estrutura básica para compartilhamento e emissão de informações ou de coordenação de incidentes é, portanto, necessária para preencher as lacunas e proporcionar as garantias necessárias para as partes interessadas no Ciberespaço (ABNT, 2015, p.13).

Desse modo, a ABNT apresenta relação de importância que uma infraestrutura crítica de comunicação pode ter para a sociedade e para o país, demonstrando a necessidade de sua adequada proteção e requerendo a estrutura para compartilhamento e emissão de informações ou de coordenação de incidentes.

2.1.1 Arcabouço sobre segurança da infraestrutura crítica

Em dezembro de 2018, foi editado o Decreto nº 9.573 que trata da Política Nacional da Segurança de Infraestruturas Críticas (PNSIC). Essa política estabelece competência do Gabinete de Segurança Institucional (GSI) para acompanhamento dos assuntos pertinentes às infraestruturas críticas estabelecendo princípios, objetivos e diretrizes para o tema. A PNSIC prevê a criação da Estratégia Nacional de Segurança de Infraestruturas Críticas (Ensic) e do Plano Nacional de Segurança de Infraestruturas Críticas (Plansic). Toda via, o escopo dessa política é limitado à Administração Pública Federal (Brasil, 2018a).

Em dezembro de 2020, foi editado o Decreto nº 10.569 que estabeleceu a Estratégia Nacional de Segurança de Infraestruturas Críticas (Ensic). No que tange ao escopo do presente estudo, a Ensic já apresenta iniciativas específicas para alcançar o objetivo de "desenvolver um sistema dedicado à gestão de informações relacionadas à segurança de infraestruturas críticas". São elas: a iniciativa 4.2.1 - dispor de um sistema dedicado (central) para a captação, a integração, o armazenamento e o compartilhamento de informações relacionadas à segurança das infraestruturas críticas e a iniciativa 4.2.2 - "promover o compartilhamento de informações relevantes para a segurança de infraestruturas críticas, considerando regras de segurança da informação e a legislação específica" (Brasil, 2020b).

Em setembro de 2022 foi aprovado o Decreto nº 11.200, que estabeleceu o Plano Nacional de Segurança de Infraestruturas Críticas (Plansic). Este plano, decorrência direta da PNSIC e da Ensic, cria o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas e, no que tange ao escopo do presente estudo, define o Ministério das Comunicações como responsável pela elaboração de planos setoriais relacionados ao setor de telecomunicações (BRASIL, 2022a).

2.1.2 Arcabouço sobre cibersegurança

Em dezembro de 2018, foi instituída, por meio do Decreto nº 9.637, a Política Nacional de Segurança da Informação (PNSI). A PNSI abrange temas como a cibersegurança, a segurança física e proteção de dados organizacionais, ações destinadas a assegurar critérios essenciais da segurança da informação e a defesa cibernética, estabelecendo princípios, objetivos, instrumentos, e competência a diversos órgãos e entidades da administração pública federal. Cabe destacar que esta política é aplicável somente à Administração Pública Federal (Brasil, 2018c).

Em fevereiro de 2020, por meio do Decreto nº 10.222 e fundamentada na PNSI, foi instituída a Estratégia Nacional de Cibersegurança (E-Ciber). A E-Ciber, por sua vez, trouxe objetivos estratégicos e ações estratégicas dentro de eixos temáticos identificados como críticos à cibersegurança da Administração Pública Federal (Brasil, 2020b).

Em dezembro de 2020, por meio da Resolução nº 740, a Agência Nacional de Telecomunicações (Anatel) publicou o Regulamento de Cibersegurança Aplicada ao Setor de Telecomunicações. Este regulamento estabelece definições, princípios, diretrizes, obrigações observáveis às operadoras de serviços públicos de telecomunicações, determinando ainda a

necessidade de que essas empresas possuam políticas de cibersegurança, notifiquem incidentes relevantes, estabeleçam ciclos de avaliação de vulnerabilidades relacionadas à cibersegurança e enviem informações sobre as infraestruturas críticas de telecomunicações (Brasil, 2020c).

Em seu turno, em janeiro de 2021, a Anatel, fundamentando-se na E-Ciber e em outros normativos, editou o ato nº 77, que definiu requisitos de cibersegurança para equipamentos de telecomunicações. Assim, os equipamentos utilizados para a prestação de serviços de telecomunicação passaram a prescindir de critérios mínimos relacionados à atualização de *software/firmaware,* ao gerenciamento remoto, à instalação e operação, acesso para configuração, a serviços de comunicação de dados, aos dados pessoais e dados pessoais sensíveis e à capacidade de mitigação de ataques. O ato normativo também definiu critérios aplicáveis aos fornecedores de equipamentos de telecomunicação (Brasil, 2021).

2.1.3 Propostas em discussão

Durante o desenvolvimento deste trabalho encontra-se em discussão projeto de lei que institui a Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCiber) (Brasil, 2023). De acordo com a minuta:

> a PNCiber é uma proposta voltada a unificar a "colcha de retalhos" regulatória existente no país, minimizar o crescente número de incidentes que acometem o país, gerando enormes prejuízos para a sociedade brasileira, buscar diminuir o débito tecnológico nacional no setor, e ampliar a participação brasileira na cooperação internacional sobre a temática. (BRASIL, 2023, p. 1).

A proposta propõe integrar o arcabouço jurídico relacionado à cibersegurança em um único instrumento legal e, se aprovado pelo Congresso Nacional, passará a ser aplicável à toda a sociedade brasileira. A proposta baseia-se nas melhores práticas mundiais e propõe a criação da Agência Nacional de Cibersegurança (ANCiber), agência reguladora vinculada ao Gabinete de Segurança Institucional (GSI). Dentre o escopo deste estudo, destaca-se a criação de uma unidade organizacional de inteligência, com atribuições inerentes às atividades desta espécie.

2.2 REVISÃO DA LITERATURA PRODUZIDA PELA ESCOLA SUPERIOR DE DEFESA E PELA ESCOLA SUPERIOR DE GUERRA

Diversos estudos existentes nos repositórios da Escola Superior de Defesa e da Escola Superior de Guerra abordam a proteção do ciberespaço. Entre os estudos relacionados ao tema desta pesquisa destacam-se os seguintes:

Costa, Ferreira e Cabral (2022) afirmam que o Estado brasileiro é vulnerável a ameaças que trafegam no ciberespaço. Os autores apresentaram desafios em relação à certificação de produtos de tecnologia da informação e comunicação, bem como alertas relacionados a produtos não certificados em cibersegurança. Em suas conclusões, os autores propuseram que a criação de uma Agência Brasileira de Cibersegurança poderia mitigar as vulnerabilidades por eles constatadas. Cabe ressaltar que a criação desta agência está em discussão no nível político do Governo Federal, conforme já apresentado na seção 2.1.3.

Monfardini (2020) analisou se as medidas e os mecanismos de proteção das informações do Serviço Federal de Processamento de Dados (Serpro) estariam em aderência com a Estratégia Nacional de Cibersegurança. No trabalho, o autor constata que "o Serpro possui uma estrutura interna de gestão de segurança da informação e governança cibernética robusta, e que está alinhada aos propósitos da E-Ciber" (p. 21).

Araújo (2020) estudou a proteção de infraestruturas críticas do Brasil. O autor aponta marcos como a criação do Centro de Defesa Cibernética, em 2012, e do Comando de Defesa Cibernética, em 2016, e as ações de coordenação com o Gabinete de Segurança Institucional, visando a participação da Defesa Cibernética na proteção de infraestruturas críticas. O autor destaca o Exercício Guardião Cibernético (EGC), coordenado pelo ComDCiber, que conta a participação de diversos atores e ressalta a cooperação entre esses atores como ação fundamental para mitigar as ameaças no setor cibernético.

Segundo (2019) identificou que o número de ataques cibernéticos tem crescido ao longo do tempo. O autor destaca os ataques contra o Estado e que impactam a infraestrutura crítica do País – meios de telecomunicações, energia, finanças, água e transporte. Para o autor, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou mesmo aqueles que permitam seu pronto restabelecimento.

Oliveira (2021) analisou a adoção da tecnologia de comunicação móvel de quinta geração (5G) em diversos países com foco nos impactos à Segurança Nacional. Neste estudo, a autoria apresenta informações sobre como a China utilizou-se do Desenvolvimento da tecnologia 5G como forma de domínio da cadeia produtiva da tecnologia e as estratégias de reação dos Estados Unidos para a redução do avanço. Para a autora "é vital que o Brasil passe a ser um ator desenvolvedor de tecnologia, especializando-se nos segmentos necessários e

relevantes, deixando de ser refém de um ou outro fornecedor. A dependência de um único fornecedor seria uma ameaça à Segurança" (p. 35).

2.3 REVISÃO DE OUTROS ARTIGOS ACADÊMICOS

Os artigos acadêmicos analisados possuem muita dispersão quanto à área de conhecimento de sua aplicabilidade. Alguns estão relacionados à área de ciência da computação, outros à geopolítica e outros relacionados ao direito. Isso demonstra o caráter multidisciplinar e transversal em relação ao tema abordado. A seguir apresenta-se a síntese dos principais artigos analisados.

De acordo com Belli (2021), Brasil, Rússia, Índia, China e África do Sul deram especial atenção à cibersegurança na Declaração de Nova Delhi. Para o autor, os governos destes países adotaram inúmeras leis e regulações e que a cooperação entre os membros do BRICS tem avançado, possibilitando combinar política, tecnologia e iniciativas de pesquisa.

Martínez (2022) utilizou da metodologia Pestel (Político, Econômica, Social, Ecológico e Legal) para prospectar tendências relacionadas à cibersegurança na Colômbia. No escopo deste estudo, o autor identifica, dentre outras, questões relacionadas ao roubo e venda de identidade e informações sensíveis, roubo de informações sensíveis do Estado, patrocínio de ataques cibernéticos com fins econômicos e de extorsão e incremento das regulamentações e controle de dados.

Svintsytskyi (2022) descreveu o sistema de cibersegurança da Ucrânia e seu papel para a segurança nacional. Para o autor, a cibersegurança precisa ser endereçada de forma abrangente e requer ação coordenada em nível nacional, regional e internacional com o objetivo de prevenir, preparar e responder aos incidentes pelo governo, setor privado e sociedade civil. O autor identifica problemas como a falta de pessoal especializado, a inconsistência da legislação com a realidade contemporânea e a dificuldade de organizar a interação entre as entidades que tratam sobre o tema. O autor propõe a criação de uma plataforma de pesquisas avançada em cibersegurança.

Purasiainen e Kytomaa (2023) analisaram o desenvolvimento sobre a legislação relacionada à infraestrutura crítica da União Europeia, que atende a 27 países desenvolvidos. A legislação sobre infraestruturas críticas é de 2008, portanto, quase uma década anterior à legislação brasileira. Os autores apresentam que, desde 2017, tem havido discussões sobre a ampliação do arcabouço legal para incluir o conceito de "resiliência", termo que se refere-se ao

"'antes, durante e depois' de um evento indesejado ou disrupção da infraestrutura crítica e que cobre todo o ciclo de gerenciamento de crise" (PURASIAINEN e KYTOMAA, 2023, p. 87, tradução dos autores). Em 2022, a legislação sofreu alterações, estando a "proteção da infraestrutura crítica" alterada para a "resiliência das entidades críticas", isto é, "a manutenção das funções sociais vitais ou atividades econômicas do mercado interno" (Comissão Europeia, *apud* PURASIAINEN e KYTOMAA, 2023, p. 89, tradução dos autores).

Ninković (2021) analisou documentos oficiais dos Estados Unidos da América (EUA), Reino Unido e Austrália sobre a resiliência da infraestrutura crítica destes países. De acordo com autor, o termo "resiliência" passa a ser adotado nos documentos do Departamento de Segurança Interna dos EUA em 2002. Dentre outras definições, o termo pode ser compreendido como a "capacidade dos sistemas, das infraestruturas, do governo, das empresas e dos cidadãos para resistir, absorver, recuperar ou adaptar-se a uma ocorrência adversa que possa causar dano, destruição ou perda de importância nacional" (Departamento de Segurança Interna dos EUA *apud* NINKOVIĆ, 2021, tradução dos autores).

Llanten-Lucio, Amador-Donado, Márceles-Villalba (2022a, 2022b) propuseram a validação de um *framework* de cibersegurança para mitigação de ameaças. De acordo com os autores, mesmo utilizando-se de *hardware* com limitações de capacidade, foi possível demonstrar a operação do *framework* ao reconhecer ataques e automaticamente gerar regras de identificação.

Silaule, Makhubele e Mamorobela (2022) desenvolveram um modelo para reduzir as ameaças internas de cibersegurança em uma empresa de telecomunicações sul-africana. Para os autores, as normas de pessoal levam à redução da intenção de comportamento inapropriado e, consequentemente à redução das ameaças internas.

Pinto e Grassi (2020) buscaram compreender como o Brasil está atuando em relação à segurança de suas infraestruturas críticas. Todavia, os autores destacaram projetos orientados a temas de defesa, como o Sistema Militar de Defesa Cibernética (SMDC), o Simulador de Operações Cibernéticas (Simoc), o Centro de Defesa Cibernética do Exército Brasileiro (CDCiber), o Comando de Defesa Cibernética (ComDCiber) e a Escola Nacional de Defesa Cibernética (ENaDCiber).

Vichi, Pinto e Sá (2020) consideram necessário ampliar estudos sobre políticas de segurança relacionadas à infraestrutura de cabos submarinos no Brasil. Identificaram poucos

pontos de ancoramento e que esses cabos são operados por uma pequena quantidade de empresas privadas. Lopes (2021) realizou mapeamento dos cabos submarinos, relacionando-os com os com os Distritos Navais que cobrem a região e propõe a regulação do uso do mar no que tange a proteção dessa valiosa infraestrutura de comunicação.

Ademais, da análise dos artigos é possível constatar que a legislação dos EUA está avançando para o conceito de "resiliência das infraestruturas críticas", e, no caso da União Europeia, para "resiliência das entidades críticas", indicando que, possivelmente o arcabouço regulatório brasileiro relacionado à proteção das infraestruturas críticas tenha de ser atualizado. Assim sugere-se, também, estudos relacionados à resiliência das entidades críticas

2.4 ENTREVISTAS REALIZADAS

Para a realização deste estudo exploratório foram realizadas duas entrevistas abertas com representantes do alto escalão da Agência Nacional de Telecomunicações (Anatel) e do Ministério das Comunicações (MCom).

2.4.1 Agência Nacional de Telecomuniações

Na Agência Nacional de Telecomunicações, o entrevistado foi o senhor Gustavo Santana Borges, Superintendente de Controle de Obrigações da agência. Para o entrevistado, as questões relacionadas à cibersegurança e segurança da infraestrutura crítica tem ganhado cada vez mais relevância, em especial devido ao desenvolvimento de tecnologias como as tecnologias de redes definidas por software ou de comunicação móvel de quinta geração (5G).

O órgão tem sua atuação pautada para a prestação pelas operadoras dos serviços de telecomunicação, sendo estes serviços considerados serviços essenciais à população. Neste sentido, a Agência preocupa-se com a disponibilidade dos serviços de telecomunicação. Essa disponibilidade pode ser avaliada, em boa medida, pela redundância dos sistemas e por meio de ações de conformidade, inspeções físicas e notificações de inconformidades.

A Agência aprovou em 2021 o Regulamento de Cibersegurança Aplicada ao Setor de Telecomunicações (vide seção 2.1.2). O cumprimento das obrigações estabelecidas por parte das operadoras é monitorado pelo Grupo de Trabalho para assuntos cibernéticos (GT-Ciber) que realiza a validação da conformidade e inspeções, todavia os resultados consolidados ainda não estão disponíveis para consulta.

O gestor entende que a cibersegurança é inerente ao negócio das operadoras de telecomunicação, sendo o papel da agência complementar uma vez que os serviços de

telecomunicações são considerados serviços essenciais para a população. O gestor observa que, mesmo antes da vigência do regulamento, as empresas realizaram investimentos em estrutura organizacional, infraestrutura de telecomunicação, formação de especialistas em cibersegurança e obtenção de ferramentas de segurança.

A Agência atua ao definir procedimentos de contingência, como o reestabelecimento dos serviços, o trabalho de reação a crises, na abertura de *roaming* entre operadoras e na disponibilização de antenas móveis, possibilitando a recuperação dos serviços no caso de interrupções como, por exemplo, as que ocorrem nos eventos climáticos.

Há, também, trabalho realizado em conjunto com o Gabinete de Segurança Institucional para o caso de paralização de serviços dos órgãos públicos. Todavia, órgãos de missão crítica (destaque para o setor elétrico e financeiro) precisam definir e manter a redundância de suas infraestruturas. O entrevistado destacou intersecção entre a segurança e a defesa, em especial com o apoio do Guardião Cibernético para a definição de protocolos de reação.

Hoje há uma lista de notificação de incidentes cibernéticos, como por exemplo, ataque de negação de serviço distribuído (ataque DDoS), roubo de dados, acesso indevido, *ramsomware*. Porém não há o compartilhamento das evidências e artefatos utilizados nos ataques.

Em relação à rede de comunicação da administração pública federal, o gestor observou que a Anatel não participa da definição de requisitos de segurança dos serviços de telecomunicação contratados pelo Governo; esta decisão competiria ao próprio órgão ou entidade da administração, em conformidade com especificação para contratação em edital.

Na análise do entrevistado, os setores elétrico, financeiro e de telecomunicação possuem maior maturidade em cibersegurança em relação aos demais. Para ele, falta órgão de governo que promova visão transversal no País, inclusive no âmbito estadual e municipal e serviços essenciais em geral. Todavia, deve-se tomar cuidado com o incremento na redundância de esforços para tratar os assuntos relacionados ao ciberespaço.

2.4.2 Ministério das Comunicações

No Ministério das Comunicações (MCom), o entrevistado foi o senhor Agostinho Linhares de Souza Filho, Coordenador-Geral de Acompanhamento Regulatório de Telecomunicações.

O entrevistado menciona a existência dos diversos decretos relacionados ao assunto, desde a transformação digital do governo até a PNSIC. Destacou que, em função da PNSIC, o Ministério está realizando o mapeamento das infraestruturas críticas, sendo as principais identificadas até o momento o SGDC, o *backbone,* os cabos submarinos e os projetos para o desenvolvimento da Rede de Atendimento à Administração Pública Federal (RAAPF) e da Rede Móvel Segura do DF (RMSDF).

O SGDC é considerado crítico por possuir, em 100% do território nacional cobertura civil e militar. O entrevistado ressalta que os novos satélites estão sendo construídos com a tecnologia de redes definidas por software e poderiam ser utilizados como *backup* ou contingência de sistemas críticos, desde que se insira algum requisito de segurança adicional (como por exemplo, criptografia). Todavia, isso traria um nível de dependência das empresas estrangeiras de comunicação, caso já registrado com o bloqueio realizado por uma operadora na guerra Ucrânia.

Em relação aos cabos de comunicação submarinos, o entrevistado destaca que estes cabos estão concentrados na cidade de Fortaleza, Ceará. As mais diversas operadoras de telecomunicação que hoje não contam com adequada proteção no ponto de ancoragem até a chegada no *datacenter*. Um sinistro significativo que ocorra em Fortaleza poderia, em tese, desconectar o Brasil do resto do mundo. O entrevistado menciona também a ausência de uma rota para escoamento do tráfego via Oceano Pacífico, o que poderia ser uma redundância adicional para as comunicações do País.

3. DISCUSSÃO DOS RESULTADOS

Em relação à pesquisa bibliográfica apresentada, merece destaque o fato que foi identificado número pequeno de estudos acadêmicos relacionados à proteção da infraestrutura crítica em língua pátria se comparado aos estudos em língua inglesa. Do mesmo modo, são poucos os estudos relacionados à Política Nacional da Segurança de Infraestruturas Críticas (PNSIC), a Estratégia Nacional de Segurança de Infraestruturas Críticas (Ensic) e a Estratégia Nacional de Cibersegurança (E-Ciber), estando estes estudos concentrados na Escola Superior de Defesa e na Escola Superior de Guerra.

Em relação aos métodos e às propostas de aprimoramento que possibilitariam outros ganhos para cibersegurança, durante a pesquisa, dentre os artigos analisados, não foi encontrado nenhum estudo propondo integração dos ciclos de inteligência e contrainteligência (Nolan,

2002) com enfoque em cibersegurança. Todavia, a norma ABNT ISO/IEC 27032, ao indicar a necessidade de uma estrutura básica para compartilhamento e emissão de informações ou de coordenação de incidentes, requer, de algum modo, a integração dos ciclos de inteligência e contrainteligência. Essa integração também pode ser encontrada no projeto de lei que cria a Agência Nacional de Cibersegurança (ANCiber), uma vez que a proposta inclui uma unidade organizacional com atribuições de inteligência, o que levaria a adoção, ainda que indireta, do modelo.

Na análise dos autores, a adoção do ciclo integrado de inteligência e contrainteligência não seria uma medida simples. Ela exigiria a formação de equipe técnica nas áreas de ciência da computação, ciência de dados, engenharia de software e de computação qualificada especialmente para questões relacionadas à cibersegurança, além do desenvolvimento de *hardware* e *software* especializado em coleta e análise de informações relacionadas aos ataques cibernéticos para posterior análise, desenvolvimento e aplicação de contramedidas de segurança. Neste ponto, destaca-se que o *framework* proposto por de Llanten-Lucio, Amador-Donado, Márceles-Villalba (2022a, 2022b) pode ser útil na coleta de informações de inteligência em cibersegurança.

Ao longo desse estudo, pode-se identificar que, nos últimos anos, foram aprovadas, no âmbito do Poder Executivo Federal, uma série de normas que tratam sobre cibersegurança e infraestrutura crítica. Destacam-se: a Política Nacional da Segurança de Infraestruturas Críticas (PNSIC), a Estratégia Nacional de Segurança de Infraestruturas Críticas (Ensic), o Plano Nacional de Segurança de Infraestruturas Críticas (Plansic), a Política Nacional de Segurança da Informação (PNSI) e a Estratégia Nacional de Cibersegurança (E-Ciber). Essas normas têm sido academicamente estudas, em especial, no âmbito da Escola Superior de Defesa e da Escola Superior de Guerra. Foram encontrados poucos estudos fora do âmbito dessas escolas.

Da análise do arcabouço legal, a edição da PNSIC e da PNSI deu atribuições relevantes ao Gabinete de Segurança Institucional como coordenador das ações de cibersegurança e de segurança das infraestruturas críticas em diversos documentos esparsos. A integração entre os órgãos e entidades da Administração Pública Federal ainda está em desenvolvimento, em especial, ao se considerar a proposição da Política Nacional de Cibersegurança (PNCiber). A natureza desses normativos limitam sua aplicabilidade apenas à Administração Pública Federal.

Por força de regulamentos da Anatel, as operadoras privadas de telecomunicação, na qualidade de empresas prestadoras de serviço de interesse público relevante, têm iniciado ações

para garantir a cibersegurança e a infraestrutura crítica provida por essas empresas.
Todavia, os requisitos de cibersegurança dos serviços contratados pelos órgãos e entidades da Administração Pública Federal são definidos nos termos de referência por eles produzidos. Como existem órgãos com diferentes níveis de expertise, a cibersegurança pode ser mais frágil em determinado órgão ou entidade, possivelmente reduzindo o nível de segurança de toda a rede da administração pública.

A Telebras, por ser sociedade de economia mista vinculada à Administração Pública Federal, tem contribuído para a proteção das comunicações governamentais. Essa constatação justifica-se à medida em que seus projetos atuais (*backbone* e SGDC), bem como os projetos em desenvolvimento – Rede de Atendimento à Administração Pública Federal (RAAPF) e Rede Móvel Segura do DF (RMSDF) – alinham-se às Políticas de segurança definidas pelo Estado (PNSIC e PNSI) e apresentam-se como uma evolução quanto aos requisitos de segurança. Neste ponto, é importante mencionar que Rede da Atendimento à Administração Pública Federal (RAAPF) conectará órgãos da Administração Pública e contará com o Serviço de Comunicações Seguras do Estado (SCSE), com o objetivo a privacidade e o sigilo dos dados trafegados. A Rede Móvel Segura do DF (RMSDF) será uma rede de comunicação que utilizará uma rede de comunicação móvel de quarta geração (4G) para conectar os dispositivos de comunicação (rádio comunicadores) das diversas forças de defesa e segurança. Como a RAAPF e a RMSDF ainda são projetos em desenvolvimento, não foram incluídas no escopo deste estudo.

Nos termos da norma ABNT ISO/IEC 27032, serviços de infraestrutura crítica são considerados por alguns governos como serviços relacionados à segurança nacional. Assim, constata-se que, os serviços prestados pela Telebras poderão vir a ser considerados como de segurança nacional no futuro, em especial, com o início da operação da RAAPF e da RMSDF.

Outro achado importante, que originalmente não fez parte do escopo deste estudo e merece destaque, é o fato de que o representante do Ministério das Comunicações mencionou a dependência brasileira em relação aos cabos submarinos ancorados em Fortaleza. Esse apontamento vai ao encontro dos trabalhos de Vichi, Pinto e Sá (2020) e Lopes (2021) uma vez que as comunicações de alta velocidade globais se realizam majoritariamente através dos cabos submarinos. Sobre este ponto, cumpre mencionar que a Telebras até 2018 era sócia do empreendimento de lançamento do cabo submarino Ella Link, que conecta Fortaleza no Brasil a Sines em Portugal, além de outras cidades. A maioria das conexões submarinas originadas no

Brasil são terminadas nos Estados Unidos. Assim, a participação da Telebras no empreendimento era entendida como estratégica uma vez que o projeto estabelece uma rota direta entre Brasil e Portugal, sendo uma alternativa para escoamento do tráfego, além de apresentar melhor qualidade de serviços. Por falta de previsão orçamentária de investimentos, a empresa teve de se retirar do negócio, possibilitando a sua continuidade de modo independente (Telebras, 2018).

A partir das entrevistas realizadas, recebeu menções e merece destaque o Exercício Guardião Cibernético, organizado pelo Comando de Defesa Cibernética do Exército (ComDCiber). De acordo com os entrevistados, o exercício permite que as empresas melhorem seus processos relacionados à cibersegurança. Ressalta-se que a Telebras tem participado dos exercícios. Todavia, a análise em Defesa Cibernética não foi escopo deste estudo.

Para responder à questão de "como órgãos e entidades da Administração apoiam e poderiam contribuir para ampliar a proteção das comunicações da Administração Pública Federal no ciberespaço" foi possível constatar que, dentro de suas competências, os órgãos e entidades da Administração Pública Federal estão realizando atividades que promovam a cibersegurança e segurança das infraestruturas críticas de telecomunicações. Todavia, o arcabouço legal atual é diretamente aplicável apenas às entidades integrantes da Administração Pública Federal, tornando incompleta a segurança desses itens, em especial no que tange aos Estados, Municípios, às empresas e à sociedade em geral. Vislumbra-se necessário um arcabouço legal e normativo que contemple a proteção das comunicações de todos os entes estatais. Caso contrário, a proteção seria incompleta.

Em relação aos métodos e às propostas de aprimoramento que possibilitariam outros ganhos para cibersegurança, durante a pesquisa, dentre os artigos analisados, não foi encontrado nenhum estudo propondo integração dos ciclos de inteligência e contrainteligência para cibersegurança.

Havia uma expectativa de que, de algum modo, os órgãos e entidades que operam e mantém a infraestrutura críticas da Administração Pública Federal pudessem estar compartilhando informações entre si e utilizando o ciclo integrado de inteligência e contrainteligência proposto por Nolan (2002) para promover a cibersegurança dessas infraestruturas. Todavia não foi possível constatar a adoção do referido ciclo. O arcabouço legal e regulatório a que se refere o tema é aplicável apenas aos órgãos e entidades que compõe a Administração Pública Federal e o arcabouço legal e regulatório aplicável não fundamenta tal

hipótese. É possível vislumbrar que, no futuro, com a aprovação pelo Congresso Nacional da proposta para Política Nacional de Cibersegurança (PNCiber), venha a ser possível a realização de atividades de inteligência e contrainteligência para a cibersegurança e segurança das infraestruturas críticas de comunicação do País.

Considerando o avanço no arcabouço normativo dos EUA e da União Europeia e as críticas contidas no estudo de Svintsytskyi (2022) sobre o sistema de cibersegurança da Ucrânia e a opinião colhida com os entrevistados, parece que a adoção da Política Nacional de Cibersegurança possibilitará, no futuro próximo, resultados mais efetivos à necessidade do País quanto à proteção de suas infraestruturas críticas. Essa análise se justifica à medida em que: (i) reduz o arcabouço legal; (ii) integra as ações em um órgão; (iii) promove a contratação de pessoal qualificado; (iv) amplia o escopo do atual arcabouço para incluir os estados, os municípios, o setor privado e a população em geral.

4. CONSIDERAÇÕES FINAIS

A intenção deste trabalho foi descrever como os órgãos e as entidades da Administração apoiam e poderiam contribuir para ampliar a proteção das comunicações da Administração Pública Federal no ciberespaço, supondo a possível adoção do ciclo integrado de inteligência e contrainteligência. A análise baseia-se na necessidade de melhoria das medidas de cibersegurança adotadas e a serem adotadas pela empresa Telecomunicações Brasileiras S/A – Telebras – uma sociedade de economia mista federal, que, desde 2010, tem a atribuição de implementar a rede da administração pública federal e desde 2012 participa do projeto que lançou e opera o Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC). A empresa também participa dos projetos Rede de Atendimento à Administração Pública Federal (RAAPF), que conectará órgãos da Administração Pública, e da Rede Móvel Segura do DF (RMSDF), que integra os sistemas de comunicação da defesa e das forças de segurança, ambos em desenvolvimento.

Como integrante da Administração Pública Federal (APF), a Telebras busca atender às Políticas de Estado relacionadas à cibersegurança e da infraestrutura crítica de telecomunicação. Constatou-se que as políticas relacionadas à cibersegurança e à segurança das infraestruturas críticas se aplicam apenas à APF, tornando-as incompletas para a segurança da sociedade como um todo. Constatou-se também que o marco regulatório que possibilitaria maior proteção de toda a sociedade ainda está em discussão junto ao Congresso Nacional. Não foi possível identificar estudos ou indicações que confirmem a hipótese de que o ciclo integrado de

inteligência e contrainteligência esteja sendo adotado pelas entidades que cuidam da cibersegurança e da segurança das infraestruturas críticas de telecomunicações do País.

4.1 ESTUDOS FUTUROS

Observada as conexões dos cabos submarinos brasileiros (LOPES, 2021), pode-se constatar que essas comunicações ocorrem exclusivamente por meio do Oceano Atlântico. Cabe destacar que o governo brasileiro mantém o programa Norte Conectado. Esse programa, com apoio de diversas empresas, está construindo uma rede de cabos subfluviais que conectarão 59 municípios na região amazônica. Assim, à guisa de estudos futuros, é possível vislumbrar que, com a conclusão do projeto Norte Conectado, possa ser estabelecido uma ancoragem de cabo submarino no Oceano Pacífico e por sua vez, conectado aos cabos subfluviais a Amazônia. Essa medida representaria uma rota alternativa do tráfego de comunicação, diminuindo a dependência de Fortaleza e aumentando a resiliência da infraestrutura. Sugere-se também estudos relacionados à defesa dos meios de comunicação subfluviais.

Ao longo do desenvolvimento deste estudo, foram analisados a proposta de convergência de esforços realizada pelos BRICS, a adoção da metodologia Pestel para prospectar ameaças a cibersegurança na Colômbia, o sistema de cibersegurança adotado pela Ucrânia, União Europeia, Estados Unidos da América, Reino Unido e Austrália. Um comparativo entre os arcabouços regulatórios entre diferentes países não foi escopo para este estudo, porém fica como sugestão de estudos futuros.

Ademais, da análise dos artigos é possível constatar que a legislação dos EUA está avançando para o conceito de “resiliência das infraestruturas críticas”, e, no caso da União Europeia, para “resiliência das entidades críticas”, indicando que, possivelmente o arcabouço regulatório brasileiro relacionado à proteção das infraestruturas críticas tenha de ser atualizado. Assim sugere-se, também, estudos relacionados à resiliência das entidades críticas.

Sugere-se também, a título de estudos futuros, aplicar uma metodologia que identifique a tendência da pesquisa em relação aos artigos científicos que abordem os temas tratados neste estudo, em especial, classificando-os de acordo com a área do conhecimento e realizando análise das palavras chaves dos textos publicados.

REFERÊNCIAS

ARAUJO, José Euclides Oliveira de. **A atuação da defesa cibernética na proteção de infraestruturas críticas do Brasil**. 2020. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa) – Escola Superior de Guerra, Campus Brasília, DF, 2020. Disponível em: https://repositorio.esg.br/handle/123456789/1258. Acesso em: 08 jun. 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27032**: Tecnologia da Informação – Técnicas de Segurança – Diretrizes para Cibersegurança. Rio de Janeiro, 2015.

BELLI, Luca. Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. **The African Journal of Information and Communication**, [*S.l.*], v. 28, p. 1-14, 2021. Disponível em: https://orcid.org/0000-0002-9997-2998. Acesso em: 3 ago. 2023.

BRASIL. Lei n° 9.883 de 07 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, 08 dez. 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9883.htm. Acesso em: 08 jun. 2016.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa.** 2ª ed. Brasília, DF: Ministério da Defesa, 2008. Disponível em: http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf. Acesso em: 30 abr. 2023.

BRASIL. Decreto nº 7.175 de 12 de maio de 2010. Institui o Programa Nacional de Banda Larga - PNBL; dispõe sobre remanejamento de cargos em comissão; altera o Anexo II ao Decreto no 6.188, de 17 de agosto de 2007; altera e acresce dispositivos ao Decreto no 6.948, de 25 de agosto de 2009; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, 13 mai. 2010. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/decreto/d7175.htm. Acesso em: 08 jun. 2023.

BRASIL, Decreto nº 8.135, de 4 de novembro de 2013. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. **Diário Oficial da União**: seção 1, Brasília, DF, 05 nov. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8135.htm. Acesso em: 08 jun. 2023.

BRASIL. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995**. Diário Oficial da União**: seção 1, Brasília, DF, 17 jul. 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 08 jun. 2023.

BRASIL. Decreto Nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial da União**: seção 1, Brasília, DF, 23 nov.

2018. (2018ª). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 3 ago. 2023.

BRASIL. Decreto Nº 9.612, de 17 de dezembro de 2018. Dispõe sobre políticas públicas de telecomunicações. **Diário Oficial da União**: seção 1, Brasília, DF, 18 dez. 2018. (2018b). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9612.htm. Acesso em: 08 jun. 2023.

BRASIL. Decreto Nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. **Diário Oficial da União**: seção 1, Brasília, DF, 27 dez. 2018. (2018c). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 3 ago. 2023.

BRASIL. Decreto Nº 10.222 de 5 de fevereito de 2020. Aprova a Estratégia Nacional de Cibersegurança. **Diário Oficial da União**: seção 1, Brasília, DF, 06 fev. 2020. (2020ª). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 3 ago. 2023.

BRASIL. Decreto Nº 10.569 de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial da União**: seção 1, Brasília, DF, 10 dez. 2020. (2020b). Disponível em: https://www.planalto.gov.br/cCivil_03/_Ato2019-2022/2020/Decreto/D10569.htm. Acesso em: 3 ago. 2023.

BRASIL. Resolução nº 740, de 21 de dezembro de 2020. Aprova o Regulamento de Cibersegurança Aplicada ao Setor de Telecomunicações. **Diário Oficial da União**: seção 1, Brasília, DF, 24 dez. 2020. (2020c). Disponível em: https://www.in.gov.br/web/dou/-/resolucao-n-740-de-21-de-dezembro-de-2020-296152776. Acesso em; 3 ago. 2023.

BRASIL. Ato nº 77, de 5 de janeiro de 2021. Requisitos de Cibersegurança para Equipamentos para Telecomunicações. **Diário Oficial da União**: seção 1, Brasília, DF, 07 jan. 2021. Disponível em: https://www.in.gov.br/web/dou/-/ato-n-77-de-5-de-janeiro-de-2021-297933302. Acesso em: 3 ago. 2023.

BRASIL. Decreto Nº 11.200, de 15 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial da União**: seção 1, Brasília, DF, 16 set. 2022. (2022a). Disponível em: https://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2022/Decreto/D11200.htm. Acesso em; 3 ago. 2023.

BRASIL. Decreto Nº 11.299, de 21 de dezembro de 2022. Altera o Decreto nº 9.612, de 17 de dezembro de 2018, que dispõe sobre as políticas públicas de telecomunicações. **Diário Oficial da União**: seção 1, Brasília, DF, 22 dez. 2022. (2022b) Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11299.htm. Acesso em: 08 jun. 2023.

BRASIL. Decreto Nº 11.299, de 21 de dezembro de 2022. Altera o Decreto nº 9.612, de 17 de dezembro de 2018, que dispõe sobre as políticas públicas de telecomunicações. **Diário Oficial da União**: seção 1, Brasília, DF, 22 dez. 2022. Disponível em:

http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11299.htm. Acesso em: 8 jun. 2023.

BRASIL. Presidência da República. **PNCiber – Apresentação do Projeto**. Audiência Pública nº 01/2023. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf. Acesso em: 3 ago. 2023

COSTA, Álvaro Lobo; FERREIRA, André Luiz Alves; CABRAL, Victor José Queiroz. **A Criação de uma Agência Brasileira de Cibersegurança como Estratégia de Defesa Nacional**. 2022. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa) – Escola Superior de Defesa, Brasília, DF, 2022. Disponível em: https://repositorio.esg.br/handle/123456789/1650. Acesso em: 8 jun. 2023.

DONADO, Siler Amador; LUCIO, Yeisón Isaac; MÁRCELES, Katerine. Arquitectura de un Framework de ciberseguridad inteligente basado en tecnología Blockchain para IIoT. **Ingeniería y competitividad: revista científica y tecnológica**, [*S.l.*], v. 24, n. 2, p. 1-13, 2022. Disponível em: https://doi.org/10.25100/iyc.v24i2.11761. Acesso em: 3 ago. 2023.

DUVENAGE, Petrus; VON SOLMS, Sebastiaan. The case for cyber counterintelligence. In: **2013 International Conference on Adaptive Science and Technology**. [*S.l.*], IEEE, 2013. p. 1-8. Disponível em: https://ieeexplore.ieee.org/document/6707493. Acesso em: 01 out. 2023.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

LEVI, Pierre. **A inteligência coletiva: por uma antropologia do ciberespaço**. 3ª ed. São Paulo: Loyola, 2000.

LLANTEN-LUCIO, Yeison-Isaac; AMADOR-DONADO, Siler; MÁRCELES-VILLALBA, Katerine. Validation of Cybersecurity Framework for Threat Mitigation. **Revista Facultad de Ingeniería**, [*S.l.*], v. 31, n. 62, 2022. Disponível em: https://doi.org/10.19053/01211129.v31.n62.2022.14840. Acesso em: 3 ago 2023.

MARTÍNEZ, J. J. Cano. Prospectiva de ciberseguridad nacional para Colombia a 2030. **Revista Científica General José María Córdova**, [*S.l.*], 20(40), 815-832, 2022. Disponível em: https://dx.doi.org/10.21830/19006586.86. Acesso em: 3 ago. 2023.

MONFARDINI, Luiz Augusto Fonseca. **Análise das Medidas de Proteção das Informações Econômico-Fiscais no Serpro acerca da Estratégia Nacional de Cibersegurança**. 2022. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa) – Escola Superior de Guerra, Campus Brasília, DF, 2022. Disponível em: https://repositorio.esg.br/handle/123456789/1255. Acesso em: 08 jun. 2023.

MONTEIRO, Silvana Drumond. O Ciberespaço: o termo, a definição e o conceito. **DataGramaZero – Revista de Ciência da Informação**, [*S.l.*], v. 8, n. 3, Jun 2007.

MORESI, Eduardo Amadeu Dutra. Informação: uma arma cibernética? In: **Décima Segunda Conferencia Iberoamericana en Sistemas, Cibernética e Informática: CISCI 2013**, 2013,

Orlando - FL - USA. Anais da Décima Segunda Conferencia Iberoamericana en Sistemas, Cibernética e Informática: CISCI 2013. Orlando - FL: International Institute of Informatics and Systemics, 2013.

NINKOVIC, Vladimir M. Critical Infrastructure Resilience-National Approaches in the United States of America, the United Kingdom and Australia. **Zbornik Radova**, [*S.l.*], v. 55, p. 1205, 2021. Disponível em: https://zbornik.pf.uns.ac.rs/wp-content/uploads/2022/03/doi_10.5937_zrpfns55-30333.pdf. Acesso em: 3. ago. 2023.

NOLAN, Jhon A. Inteligência e Segurança nos Negócios *in* MILLER, JERRY P. *et al*. **O milênio da inteligência competitiva.** Tradução: Raul Rubenich. Porto Alegre: Bookman, 2002.

OLIVEIRA, Ângela Beatriz Cardoso de. **A Tecnologia 5g e possíveis impactos para a Segurança Nacional.** 2021. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa) – Escola Superior de Defesa, Brasília, DF, 2022. Disponível em: https://repositorio.esg.br/handle/123456789/1519. Acesso em: 08 jun. 2023.

PERIN VICHI, Leonardo; JACON AYRES PINTO, Danielle; NERY DE SÁ, André Luiz. **A Defesa da Infraestrutura de Cabos Submarinos: por uma interface entre a Defesa Cibernética e a Segurança Marítima no Brasil**. [*S.l.*], 2020. Disponível em: http://dx.doi.org/10.21544/1809-3191.v26n2.p326-346. Acesso em: 3 ago. 2023.

PINTO, Danielle Jacon Ayres; GRASSI, Jéssica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**, [*S.l.*], v. 7, n. 2, 2020. Disponível em: https://doi.org/10.26792/rbed.v7n2.2020.75178. Acesso em: 3 ago. 2023.

PURSIAINEN, Christer; KYTÖMAA, Eero. From European critical infrastructure protection to the resilience of European critical entities: what does it mean?. **Sustainable and Resilient Infrastructure**, [*S.l.*], v. 8, n. sup1, p. 85-101, 2023. Disponível em: https://doi.org/10.1080/23789689.2022.2128562. Acesso em: 3 ago. 2023.

SEGUNDO, Célio Borges Taquary. **A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos**. 2019. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa) – Escola Superior de Guerra, Campus Brasília, DF, 2022. Disponível em: https://repositorio.esg.br/handle/123456789/1205. Acesso em: 08 jun. 2023.

SILAULE, Carol B.; MAKHUBELE, Lean M.; MAMOROBELA, Stevens P. A model to reduce insider cybersecurity threats in a South African telecommunications company. **South African Journal of Information Management**, [*S.l.*], v. 24, n. 1, p. 1-8, 2022. Disponível em: https://doi.org/10.4102/ sajim.v24i1.1573. Acesso em: 3 ago. 2023.

SVINTSYTSKYI, Andrii V. The system of cybersecurity bodies in Ukraine. **Revista Científica General José María Córdova**, [*S.l.*], v. 20, n. 38, p. 287-305, 2022. Disponível em: https://dx.doi.org/10.21830/19006586.903. Acesso em: 3 ago. 2023.

TELEBRAS (Brasil). **Fato Relevante**, [*S.l.*], 2018. Disponível em: https://www.telebras.com.br/wp-content/uploads/2019/10/Fato-Relevante-12-09-2018-Cabo-Submarino.pdf. Acesso em: 3 ago. 2023.

TELEBRAS (Brasil). **50 anos da Telebras**, [*S.l.*], 2023a. Disponível em: https://www.telebras.com.br/50anos/. Acesso em: 08 jun. 2023.

TELEBRAS (Brasil). **Conheça o COPE,** [*S.l.*], 2023b. Disponível em: https://www.telebras.com.br/telebras-sat/conheca-o-cope/. Acesso em: 08 jun. 2023.

VIANNA, Eduardo Wallier; FERNANDES, Jorge Henrique Cabral. O gestor da segurança da informação no ciberespaço governamental: grandes desafios, novos perfis e procedimentos. **Brazilian Jounal of Information Science:** Research Trends. [*S.l.*], v. 9, n. 1. 2015.