ARTIGO DOI 10.52781/cmm.a196

Sistema CYBEROS e sua vertical de redes de rádios táticos: reflexões sobre as contribuições potenciais para a Defesa Nacional

CYBEROS system and its vertical of tactical radio networks: reflections on potential contributions to National Defense

Resumo: Documentos normativos que definem políticas e estratégias norteadoras da Defesa Nacional e de várias de suas ramificações apontam a importância do setor cibernético. O fortalecimento do setor passa por várias estratégias específicas, como a integração da academia com a base industrial de defesa, o desenvolvimento de tecnologias duais e a capacitação de recursos humanos especializados. Nesse escopo, destaca-se o sistema CYBEROS, uma ferramenta computacional inovadora que viabiliza exercícios de Segurança Cibernética, por meio da simulação realista de cenários de proteção de infraestruturas críticas, bem como de redes de rádios táticos. Este trabalho apresenta reflexões sobre as contribuições potenciais dessa ferramenta à Defesa Nacional, com ênfase no setor cibernético. Para tal, realizou-se uma pesquisa qualitativa, confrontando ações estratégicas previstas no arcabouço normativo atual com os principais resultados esperados desse desenvolvimento. Constata-se que o CYBEROS e sua vertical de redes de rádios táticos contribuem de forma objetiva para diversas dessas ações estratégicas.

Palavras-chave: Defesa cibernética; Comunicações táticas; Rádio definido por software; Defesa Nacional; Proteção de infraestruturas críticas.

Abstract: Normative documents that define policies and guiding strategies for Brazilian National Defense and its various branches highlight the importance of the cyber sector. Strengthening this sector involves several specific strategies, such as integrating academia with the defense industrial base, developing dual-use technologies, and training specialized human resources. In this context, the CYBEROS system stands out as an innovative computational tool that enables Cybersecurity exercises through the realistic simulation of critical infrastructure protection scenarios and tactical radio networks. This paper presents reflections on the potential contributions of this tool to National Defense, with an emphasis on the cyber sector. To this end, a qualitative study was conducted, comparing strategic actions outlined in the current normative framework with the main expected outcomes of this development. The findings indicate that CYBEROS and its vertical of tactical radio networks contribute directly to several of these strategic actions.

Keywords: Cyber defense; Tactical communications; Software-defined radio; National Defense; Critical infrastructure protection.

Maurício Henrique Costa Dias
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (CEFET/RJ)
Rio de Janeiro, RJ, Brasil
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
maurocio.dias@cefet-rj.br

George Alex Fernandes Gomes
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
george.gomes@ime.eb.br

Danilo Habermann
Exército Brasileiro (Cel Veterano)
Campinas, SP, Brasil
danilo.habermann@gmail.com

Paulo César Pellanda
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
pellanda@ime.eb.br

Juraci Ferreira Galdino
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
galdino@ime.eb.br

Recebido: 27 ago. 2025
Aprovado: 29 jul. 2026

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
https://colecaomeiramattos.com.br/CMM

Creative Commons Attribution Licence

1 INTRODUÇÃO

A Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END) são os documentos norteadores, de caráter ostensivo, de mais alto nível da Defesa Nacional (Brasil, 2024a). A PND apresenta os pressupostos básicos do Brasil em relação à sua defesa e estabelece os Objetivos Nacionais de Defesa (OND). Por sua vez, a END orienta todos os segmentos do Estado brasileiro quanto às medidas a serem implementadas para que se atinjam os objetivos, definindo Estratégias de Defesa (ED) e Ações Estratégicas de Defesa (AED).

Um destaque importante que se percebe nessa documentação orientativa é a necessidade de fortalecimento dos três setores tecnológicos estratégicos para a Defesa Nacional: nuclear; espacial; e cibernético (Brasil, 2024a). Há o cuidado, inclusive, em se atribuir a responsabilidade de cada um desses setores a uma Força Armada específica (Marinha, Aeronáutica e Exército, respectivamente), mesmo considerando a matricialidade desses setores entre as três Forças. Vale destacar que essa composição de setores tecnológicos estratégicos e as respectivas responsabilidades são as mesmas originalmente previstas na primeira edição da END (Brasil, 2008).

Desses três setores, aquele de menor tempo de maturidade tecnológica e provavelmente o que permeia de forma mais ampla todas as três Forças Armadas (FFAA) é o cibernético. O setor cibernético compreende o conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, programas e dados de ataques, danos ou acesso não autorizado. Esse setor é essencial para a segurança e a defesa nacionais, pois as ameaças cibernéticas podem comprometer infraestruturas críticas (IC), como sistemas de energia, comunicações e defesa. A defesa cibernética envolve a implementação de medidas preventivas e reativas para detectar, responder e neutralizar ameaças, garantindo a integridade, a confidencialidade e a disponibilidade das informações e dos sistemas estratégicos do país.

Aliás, a proteção de IC sob o ponto de vista cibernético é uma preocupação global do início do século XXI que vem demandando atenção crescente, como alertado em Pinheiro (2008), Sandoval (2020) e Souza, Oliveira e Paula (2024), e com impactos evidentes nas doutrinas militares contemporâneas. Desde então, foram desenvolvidas muitas discussões a respeito do setor cibernético, da proteção de IC e de outras ramificações correlatas no contexto da Defesa Nacional do Brasil e de outras nações. Exemplos recentes dessas contribuições podem ser encontrados em Medeiros, Carvalho e Goldoni (2019), Malagutti (2022), Castilho (2023), Okabayashi (2024) e Schwether (2025).

A importância e a dimensão do setor cibernético atualmente são de tal monta que os cuidados com esse setor não podem ficar restritos ao escopo de atuação do Ministério da Defesa. Nesse contexto mais amplo, destacam-se a Política Nacional de Cibersegurança (PNCiber) (Brasil, 2023) e a Estratégia Nacional de Segurança Cibernética (E-Ciber) (Brasil, 2025). Na mesma linha de raciocínio, a proteção a IC também ganhou projeção mais ampla e legislação normativa de alto nível própria, com a formulação da Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) (Brasil, 2018a) e da Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC) (Brasil, 2020b).

Nesse mister, cresce em importância o papel esperado da comunidade acadêmica nacional, seja na sua função primária de capacitação de recursos humanos, seja na condução de Pesquisa, Desenvolvimento e Inovação (PD&I), buscando a integração com o segmento produtivo público e privado, com ênfase nos estabelecimentos que compõem a Base Industrial de Defesa (BID). Como manifestado em todo esse arcabouço normativo, esse é um dos principais caminhos

na busca por inovações tecnológicas cibernéticas, preferencialmente de caráter dual, que ajudem o país a conquistar autonomia tecnológica e fortalecer sua posição no cenário geopolítico global atual e futuro (Barbosa; Caldeira, 2021; Moreira; Galdino, 2024).

Um exemplo de ambiente acadêmico que pode ajudar a cumprir o papel esperado de contribuição para o contexto em questão é o Laboratório de Segurança Cibernética de Sistemas Ciberfísicos (LaSC) do Instituto Militar de Engenharia (IME), comissionado no final de 2021 (Camargo *et al.*, 2022). O LaSC dispõe de uma infraestrutura que permite a simulação *hardware-in-the-loop* (HIL) em tempo real de sistemas ciberfísicos submetidos a ataques de *malware* reais, viabilizando estudos e pesquisas em Segurança Cibernética, como o sistema discutido em Vu *et al.* (2024), por exemplo.

Ao final de 2022, foi celebrado um projeto de desenvolvimento firmado entre a Financiadora de Estudos e Projetos (FINEP), a Fundação de Apoio à Pesquisa, Desenvolvimento e Inovação do Exército Brasileiro (FAPEB), o Centro Tecnológico do Exército (CTEx) e o IME, denominado "Inovações Tecnológicas para Segurança Cibernética de Sistemas Ciberfísicos Aplicadas a Infraestruturas Críticas e Comunicações Estratégicas e Táticas" (ITSC2ICCOM), visando melhorar as capacidades de estudos cibernéticos e ampliar o escopo de atuação do LaSC, incorporando novos casos de uso ou "verticais" representando IC dos setores elétrico, de óleo e gás, de comunicações etc. (FAPEB, 2022). Após um processo de escolha de parceria estratégica (FAPEB, 2025), em que o CPQD foi a instituição contratada, em 2025 foi iniciado o desenvolvimento mais significativo desse projeto, o sistema CYBEROS, um *Cyber Range* (Lillemets *et al.*, 2025) nacional customizado para incorporar a simulação realista de redes, sistemas e infraestruturas reais. O sistema viabiliza treinamentos e exercícios típicos de capacitação em Segurança Cibernética, trazendo de forma inovadora ambientes virtualizados de simulações realistas de cenários de proteção de IC e de redes de comunicações militares.

A vertical que ganhou maior atenção inicial foi a de redes de rádios táticos, compostas por rádios como os da família de Rádios Definidos por Software de Defesa (RDS-Defesa), cujo desenvolvimento tem envolvido diversos integrantes da BID há mais de uma década (Branco *et al.*, 2014; Redação Tecnologia & Defesa, 2024). Essa prioridade se justifica tendo em vista que o advento das doutrinas relativas à Segurança Cibernética agregou novas preocupações com a vulnerabilidade dessas redes, em acréscimo às já previstas pelas doutrinas militares de Comunicações e Guerra Eletrônica, como exemplificado pelo mapeamento de classes de ataques a RDS táticos discutido em Silva, Moura e Galdino (2012) e pela metodologia proposta em Kloth *et al.* (2024).

Do exposto, identificou-se o seguinte problema de pesquisa: como o CYBEROS, com suas verticais, em especial a de redes de rádios táticos, pode contribuir para a Defesa Nacional? Com essa questão em vista, este artigo tem por objetivo demonstrar que as contribuições potenciais desse desenvolvimento e o contexto no qual ele está inserido se alinham aos principais documentos de orientação das políticas e estratégias nacionais de defesa, com ênfase no setor cibernético. Para tal, realizou-se uma pesquisa qualitativa focada no arcabouço normativo de alto nível de suporte à Defesa Nacional, em busca de objetivos, estratégias e ações estratégicas com os quais o CYBEROS se alinha.

A seção 2 descreve de forma mais detalhada o LaSC e o Projeto ITSC2ICCOM, no qual o sistema CYBEROS e suas verticais se inserem. A metodologia adotada no trabalho é explicada na seção 3. A seção 4 discrimina o alinhamento do sistema como um todo com as principais políticas e estratégias da Defesa Nacional pertinentes. A seção 5 traz uma reflexão mais específica sobre as contribuições potenciais da vertical de redes de rádios táticos. Conclui-se o artigo na seção 6.

2 LASC E PROJETO ITSC2ICCOM

2.1 Histórico e antecedentes

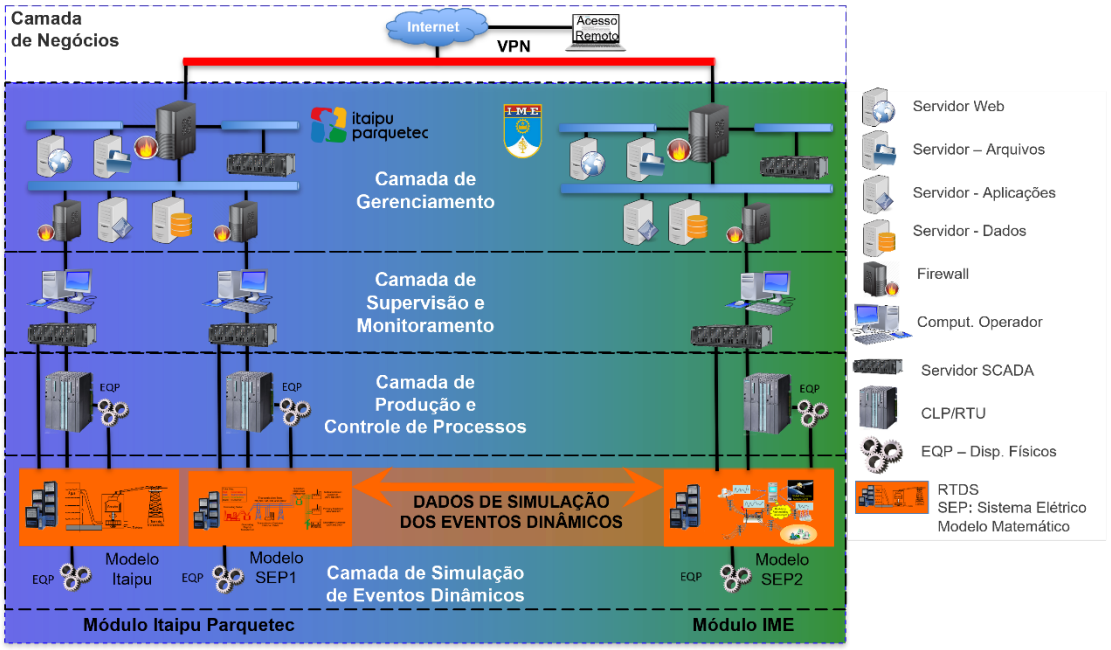
A economia e a sociedade dependem profundamente das tecnologias de informação e comunicação, o que torna o ciberespaço um domínio crítico que interfere nas esferas econômica, social e política dos Estados, exigindo a adaptação de doutrinas e estratégias de segurança. Essa dependência traz consigo uma série de vulnerabilidades e ameaças crescentes, como ataques de *phishing*, negação de serviço, vazamento de dados, espionagem e terrorismo cibernético. A disseminação indiscriminada de informações no ambiente online, inclusive de scripts para lançamento de ataques cibernéticos, possibilita que ataques cada vez mais sofisticados sejam conduzidos por usuários que não necessitam de elevado conhecimento técnico. Com isso, a confidencialidade, a integridade, a autenticidade e a disponibilidade das informações são constantemente ameaçadas. Nesse contexto, destaca-se a preocupação com ataques cibernéticos direcionados a IC, cuja interrupção ou destruição de serviços pode causar sérios impactos, comprometendo a segurança do Estado e da sociedade (Cravo, 2023; Fontes, 2024; Gomes; Laginestra, 2023; Melo; Albuquerque; Mendonça, 2022; Reis, 2024; Santos Junior *et al.*, 2019).

A criação do LaSC veio ao encontro dessa preocupação, viabilizando o apoio à realização de PD&I em Segurança Cibernética de IC do setor elétrico, por meio de simulações HIL em tempo real. As simulações envolvem modelos e dispositivos de redes elétricas (geração, transmissão e distribuição), de tecnologias da informação e comunicações, e de tecnologias de automação, todos integrados e representando fielmente o comportamento de sistemas reais, como ilustrado na Figura 1. Essas simulações da fase inicial do LaSC envolviam a aplicação de eventos cibernéticos reais, ataques de qualquer natureza, com foco na inserção de *malwares* reais e na contaminação cibernética de ambientes industriais, permitindo verificar os efeitos nas diferentes camadas, identificar vulnerabilidades e propor soluções.

Nesse relativamente curto período de existência, o LaSC vem acumulando expressiva capacidade científica, tecnológica e de inovação em Segurança Cibernética, com resultados importantes no apoio à formação de recursos humanos e à produção intelectual. Merece destaque inicial nesse contexto a criação, em 2022, do curso de Pós-Graduação em Proteção de Sistemas Elétricos (PGPSE) (IME, 2025). Ainda nessa linha, o LaSC também passou a contribuir com o desenvolvimento de pesquisas nos cursos de pós-graduação *stricto sensu* do IME.

Outro vetor de contribuição do LaSC tem sido o apoio à preparação e à composição de equipes militares brasileiras para participação em exercícios cibernéticos nacionais e internacionais. Destacam-se, inicialmente, o Cyber Flag de maio de 2024 (Barros, 2024) e o Cyber Shield de junho de 2025 (Barros, 2025), coordenados pelo United States Cyber Command e pelo United States Department of Defense, considerados os maiores exercícios de combate cibernético do mundo. Em ambas as ocasiões, um mês antes desses exercícios, uma equipe do LaSC ministrou treinamento cobrindo assuntos de Segurança Cibernética específicos sobre proteção de IC para os militares das três FFAA que compuseram os times brasileiros. O LaSC também contribuiu para o planejamento e participou do Exercício Guardião Cibernético (EGC) de 2024, e sua participação no EGC de 2025 também estava prevista. O EGC é o maior exercício de defesa cibernética do hemisfério sul, envolvendo setores públicos e privados relacionados à proteção de IC do Brasil, sendo organizado pelo Comando de Defesa Cibernética (ComDCiber) (Brasil, 2024b).

Figura 1 – LaSC: concepção lógica inicial de experimentos e simulações



Fonte: Integrantes do LaSC (2021).

Após o comissionamento do LaSC, os resultados preliminares apontavam para um potencial de contribuições em PD&I e na formação de recursos humanos muito mais amplo do que o escopo inicial, vinculado principalmente à proteção de IC do setor elétrico. Para viabilizar a expansão das atividades do laboratório e dar mais projeção a seus resultados, o IME buscou fomento com a FINEP, em parceria com o CTEx e a FAPEB, celebrando um convênio para o desenvolvimento do projeto ITSC2ICCOM (FAPEB, 2022). O objetivo do projeto é a obtenção de inovações tecnológicas para segurança cibernética de sistemas ciberfísicos aplicados à proteção de IC e às comunicações estratégicas e táticas. O desenvolvimento dessas inovações tem como foco a aplicação em sistemas de RDS e de comunicações voltadas ao emprego militar e civil, além de outros sistemas ciberfísicos.

2.2 Sistema CYBEROS

Após um período de amadurecimento a respeito de premissas, metodologia, objetivos e requisitos, foram estabelecidas as exigências para a contribuição mais significativa esperada do projeto ITSC2ICCOM: o sistema CYBEROS. Esse sistema é desenvolvido em parceria com o CPQD, instituição vencedora do edital lançado no início de 2025 (FAPEB, 2025).

O CYBEROS faz a orquestração automatizada de cenários de cibersegurança, viabilizando treinamentos e exercícios típicos desse contexto, como o consagrado modelo Capture the Flag (CTF) (Švábenský *et al.*, 2021), em ambientes virtualizados de simulações realistas. Uma inovação presente nessa concepção é a integração de módulos complementares ao que seria o núcleo típico de um Cyber Range, que permitem a operação das verticais dos cenários específicos de proteção de IC. Tal solução tem o

potencial de preencher lacunas identificadas pelo LaSC, considerando a crescente sofisticação e frequência dos ataques direcionados a setores estratégicos. Plataformas como a Hack The Box[1] e o TryHackMe[2] não são totalmente customizadas para aspectos específicos de cenários de proteção de IC nem permitem plena personalização de cenários, o que posiciona o CYBEROS como uma solução inovadora e estratégica.

A arquitetura conceitual inicial do CYBEROS é ilustrada na Figura 2. Ela é modular, escalável e compatível com o ambiente existente no LaSC, incluindo o uso de ferramentas similares ao OpenStack (Adiwal; Misbahuddin, 2023) como pilares para a virtualização e a orquestração. Ela se baseia em três módulos principais: *Frontend*, Orquestrador e *Backend*. O *Frontend* é a interface gráfica acessível aos usuários, projetada para facilitar a interação com o sistema, permitindo a configuração de cenários e topologias cibernéticas, o acompanhamento em tempo real do progresso dos exercícios e a visualização de métricas de desempenho.

O núcleo do CYBEROS é o orquestrador responsável por automatizar a criação, a configuração e a execução dos cenários simulados. Ele opera sobre uma plataforma de computação em nuvem equivalente ao OpenStack, com funcionalidades que incluem: gerenciamento de máquinas virtuais e contêineres (Tang, 2025); configuração automatizada de redes e dispositivos simulados; suporte à integração com dispositivos físicos, inclusive no formato HIL; e monitoramento contínuo do estado dos cenários e da alocação de recursos. Por sua vez, o *Backend* processa as solicitações dos usuários e as integra ao sistema. Entre as funcionalidades ofertadas estão: gestão de usuários e permissões; registro de *logs* e relatórios das atividades realizadas no sistema; e integração com bancos de dados para armazenamento seguro e eficiente.

A virtualização é uma forma de encapsular e isolar os desafios cibernéticos, garantindo um ambiente consistente e seguro para os participantes de exercícios cibernéticos. O orquestrador é essencialmente o sistema operacional da nuvem que gerencia e orquestra máquinas virtuais e/ou contêineres, bem como a infraestrutura de rede e armazenamento associada em larga escala. Essa estratégia permeia a infraestrutura de exercícios de maior escala e complexidade como os CTF modernos, permitindo a criação, o gerenciamento e o isolamento dos ambientes em que os desafios cibernéticos são hospedados.

Um requisito importante do sistema é a busca pela adoção de ferramentas *open-source* completas, sem modificá-las (Feller *et al.*, 2005). Eventuais modificações devem ser feitas por API (Bagga, 2023). Além disso, o sistema deve ser compatível com ferramentas de gerenciamento de informações e eventos de segurança (Conti *et al.*, 2018) e com ferramentas de monitoramento contínuo ou análise dinâmica de *malware* (Or-Meir *et al.*, 2019), para exploração e visualização dos dados e para rastrear a saúde dos servidores e identificar comportamentos anômalos.

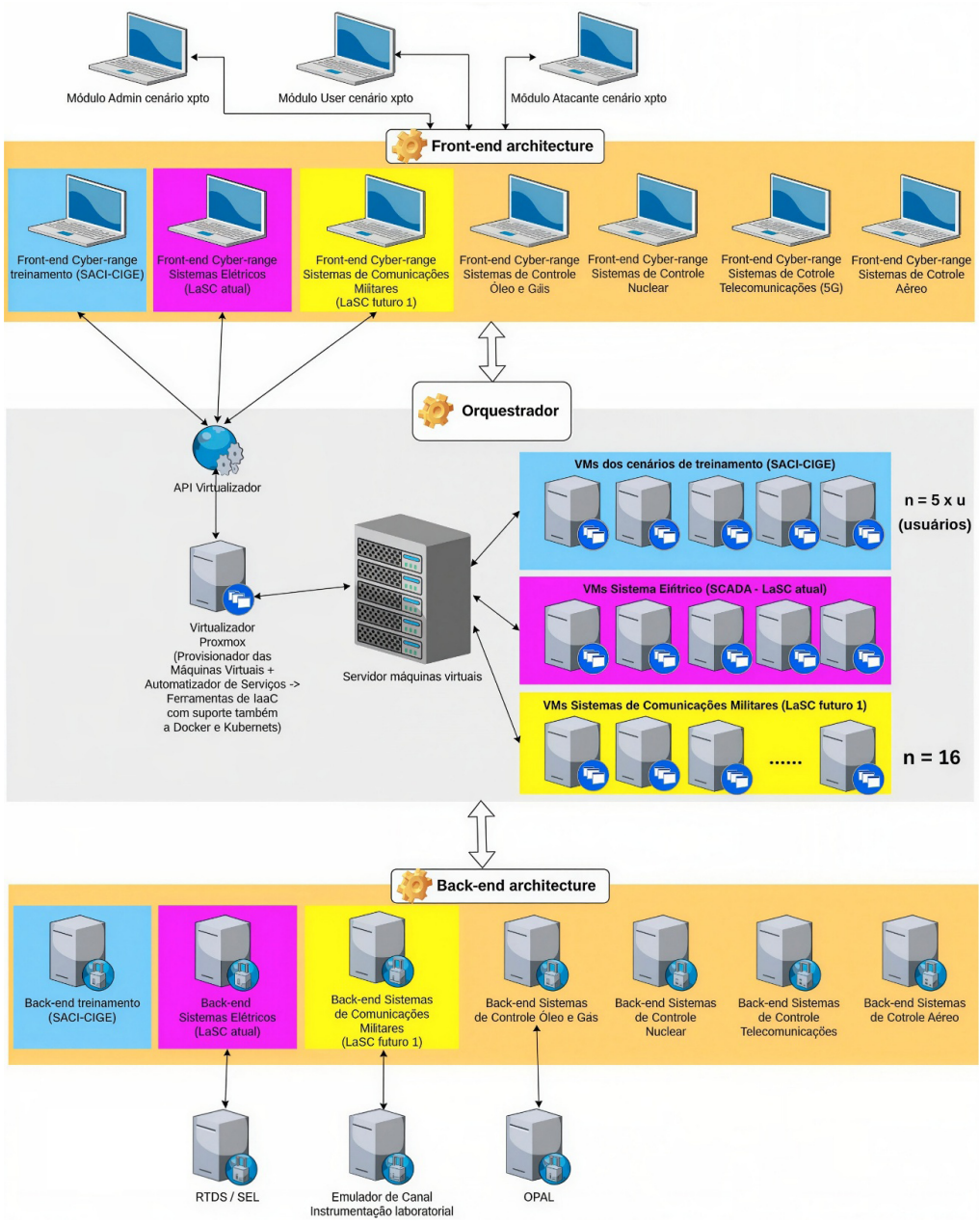
A Figura 2 ajuda a compreender o conceito das verticais integradas ao CYBEROS. Uma vertical não é exatamente um módulo em si, mas apenas representa a execução de um caso de uso ou cenário específico de simulação de exercício de segurança cibernética com suas peculiaridades. É uma máscara que representa a visão e as necessidades particulares de um perfil de usuário específico dos diferentes cenários de proteção de IC. Por exemplo, os elementos destacados na cor magenta na Figura 2 representam o uso do CYBEROS complementado por módulos integrados

1 Disponível em: https://www.hackthebox.com/. Acesso em: 12 ago. 2025.

2 Disponível em: https://tryhackme.com/. Acesso em: 12 ago. 2025.

específicos de apoio a exercícios de cibersegurança em um cenário do setor elétrico, caracterizando a vertical do setor elétrico.

Figura 2 – Concepção inicial de arquitetura do CYBEROS



Fonte: Integrantes do LaSC (2024).

Ao integrar recursos para permitir a execução de exercícios cibernéticos em um cenário realista de proteção de IC em uma vertical qualquer, a própria disponibilização desse cenário virtualizado e com integração a elementos HIL traz consigo uma outra aplicação para a ferramenta, que é a exploração de aspectos de desempenho e a simulação de uso do próprio sistema daquela

vertical. O aproveitamento efetivo desse potencial passa pela inserção de módulos complementares adicionais, integrados ao CYBEROS, cujas especificidades variam conforme a vertical. Em especial, o desenvolvimento dessa versão inicial do CYBEROS previu a viabilização da exploração desse modo de análise de desempenho para a vertical de sistemas de comunicações militares, ou mais especificamente, para redes de rádios táticos, compostas principalmente por RDS. Esse modo de uso da vertical representa uma alternativa para a realização de treinamentos ou exercícios operativos em ambiente fechado e controlado, que pode ser útil no apoio à capacitação e ao adestramento da tropa, bem como na geração de novos conhecimentos de interesse da doutrina.

2.3 Vertical de redes de rádios táticos

Os sistemas de comunicação táticos militares também estão expostos a ataques cibernéticos e, como tal, também precisam de proteção robusta (Al-Shara; Ahmad, 2018; Heinäaro, 2015; Reis, 2024; Sneps-Sneppe, 2024). O espectro eletromagnético se tornou um campo de batalha altamente contestado, no qual as exigências operacionais demandam infraestruturas de comunicações táticas especializadas, capazes de assegurar conectividade contínua e troca segura de informações mesmo sob condições adversas (Kloth *et al.*, 2024; Thomas; Fiala, 2020). Os RDS, componentes presentes de forma ostensiva nas redes de rádios táticos do século atual (Bergstrom *et al.*, 2002), embora ofereçam notável flexibilidade funcional, também ampliam significativamente a superfície de ataque cibernético devido à sua dependência de componentes lógicos e camadas de software. As vulnerabilidades dos RDS incluem, ainda, riscos associados à cadeia de suprimentos de hardware e de software, na sua maioria estrangeiros, à dependência de atualizações remotas e à utilização de bibliotecas de código aberto potencialmente comprometidas (Baldini *et al.*, 2012; Li *et al.*, 2018; Silva; Moura; Galdino, 2012, 2014).

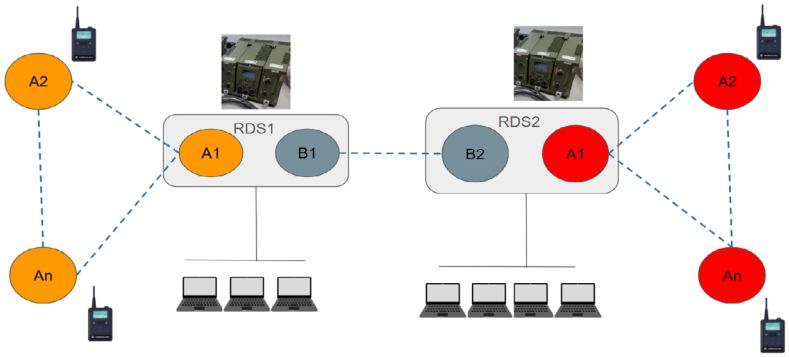
A vertical de redes de rádios táticos integra o CYBEROS como um módulo compatível com a família RDS-Defesa. Por uma questão estratégica, essa integração foi iniciada pela plataforma veicular, para comunicação tática em veículos e embarcações militares, e posteriormente será estendida aos demais tipos de rádio, à medida que forem disponibilizados (FAPEB, 2025). O RDS-Defesa veicular apresenta o Módulo de Radiofrequência (MRF), proprietário e aderente à especificação Transceiver Facility, da versão SCA 2.2.2, e o Módulo de Processamento (MP), que implementa uma arquitetura em núcleos de processamento Vermelho e Preto, separados fisicamente e interconectados por meio de um Módulo de Segurança (MSEG) (Branco *et al.*, 2014). Com esses módulos, oferece estrutura para a execução de diversas formas de onda, cada uma empregando protocolos de comunicação adequados a diversos cenários operativos (FAPEB, 2022).

A Figura 3 apresenta um caso de uso representativo da vertical em questão. As redes de rádio laranja e vermelha podem, por exemplo, atender a dois batalhões, respectivamente, afastados fisicamente entre si. As duas redes são interconectadas por RDS veiculares, os quais podem rodar simultaneamente duas formas de onda independentes, sendo úteis, portanto, para integrar redes diferentes.

A rede de rádio exemplificada na Figura 3, bem como outras topologias de comunicação, pode ser integralmente configurada no CYBEROS. Nessa estrutura, os MP – instâncias virtualizadas em servidores – executam as formas de onda em processadores emulados por máquinas virtuais. Apesar da virtualização do processamento, a transmissão e a recepção de sinais em radiofrequência

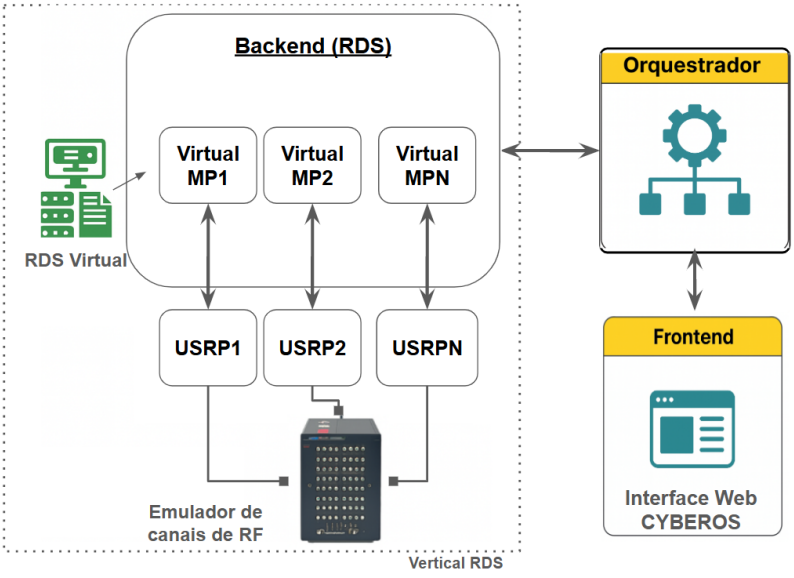
são realizadas por rádios físicos comerciais, como dispositivos USRP[3] ou similares. Esses equipamentos oferecem alta flexibilidade de operação, com ampla cobertura de frequências e larguras de banda, sendo adequados tanto para aplicações civis (como redes 4G, 5G e 6G) quanto para cenários táticos. Essa arquitetura, identificável genericamente como uma das verticais na Figura 2 (sistemas de comunicações militares – blocos na cor amarela), é detalhada na Figura 4, que aponta o uso de USRP e do emulador de canais de radiofrequência. O emulador de canais é capaz de aplicar degradações controladas aos sinais entre os diferentes nós da rede, como atenuação, desvanecimento e ruído. Com isso, é possível realizar testes de desempenho, interoperabilidade e resiliência das formas de onda em condições equivalentes às do campo, mas dentro de um ambiente de laboratório controlado.

Figura 3 – Exemplo de caso de uso de rede de rádios táticos usando RDS



Fonte: Os autores (2025).

Figura 4 – Vertical de redes de rádios táticos baseada em RDS virtualizados do CYBEROS



Fonte: Os autores (2025).

3 Disponível em: https://www.ni.com/en/support/downloads/drivers/download.ni-usrp.html. Acesso em: 12 ago. 2025.

3 METODOLOGIA

Para buscar uma contribuição ao problema de pesquisa formulado neste trabalho, adotou-se como metodologia uma pesquisa qualitativa. De modo geral, a pesquisa qualitativa visa entender fenômenos em profundidade, explorando aspectos subjetivos e contextuais, e se vale de métodos como entrevistas, grupos focais e análise de conteúdo (Lakatos; Marconi, 2017). Para este artigo, adotou-se a análise de conteúdo de documentos normativos de alto nível voltados ao planejamento da Defesa Nacional e de outras referências bibliográficas pertinentes à temática escolhida, em busca de correlações que evidenciassem de que formas uma ferramenta de inovação tecnológica como o CYBEROS, e em particular operando sua vertical de redes de rádios táticos, poderia contribuir objetivamente para a Defesa Nacional.

Sobre o escopo dos documentos normativos pesquisados, a análise se limitou a três grupos, tendo em vista o contexto tecnológico específico da inovação tecnológica em questão (setor cibernético). Com isso, foram analisadas inicialmente a PND e a END como documentos normativos de mais alto nível. Para cobrir o escopo mais específico do setor cibernético, foram consideradas a PNCiber e a E-Ciber. Por sua vez, o contexto de proteção de IC foi avaliado sob a luz da PNSIC e da ENSIC. Essa análise com foco no alinhamento normativo político e estratégico é apresentada na seção 4, apontando objetivos, estratégias e ações estratégicas que notadamente são atendidos pelo CYBEROS como um todo, e/ou considerando alguma de suas verticais.

A seção 5 foca o potencial de contribuição da vertical de redes de rádios táticos. As reflexões a esse respeito buscaram complementar os alinhamentos aos documentos normativos de alto nível identificados para o CYBEROS como um todo, apontando também contribuições de caráter tático ou operativo.

4 ALINHAMENTO COM AS PRINCIPAIS POLÍTICAS E ESTRATÉGIAS LIGADAS À DEFESA NACIONAL

4.1 PND/END

A PND é o documento condicionante de mais alto nível para o planejamento de ações destinadas à defesa do país. Voltada prioritariamente para ameaças externas, estabelece oito OND para o preparo e emprego de todas as expressões do Poder Nacional, em prol da Defesa Nacional. Por sua vez, a END define estratégias e ações estratégicas que deverão nortear a sociedade brasileira nas ações de defesa da pátria. Na versão atual, foram previstas 17 ED e 85 AED. Há ED que se repetem para diferentes OND, assim como há AED que se repetem para diferentes ED (Brasil, 2024a).

Na descrição da concepção estratégica de defesa, há um destaque importante na END que se relaciona diretamente com este trabalho, apontando que os setores governamental e industrial e o meio acadêmico, voltados para a ciência, tecnologia e inovação (CT&I), devem ser priorizados e integrados de modo a contribuir para assegurar que o atendimento às necessidades de produtos de defesa (PRODE) seja apoiado em tecnologias críticas sob domínio nacional. A END indica, ainda, que tais tecnologias devem ser obtidas mediante estímulo e fomento ao setor industrial e ao meio acadêmico, de forma sinérgica. Indica, também, que a capacitação da BID, incluído o domínio de tecnologias de uso dual, é fundamental para alcançar o abastecimento de PRODE, visando à autonomia

tecnológica do país. Percebe-se, portanto, que o desenvolvimento do CYBEROS se enquadra em todas essas premissas por trás da concepção da END, haja vista a participação do IME, do CTEx e do CPQD (uma Empresa Estratégica de Defesa – EED), assim como a natureza dual do sistema.

Entre os fundamentos da END destacam-se as Capacidades Nacionais de Defesa (CND), consideradas aquelas compostas por diferentes parcelas das expressões do Poder Nacional. A atual END se baseia em nove CND: Proteção; Pronta-resposta; Dissuasão; Coordenação e Controle; Gestão da Informação; Logística; Mobilidade Estratégica; Mobilização; e Desenvolvimento Tecnológico de Defesa. Dessas, duas, em particular, se conectam com o sistema CYBEROS e suas verticais: Proteção e Desenvolvimento Tecnológico de Defesa.

A CND de Proteção exprime o mais relevante OND, o de garantir a soberania, o patrimônio nacional e a integridade territorial. Reforçar essa CND requer a adequação e a estruturação dos sistemas de vigilância nas áreas de interesse e de controle, entre as quais o espaço cibernético se inclui. O sistema CYBEROS tem o potencial de contribuir indiretamente com essa CND, sob o ponto de vista da proteção e do monitoramento do espaço cibernético, ajudando a capacitar pessoal especializado, e viabilizando estudos e pesquisas sobre vulnerabilidades cibernéticas de IC, que podem nortear *stakeholders* em processos decisórios que busquem a adequação e a estruturação de sistemas de vigilância desse espaço estratégico.

Por sua vez, a CND de Desenvolvimento Tecnológico de Defesa proporciona o desenvolvimento e/ou a modernização de PRODE, por intermédio de ações integradas empreendidas pelo Estado, pela indústria e pelo meio acadêmico, de forma sinérgica, buscando a atualização e a independência tecnológica. Por sua natureza, o CYBEROS se enquadra nesse contexto, contribuindo diretamente para essa CND, portanto.

Os fundamentos da END tratam também do Setor de Defesa, discriminando o papel das três FFAA, assim como dos três setores tecnológicos estratégicos. A preocupação com o setor cibernético é manifestada explicitamente para as três FFAA, com ênfase no Exército, que tem um papel de liderança centralizada a esse respeito. Sobre o setor cibernético especificamente, a END manifesta que as capacitações devem incluir, como parte prioritária, as tecnologias de comunicações entre as unidades das FFAA, de modo a assegurar sua interoperabilidade e a capacidade de atuar de forma integrada, com segurança. Isso visa aprimorar a Segurança da Informação e das Comunicações e a Segurança Cibernética, em todas as instâncias do Estado, com ênfase na proteção de IC. Para tal, é necessário fomentar a PD&I com foco em tecnologias duais que permitam o planejamento e a execução das atividades cibernéticas no âmbito do Setor de Defesa e que contribuam com a Segurança Cibernética no âmbito nacional, envolvendo a comunidade acadêmica. Ainda, é recomendável que se fortaleça a atuação colaborativa entre o Setor de Defesa e a comunidade acadêmica nacional, os setores público e privado e a BID. O CYBEROS se encaixa nesses aspectos fundamentais que embasam a END.

O Quadro 1 apresenta a lista de OND, ED e AED para os quais o CYBEROS apresenta contribuições diretas ou indiretas. A justificativa desse alinhamento pode ser tomada analisando a relação com as AED, já que o atendimento a uma AED leva ao atendimento de uma ED e, por consequência, ao atendimento de um OND. Começando pela AED 1, o CYBEROS certamente se caracteriza como um desenvolvimento estratégico de Defesa do setor cibernético. Sobre a AED 2, o papel diferenciado das verticais de proteção de IC e de redes de rádios táticos que o CYBEROS

viabiliza contribui para a capacitação de pessoal especializado e para a disponibilização de ferramental de simulação realista de cenários de ataques cibernéticos, configurando um ganho indireto para incrementar o nível de segurança das IC. Essa mesma linha de raciocínio se aplica à AED 10, ainda que de forma limitada, pois o CYBEROS pode ajudar a desenvolver as capacidades de monitorar e controlar especificamente o espaço cibernético. A contribuição para a AED 11 também pode se valer desses argumentos, em especial quanto à capacidade de exploração do espaço cibernético. Por fim, a contribuição para a AED 52 é evidente e dispensa justificativas adicionais.

Quadro 1 – Alinhamento do CYBEROS à PND e à END

OND	ED	AED
I – Garantir a soberania, o patrimônio nacional e a integridade territorial	1 – Fortalecimento do Poder Nacional	1 – Desenvolver os setores estratégicos de defesa (nuclear, cibernético e espacial) 2 – Contribuir para o incremento do nível de segurança das IC de sistemas de captação, tratamento e distribuição de água; geração e distribuição de energia elétrica; transporte; produção e distribuição de combustíveis; e comunicações, entre outros
	2 – Fortalecimento da capacidade de dissuasão	10 – Desenvolver as capacidades de monitorar e controlar o espaço aéreo, o espaço cibernético, o território, as águas jurisdicionais brasileiras e outras áreas de interesse 11 – Incrementar as capacidades de defender e de explorar o espaço cibernético
III – Promover a autonomia tecnológica e produtiva na área de Defesa	9 – Fortalecimento da área de Ciência e Tecnologia de Defesa	52 – Promover o desenvolvimento da tecnologia cibernética
VIII – Incrementar a projeção do Brasil no concerto das nações e sua inserção em processos decisórios internacionais	1 – Fortalecimento do Poder Nacional	1 – Desenvolver os setores estratégicos de defesa (nuclear, cibernético e espacial) 2 – Contribuir para o incremento do nível de segurança das IC de sistemas de captação, tratamento e distribuição de água; geração e distribuição de energia elétrica; transporte; produção e distribuição de combustíveis; e comunicações, entre outros

Fonte: Os autores (2025).

4.2 PNCiber e E-Ciber

Em 2018, por meio do Decreto nº 9.637, foi publicada a Política Nacional de Segurança da Informação (PNSI) (Brasil, 2018b), que estabelecia objetivos e meios para alcançá-los a respeito de Segurança Cibernética, Defesa Cibernética, segurança física e proteção de dados organizacionais. A PNSI previa sua consecução por intermédio da Estratégia Nacional de Segurança da Informação (ENSI) e por planos nacionais. Por sua vez, previa-se que a ENSI seria construída em cinco módulos, contendo as ações estratégicas e os objetivos relacionados à Segurança da Informação, em consonância com as políticas públicas e os programas do governo federal. Os módulos da ENSI deveriam versar sobre: Segurança Cibernética; Defesa Cibernética; segurança das IC; segurança da informação sigilosa; e proteção contra vazamento de dados.

O módulo de Segurança Cibernética foi desenvolvido e publicado em 2020 como a Estratégia Nacional de Segurança Cibernética (E-Ciber) (Brasil, 2020a). Essa E-Ciber foi a orientação

manifesta do governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área de Segurança Cibernética, para o quadriênio 2020-2023.

A ENSI não se concretizou da forma originalmente planejada em 2018. Em especial, a E-Ciber saiu da alçada da PNSI e passou a estar vinculada à Política Nacional de Cibersegurança (PNCiber), estabelecida em 2023, junto com o Comitê Nacional de Cibersegurança (CNCiber), por meio do Decreto nº 11.856 (Brasil, 2023). O CNCiber é um colegiado vinculado ao Gabinete de Segurança Institucional da Presidência da República (GSI-PR). O Decreto nº 11.856 previu que a E-Ciber deveria ser atualizada nos anos seguintes, prorrogando a validade da versão anterior até sua substituição. A nova E-Ciber foi publicada em agosto de 2025 (Brasil, 2025).

A PNCiber estabelece onze objetivos em seu art. 3º, dos quais, quatro são atingidos pelo CYBEROS, em maior ou menor grau, conforme o caso. São eles: I) promover o desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética; VII) desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade; VIII) fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética; e IX) incrementar a atuação coordenada e o intercâmbio de informações de segurança cibernética entre a União, os Estados, o Distrito Federal e os Municípios, os Poderes Executivo, Legislativo e Judiciário, o setor privado e a sociedade em geral.

Os objetivos da PNCiber devem ser alcançados por meio da E-Ciber, que é estruturada em quatro eixos temáticos: I) proteção e conscientização do cidadão e da sociedade; II) segurança e resiliência dos serviços essenciais e das IC; III) cooperação e integração entre os órgãos e entidades, públicas e privadas; e IV) soberania nacional e governança. Esses eixos temáticos devem ser implementados por meio de ações estratégicas específicas, previstas no Plano Nacional de Cibersegurança, que ainda será desenvolvido. Nesse sentido, a E-Ciber atual se diferencia estruturalmente da anterior, de 2020, substituindo os antigos objetivos estratégicos por eixos temáticos e deixando o mapeamento definitivo das ações estratégicas para o Plano Nacional. De todo modo, a E-Ciber atual já apresenta, para cada eixo, uma lista de ações mínimas correspondentes.

Com relação às quatorze ações relacionadas ao eixo temático I, quatro se relacionam em maior ou menor grau com o CYBEROS: IV – incentivo à capacitação de professores e gestores, públicos e privados, em cibersegurança; V – incentivo à inclusão de temas relacionados à cibersegurança nos currículos de todos os níveis educacionais; VI – incentivo à participação em fóruns e atividades acadêmicas, técnicas e profissionais relacionadas à cibersegurança; e IX – incentivo ao desenvolvimento de planos de contingência institucionais e à realização de testes e simulações para verificação do nível de cibersegurança no órgão ou na entidade. O contexto de desenvolvimento do CYBEROS no IME, uma instituição de ensino superior, e sua inserção no LaSC, conforme discussão da seção 2, justificam o alinhamento às ações IV, V e VI. A ação IX é parcialmente atendida quanto à questão dos testes e simulações, haja vista que o CYBEROS e suas verticais se propõem a servir como ferramenta para a simulação de cenários diversos de segurança cibernética, com ênfase na proteção de IC.

O eixo temático II, que se refere a serviços essenciais e às IC, especifica um mínimo de onze ações necessárias à sua consecução. Curiosamente, apesar do destaque do CYBEROS quanto aos cenários de proteção de IC, apenas uma ação pode ser destacada como diretamente relacionada: VIII – incentivo à realização de exercícios e simulações setoriais e multissetoriais regulares destinados ao aprimoramento da resiliência dos serviços essenciais e das IC. O CYBEROS é uma ferramenta que estará

à disposição não só do IME, mas de toda a comunidade acadêmica e do setor produtivo, podendo ser utilizada em exercícios e simulações de interesse das instituições responsáveis pelas IC nacionais.

Também o eixo temático III apresenta uma única ação, entre as cinco listadas, para a qual o CYBEROS e o contexto em que se enquadra representam uma contribuição. A ação I desse eixo é o estímulo à criação e ao desenvolvimento de equipes de prevenção e resposta a incidentes de cibersegurança, centros de análise e compartilhamento de informações e laboratórios especializados em cibersegurança. O LaSC, laboratório no qual o CYBEROS é desenvolvido e hospedado, certamente se enquadra como laboratório especializado em cibersegurança e, como tal, apresenta potencial para o desenvolvimento de equipes voltadas para lidar com incidentes cibernéticos.

Por fim, o eixo IV lista dez ações mínimas para atender e proteger os interesses da sociedade brasileira no ciberespaço e garantir um ambiente cibernético confiável que assegure o crescimento econômico e tecnológico do país. Metade dessas ações se alinham ao potencial do CYBEROS. Duas dessas ações mais uma vez se alinham pelo contexto acadêmico no qual o CYBEROS se enquadra: III – formação e capacitação técnico-profissional em cibersegurança em escala compatível com as necessidades nacionais; e IX – incentivo à criação de linhas de pesquisa para graduação e pós-graduação *stricto sensu* e à concessão de bolsas de estudo para a formação de especialistas e de professores brasileiros em cibersegurança. Outras duas ações remetem ao potencial inovador da ferramenta, à participação de uma EED no seu desenvolvimento e ao fomento por recursos públicos obtido, principalmente via FINEP: IV – redução do débito tecnológico do país em tecnologias emergentes e disruptivas por meio de ações governamentais afirmativas e incrementais; e X – incentivo ao desenvolvimento de produtos, serviços e tecnologias nacionais destinados ao aprimoramento da cibersegurança no país. Há ainda o potencial do CYBEROS para contribuir com a ação V – incentivo ao desenvolvimento de capacidade de avaliação continuada de conformidade em segurança de produtos, serviços e tecnologias de cibersegurança, capacidade essa discutida especificamente para a vertical de redes de rádios táticos na seção 5.

4.3 PNSIC/ENSIC

A atenção do Estado brasileiro com a segurança de IC ganhou força no final da primeira década de 2000, o que é evidenciado pela inclusão dessa preocupação na primeira versão da END, em 2008. As discussões que se sucederam desde então levaram à aprovação da PNSIC (Brasil, 2018a), e posteriormente à publicação do Decreto nº 9.819, em 2019, que inseriu a proteção de IC no rol de competências da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo.

A PNSIC define IC como instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou na segurança do Estado e da sociedade. Também caracteriza a segurança das IC como um conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às IC. Ela traz, ainda, orientações para o esforço conjunto a ser desenvolvido pelos órgãos e entidades dos setores público e privado a esse respeito.

No Decreto que traz a PNSIC foi definida a necessidade de se estabelecer a ENSIC como um dos instrumentos para a implementação dessa política. A ENSIC, publicada em 2020 (Brasil, 2020b), consolida os conceitos e identifica os principais desafios para a atividade de segurança de IC. Nela, foram estabelecidos quatro eixos estruturantes (EE), que constituem os principais

pilares para a efetividade da atividade de segurança de IC. Os eixos organizam os desafios de modo a criar uma estratégia organicamente coerente e coesa, que deve impulsionar o funcionamento da atividade de segurança de IC. Para cada EE, a ENSIC estabelece alguns objetivos estratégicos (OE), que foram dispostos sem ordem de prioridade, retratando o foco estratégico para direcionar os esforços na implementação da PNSIC, além de sinalizar os resultados a serem alcançados. Houve ainda o desdobramento dos OE em várias iniciativas estratégicas (IE), que fornecem a direção para o emprego efetivo desses esforços.

O CYBEROS contribui com dois EE da ENSIC. O primeiro alinhamento se dá com o EE 2 – Conscientização e capacitação, em seu OE 2.2 – Fomentar a capacitação e a educação em segurança de IC, e, mais especificamente, por meio da IE 2.2.1 – Fomentar as ações de capacitação existentes em defesa e segurança de IC. A criação do LaSC se deu justamente no contexto das preocupações estatais com a segurança de IC, e o desenvolvimento do CYBEROS, em especial considerando sua customização para esse cenário, reforça o alinhamento em questão.

A outra contribuição à ENSIC se dá em relação ao EE 4 – Gestão de dados e informações, em seu OE 4.3 – Incentivar a adoção de recursos e de procedimentos voltados para a Segurança Cibernética nas IC, e por meio da IE 4.3.2 – Orientar as IC a observarem a E-Ciber, principalmente o disposto em seu item 2.3.5 – Elevar o nível de proteção das IC nacionais. A contribuição do CYBEROS para esse trio EE/OE/IE é evidente, tendo em vista que o sistema se constitui em ferramenta de apoio a estudos e treinamentos cibernéticos realistas que apoiam a construção de conhecimento especializado para a confecção de procedimentos e planos de ação específicos a serem adotados pelas instituições e pelo pessoal envolvido com a segurança de IC.

5 CONTRIBUIÇÕES DA VERTICAL DE REDES DE RÁDIOS TÁTICOS

Uma das principais inovações do CYBEROS reside na sua vertical de redes de rádios táticos. Essa vertical incorpora um emulador de canal de radiofrequência capaz de aplicar degradações controladas ao sinal, simulando ambientes de campo complexos dentro de um laboratório controlado, para realizar testes automatizados com módulos físicos ou virtualizados de RDS. Com isso, a vertical proporciona simulações realistas, executando testes de desempenho, interoperabilidade e resiliência em condições equivalentes às de operações reais, civis ou militares. Permite, ainda, a análise abrangente de vulnerabilidades, mapeando de forma estruturada ameaças críticas às redes baseadas em RDS. Contribui para a padronização e a certificação, haja vista que os resultados dos ensaios auxiliam no desenvolvimento e no emprego de base normativa para a Segurança Cibernética. Amplia o rol de modelos para experimentos, pelo uso de cenários híbridos que combinam ataques no espectro eletromagnético e ameaças cibernéticas. Por fim, propicia subsídio técnico para atendimento oportuno de demandas de segurança e de desempenho, ajudando a preservar a superioridade informacional e a capacidade de Comando e Controle em cenários altamente contestados.

A vertical de redes de rádios táticos agiliza a identificação de novas ameaças e a realização de testes de contramedidas para sistemas que suportam IC, implementando funcionalidades para simular e analisar vulnerabilidades. Isso é vital para o aprimoramento dos dispositivos de segurança e a adoção de outros procedimentos de proteção, uma vez que as ameaças cibernéticas evoluem em

ritmo acelerado. Além disso, a automação de tarefas otimiza esforços, reduzindo custos e o tempo de resposta a incidentes. Como grande parte das IC é operada por empresas privadas, a vertical de redes de rádios táticos também pode proporcionar a colaboração e o compartilhamento de informações padronizadas entre os setores público e privado, promovendo, assim, uma governança mais integrada e eficaz da cibersegurança (Cravo, 2023; Gomes; Laginestra, 2023; Reis, 2024).

A experimentação ágil e automatizada proporcionada pela vertical em questão acelera a PD&I de novas capacidades de Comunicações e Guerra Eletrônica, mantendo o Brasil à frente de potenciais adversários. Um país com capacidades cibernéticas avançadas e uma estratégia de defesa robusta ganha respeito e destaque no cenário internacional, fortalecendo sua posição diplomática e de cooperação (Cravo, 2023).

Como já destacado na subseção 4.1, o CYBEROS e suas verticais contribuem para o desenvolvimento da capacitação cibernética nos campos industrial e militar. Mais especificamente quanto à vertical de redes de rádios, ela proporciona a identificação proativa e a mitigação de vulnerabilidades em software e protocolos, atividades fundamentais para aprimorar a segurança de redes e sistemas. A simulação tanto de ataques no espectro eletromagnético quanto de ameaças cibernéticas pode ser realizada para identificar vulnerabilidades antes que se tornem incidentes reais, minimizando perdas e prejuízos que poderiam ser catastróficos. Isso inclui ataques de negação de serviço, que são uma das maiores ameaças que o Brasil enfrenta, simulando o bloqueio de transmissores de radiofrequência ou a interrupção de serviços essenciais. Por meio dessa vertical de redes de rádios, é possível executar testes de formas de onda em RDS virtualizados e físicos, o que permite às FFAA e ao setor produtivo avaliar a efetividade e a segurança de novas tecnologias de comunicação antes de sua implementação. Isso acelera o desenvolvimento de soluções nacionais e ajuda a reduzir a dependência tecnológica externa. O emprego dessa vertical também é capaz de ampliar a frequência e o realismo de exercícios como o EGC, possibilitando testar a resiliência dos sistemas táticos de comunicação de forma contínua e eficiente (Cravo, 2023; Gomes; Laginestra, 2023).

Com a facilitação de simulações de cenários complexos e de práticas de respostas a ataques, a vertical em questão se constitui em uma ferramenta poderosa para capacitar e treinar os escassos recursos humanos tanto das FFAA quanto de outros setores da sociedade na área de Segurança Cibernética (Fontes, 2024; Cravo, 2023). A vertical ainda é capaz de potencializar a Inteligência Estratégica, gerando conhecimento útil sobre tendências e cenários de ameaças cibernéticas de alta complexidade para técnicos e gestores no âmbito da Defesa Cibernética (Melo; Albuquerque; Mendonça, 2022).

Outra contribuição da vertical de redes de rádios é como ferramenta de experimentação e certificação, podendo promover a convergência de esforços de forma mais coesa entre os diversos atores da sociedade e facilitar a implementação das políticas, diretrizes, regulamentos e requisitos específicos para a Segurança Cibernética (Cravo, 2023; Gomes; Laginestra, 2023).

6 CONSIDERAÇÕES FINAIS

Este artigo apresentou reflexões sobre as contribuições para a Defesa Nacional do CYBEROS, um *Cyber Range* nacional customizado para a realização de exercícios cibernéticos, considerando cenários realistas de proteção de IC, bem como o uso de redes de rádios táticos militares.

O próprio contexto em que esse sistema é desenvolvido foi relevante nesta discussão, por diversos aspectos realçados ao longo do texto.

O CYBEROS e o ambiente em que se insere foram apresentados, de modo a destacar as características mais relevantes com potencial de conexão com as demandas da Defesa Nacional. Para que esse alinhamento fosse mais objetivo, uma pesquisa qualitativa foi realizada com foco em documentos normativos de alto nível da Defesa Nacional, pertinentes aos temas principais de contextualização do sistema em questão: Segurança Cibernética e proteção de IC. Com isso, foram identificados e analisados três pares de políticas e estratégias nacionais: PND/END; PNCiber/E-Ciber; e PNSIC/ENSIC. Outras referências relevantes de nível tático ou operativo também foram consideradas de forma complementar na análise das contribuições potenciais específicas da vertical de redes de rádios táticos vinculada ao CYBEROS.

O sistema analisado neste trabalho contribui para enfrentar vários dos principais desafios para a CT&I na Defesa, em especial no setor tecnológico estratégico cibernético, tais como a dependência de tecnologias estrangeiras, o cerceamento tecnológico e a necessidade de formação de recursos humanos qualificados. Foi possível apontar de forma clara de que formas o sistema contribui ou pode contribuir para diversos objetivos, estratégias e ações estratégicas dos três pares de documentos de alto nível da Defesa Nacional mais pertinentes. Várias reflexões complementares a respeito do potencial específico da vertical de redes de rádios táticos para contribuir com a Defesa Nacional também foram discutidas. Em suma, o CYBEROS e suas verticais se constituem em uma ferramenta que ajuda o Brasil a fortalecer sua soberania tecnológica e a se posicionar como um ator relevante no cenário internacional de Defesa, na área de Segurança Cibernética.

AGRADECIMENTOS

Este trabalho foi realizado no âmbito do projeto ITSC2ICCOM, com o apoio financeiro da Financiadora de Estudos e Projetos (FINEP) – Instrumento Contratual, Código nº 01.22.0523.00 (Ref. 1890/22). Menção especial também aos demais integrantes do LaSC que contribuíram direta ou indiretamente para a viabilização deste artigo.

REFERÊNCIAS

ADIWAL, Sanjay; MISBAHUDDIN, Mohammad. Intrusion Detection and Prevention in OpenStack: A Case Study on Enhancing Security and Threat Detection. **SN Computer Science**, v. 4, n. 830, 2023. DOI: 10.1007/s42979-023-02265-3

AL-SHARA, A.; AHMAD, M. **Cyber Warfare**: Attacks and Countermeasures. Cham: Springer, 2018.

BAGGA, J. Introduction to APIs. *In*: BAGGA, J. **Introduction to Integration Suite Capabilities**. Berkeley: Springer, 2023.

BALDINI, G. *et al*. Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead. **IEEE Communications Surveys & Tutorials**, v. 14, n. 2, p. 355-379, 2012. DOI: 10.1109/SURV.2011.032511.00097

BARBOSA, F. G. F. T.; CALDEIRA, A. B. Desafios da inovação como estratégia para a geração de capacidades militares terrestres. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 15, n. 54, p. 273-293, 2021.

BARROS, M. Instituto Militar de Engenharia Capacita Militares para Cyber Flag 24-1. **Defesa em Foco**, 17 jun. 2024. Disponível em: https://www.defesaemfoco.com.br/instituto-militar-de-engenharia-capacita-militares-para-cyber-flag-24-1/. Acesso em: 6 ago. 2025.

BARROS, M. Cyber Shield 2025: Defesa Cibernética do Brasil em destaque nos EUA. **Defesa em Foco**, 10 jun. 2025. Disponível em: https://www.defesaemfoco.com.br/cyber-shield-2025-defesa-cibernetica-do-brasil-em-destaque-nos-eua/. Acesso em: 25 jun. 2025.

BERGSTROM, C. *et al*. Software defined radio (SDR) special military applications. **MILCOM 2002**, Anaheim, v. 1, p. 383-388, 2002. DOI: 10.1109/MILCOM.2002.1180472

BRANCO, M. G. C. *et al*. Rádio Definido por Software do Ministério da Defesa – Visão geral das primeiras contribuições do CPqD. **Cadernos CPqD Tecnologia**, v. 10, n. esp., p. 9-16, 2014.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF, 2008.

BRASIL. Presidência da República. Decreto nº 9.573, de 22 novembro de 2018. **Diário Oficial da União**, Brasília, DF, 2018a.

BRASIL. Presidência da República. 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, e altera o Decreto nº 2.295, de 4 de agosto de 1997. **Diário Oficial da União**, Brasília, DF, 2018b.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estratégia Nacional de Segurança Cibernética**. Brasília, DF, 2020a.

BRASIL. Presidência da República. Decreto nº 10.569, de 9 dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial da União**, Brasília, DF, 2020b.

BRASIL. Presidência da República. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. **Diário Oficial da União**, Brasília, DF, 2023.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Decreto Legislativo nº 61, 23 mai. 2024. Brasília, DF, 2024a.

BRASIL. Exército Brasileiro. Exército coordena o maior exercício cibernético do Hemisfério Sul. **Noticiário do Exército**, 11 out. 2024b. Disponível em: https://www.eb.mil.br/web/noticias/w/exercito-coordena-maior-exercicio-cibernetico-do-hemisferio-sul. Acesso em: 6 ago. 2025.

BRASIL. Presidência da República. **Decreto nº 12.573, de 4 de agosto de 2025**. Institui a Estratégia Nacional de Cibersegurança. **Diário Oficial da União**, Brasília, DF, 2025.

CAMARGO, O. A. M. *et al*. Laboratório de Segurança Cibernética para Análise de Malwares Reais em Infraestruturas Críticas. **Congresso Brasileiro de Automática - CBA**, v. 3, n. 1, 2022.

CASTILHO, C. A. C. **A Segurança Cibernética na proteção das infraestruturas críticas brasileiras**. Trabalho de Conclusão de Curso (Curso Superior de Segurança e Defesa Cibernética) – Escola Superior de Guerra, Rio de Janeiro, 2023.

CONTI, M. *et al*. Internet of Things security and Forensics: Challenges and Opportunities. **Future Generation Computer Systems**, v. 78, p. 544-546, 2018. DOI: 10.1016/j.future.2017.07.060

CRAVO, C. V. **Em busca de uma estratégia nacional de segurança cibernética: marco legal e autoridade nacional de segurança cibernética**. 2023. Tese (Doutorado em Estudos Estratégicos Internacionais) – Programa de Pós-Graduação em Estudos Estratégicos Internacionais, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023. Disponível em: https://lume.ufrgs.br/handle/10183/263232. Acesso em: 6 ago. 2025.

FELLER, J. *et al*. (orgs.). **Perspectives on Free and Open Source Software**. Cambridge: MIT Press, 2005.

FONTES, P. R. **A contribuição da Inteligência Estratégica para a Defesa Nacional contra Ameaças Cibernéticas**. 2024. Trabalho de Conclusão de Curso (Especialização em Inteligência Estratégica) – Escola Superior de Defesa, Brasília, DF, 2024.

FUNDAÇÃO DE APOIO À PESQUISA, DESENVOLVIMENTO E INOVAÇÃO DO EXÉRCITO BRASILEIRO – FAPEB**. ITSC2ICCOM – Convênio FINEP-FAPEB Nº 01.22.0523.00**. Rio de Janeiro: FAPEB, 2022. Disponível em: https://fapeb.com.br/its2iccom-convenio-finep-fapeb-no-01-22-0523-00/. Acesso em: 6 ago. 2025.

FUNDAÇÃO DE APOIO À PESQUISA, DESENVOLVIMENTO E INOVAÇÃO DO EXÉRCITO BRASILEIRO – FAPEB. **Chamada Pública nº 05/2025 – ITSC2ICCOM**: contratação de serviço de desenvolvimento e entrega de um orquestrador e provisionador de ambientes virtualizados heterogêneos completos. Rio de Janeiro: FAPEB, 2025. Disponível em: https://fapeb.com.br/wp-content/uploads/2025/06/EDITAL-PARA-CHAMADA-PUBLICA-PROJETO-ORQUESTRADOR-ERRATA-DE-CRONOGRAMA.pdf. Acesso em: 6 ago. 2025.

GOMES, N. L. S.; LAGINESTRA, A. M. Governança da Segurança Cibernética e os desafios do século XXI: a relação civis-militares no sector cibernético do Brasil. **Revista Foco**, Curitiba, v. 16, n. 7, p. 1-17, 2023. DOI: 10.54751/revistafoco.v16n7-056

HEINÄARO, K. Cyber attacking tactical radio networks. *In*: **International Conference on Military Communications and Information Systems (ICMCIS)**. Cracóvia, 2015. p. 1-6. DOI: 10.1109/ICMCIS.2015.7158684

INSTITUTO MILITAR DE ENGENHARIA – IME. **Pós-Graduação em Proteção de Sistemas Elétricos (PGPSE)**. Rio de Janeiro, 2025. Disponível em: https://pgpse.ime.eb.br/. Acesso em: 6 ago. 20256.

KLOTH, S. *et al*. Towards a Cyber Defense System in Software-Defined Tactical Networks. *In*: **International Conference on Military Communication and Information Systems (ICMCIS)**, 2024. p. 1-8. DOI: 10.1109/ICMCIS61231.2024.10540952

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de Metodologia Científica**. 8. ed. São Paulo: Atlas, 2017.

LI, K. *et al*. Security Mechanisms to Defend against New Attacks on Software-Defined Radio. In: **International Conference on Computing, Networking and Communications (ICNC)**, Maui, p. 537-541, 2018. DOI: 10.1109/ICCNC.2018.8390381

LILLEMETS, P. *et al*. A Systematic Review of Cyber Range Taxonomies: Trends, Gaps, and a Proposed Taxonomy. **Future Internet**, v. 17, n. 6, p. 259, 2025. DOI: 10.3390/fi17060259

MALAGUTTI, M. Ameaças ao Ciberespaço, Logística e Segurança Nacional, Não Necessariamente nessa Ordem. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 16, n. 57, p. 417-441, 2022.

MEDEIROS, B. P.; CARVALHO, A. C.; GOLDONI, L. R. F. Uma análise sobre o processo de securitização do ciberespaço. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 13, n. 46, p. 45-66, 2019.

MELO, R. C. R.; ALBUQUERQUE, R. O.; MENDONÇA, F. L. L. Modelo para mapeamento de ameaças cibernéticas. *In*: Iberian Conference on Information Systems and Technologies (CISTI), 17., 2022. **Anais** [...]. Madrid, 2022. p. 1-745.

MOREIRA, R. G.; GALDINO, J. F. A "dualidade" da dualidade tecnológica: implicações para países em desenvolvimento. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 18, n. 62, p. 189-216, 2024.

OKABAYASHI, V. H. **Defesa cibernética em infraestruturas críticas: estratégias avançadas para mitigação de ameaças**. 2024. Trabalho de Conclusão de Curso (Curso de Altos Estudos de Política e Estratégia) — Escola Superior de Guerra, Rio de Janeiro, 2024.

OR-MEIR, O. *et al*. Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. **ACM Computing Surveys**, v. 2, n. 5, 2019. DOI: 10.1145/3329786

PINHEIRO, A. S. A tecnologia da informação e a ameaça cibernética na guerra irregular do século XXI. **Coleção Meira Mattos**, Rio de Janeiro, n. 18, p. 4-11, 2008.

REDAÇÃO TECNOLOGIA & DEFESA. RDS-RONDON, mais um integrante da família RDS-DEFESA. **Tecnologia & Defesa**, 5 fev. 2024. Disponível em: https://tecnodefesa.com.br/rds-rondon-mais-um-integrante-da-familia-rds-defesa/. Acesso em: 6 ago. 2025.

REIS, J. P. **Segurança cibernética: uma abordagem conceitual com elementos de análise de risco**. 2024. Trabalho de Conclusão de Curso (Especialização em Inteligência Estratégica) – Escola Superior de Defesa, Brasília, DF, 2024.

SANDOVAL, A. A. J. Como a tecnologia está controlando nossa infraestrutura crítica, civis e militares trabalhando juntos para minimizar ciberataques. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 14, n. especial, p. 153-168, 2020.

SANTOS JUNIOR, J. B. S. *et al*. Novas ameaças e a cibersegurança: uma análise do sistema brasileiro de defesa cibernética frente ao caso da espionagem durante o governo Dilma Roussef. *In*: **Congresso Acadêmico de Defesa Nacional**, 2019, Rio de Janeiro, v. 1, p. 110-120. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/novasa_ameacasa_ea_aa_cibersegurancaa_umaa_analisea_doa_sistemaa_brasileiroa_dea_defesaa_cibernetica.pdf. Acesso em: 6 ago. 2025.

SCHWETHER, N. A evolução e o futuro da Ciberguerra: um estudo aprofundado de Portugal. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 18, n. 63, p. 463-479, 2025.

SILVA, F. A. B.; MOURA, D. F. C.; GALDINO, J. F. Classes of attacks for tactical software defined radios. **International Journal of Embedded and Real-Time Communication Systems**, v. 3, n. 4, p. 57-82, 2012. DOI: 10.4018/jertcs.2012100104

SILVA, F. A. B.; MOURA, D. F. C.; GALDINO, J. F. Security Issues in Tactical Software-Defined Radios: Analysis of Attacks and Case Studies. *In*: **ADVANCING EMBEDDED SYSTEMS AND REAL-TIME COMMUNICATIONS WITH EMERGING TECHNOLOGIES**. Hershey: IGI Global, 2014, p. 22-53.

SNEPS-SNEPPE, M. On Cyber Threats in Military Communication Nets. *In*: **IEEE WORKSHOP ON MICROWAVE THEORY AND TECHNOLOGY IN WIRELESS COMMUNICATIONS (MTTW)**, Riga, Latvia, 2024. p. 12-17. DOI: 10.1109/MTTW64344.2024.10742192

SOUZA, R. C. S.; OLIVEIRA, T. F. D.; PAULA, M. G. A Guerra Cibernética Russo-Ucraniana: os ataques russos às Infraestruturas Críticas ucranianas e possíveis lições para o Exército Brasileiro. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 18, n. 61, p. 143-158, 2024.

ŠVÁBENSKÝ, V. *et al*. Cybersecurity knowledge and skills taught in capture the flag challenges. **Computers & Security**, v. 102, p. 102154, 2021. DOI: 10.1016/j.cose.2020.102154

TANG, C. Meta's Hyperscale Infrastructure: Overview and Insights. **Communications of the ACM**, v. 8, n. 1, 2025. DOI: 10.1145/3629263

THOMAS, J.; FIALA, M. Resilient Tactical Communications in Adversarial Environments. **Defence Technology Review**, v. 28, 2020.

VU, L. *et al*. A Cyber-HIL for Investigating Control Systems in Ship Cyber Physical Systems Under Communication Issues and Cyber Attacks. **IEEE Transactions on Industry Applications**, v. 60, n. 2, p. 2142-2152, 2024. DOI: 10.1109/TIA.2023.3311429