ARTÍCULO DOI 10.52781/cmm.a196

El sistema CYBEROS y su vertical de redes de radios tácticos: reflexiones sobre las posibles contribuciones a la Defensa Nacional

CYBEROS system and its vertical of tactical radio network: reflections on potential contributions to national defense

Resumen: Los documentos normativos que definen las políticas y estrategias rectoras de la Defensa Nacional y de varias de sus ramas destacan la importancia del sector cibernético. El fortalecimiento de este sector pasa por varias estrategias específicas, como la integración del ámbito académico con la base industrial de defensa, el desarrollo de tecnologías de doble uso y la capacitación de recursos humanos especializados. En este contexto, destaca el sistema CYBEROS, una herramienta computacional innovadora que permite realizar ejercicios de ciberseguridad mediante la simulación realista de escenarios de protección de infraestructuras críticas, así como de redes de radios tácticos. Este trabajo presenta reflexiones sobre las posibles contribuciones de esta herramienta a la Defensa Nacional, con énfasis en el sector cibernético. Para ello, se realizó una investigación cualitativa en la que se compararon las acciones estratégicas previstas en el marco normativo actual con los principales resultados esperados de ese desarrollo. Se constata que CYBEROS y su vertical de redes de radios tácticos contribuyen de manera objetiva a varias de esas acciones estratégicas.

Palabras clave: Ciberdefensa; Comunicaciones tácticas; Radio definida por software; Defensa nacional; Protección de infraestructuras 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 it involves several 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 offers cybersecurity exercises by realistically simulating critical infrastructure protection scenarios and tactical radio networks. This study reflects on the potential contributions of this tool to national defense, especially regarding the cyber sector. For this, a qualitative study was conducted comparing strategic actions 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 directly contribute 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
mauricio.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

Recibido: 27 ago. 2025
Aprobado: 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 INTRODUCCIÓN

La Política Nacional de Defensa (PND) y la Estrategia Nacional de Defensa (END) son los documentos rectores, de carácter público, de más alto nivel de la Defensa Nacional (Brasil, 2024a). La PND presenta los supuestos básicos de Brasil en relación con su defensa y establece los Objetivos Nacionales de Defensa (OND). A su vez, la END orienta a todos los sectores del Estado brasileño sobre las medidas que deben implementarse para alcanzar los objetivos, definiendo Estrategias de Defensa (ED) y Acciones Estratégicas de Defensa (AED).

Un aspecto destacado que se observa en esta documentación orientativa es la necesidad de fortalecer los tres sectores tecnológicos estratégicos para la Defensa Nacional: el nuclear, el espacial y el cibernético (Brasil, 2024a). Incluso se tiene cuidado de asignar la responsabilidad de cada uno de estos sectores a una Fuerza Armada específica (Armada, Fuerza Aérea y Ejército, respectivamente), aun considerando la estructura matricial de estos sectores entre las tres Fuerzas. Cabe destacar que esta composición de sectores tecnológicos estratégicos y sus respectivas responsabilidades son las mismas que se previeron originalmente en la primera edición de la END (Brasil, 2008).

De estos tres sectores, el que presenta un menor tiempo de madurez tecnológica y probablemente el que se extiende de manera más amplia por las tres Fuerzas Armadas (FFAA) es el cibernético. El sector cibernético abarca el conjunto de tecnologías, procesos y prácticas diseñadas para proteger redes, computadoras, programas y datos contra ataques, daños o acceso no autorizado. Este sector es esencial para la seguridad y la defensa nacionales, ya que las amenazas cibernéticas pueden comprometer las infraestructuras críticas (IC), como los sistemas de energía, comunicaciones y defensa. La defensa cibernética implica la implementación de medidas preventivas y reactivas para detectar, responder y neutralizar amenazas, garantizando la integridad, la confidencialidad y la disponibilidad de la información y los sistemas estratégicos del país.

De hecho, la protección de las IC desde el punto de vista cibernético es una preocupación global de principios del siglo XXI que ha venido exigiendo una atención cada vez mayor, tal como lo han señalado Pinheiro (2008), Sandoval (2020) y Souza, Oliveira y Paula (2024), y que tiene repercusiones evidentes en las doctrinas militares contemporáneas. Desde entonces, se han desarrollado numerosos debates sobre el sector cibernético, la protección de las IC y otras ramificaciones relacionadas en el contexto de la Defensa Nacional de Brasil y de otras naciones. Se pueden encontrar ejemplos recientes de estas contribuciones en Medeiros, Carvalho y Goldoni (2019), Malagutti (2022), Castilho (2023), Okabayashi (2024) y Schwether (2025).

La importancia y la magnitud del sector cibernético en la actualidad son tan grandes que la atención que se le brinda no puede limitarse al ámbito de actuación del Ministerio de Defensa. En este contexto más amplio, destacan la Política Nacional de Ciberseguridad (PNCiber) (Brasil, 2023) y la Estrategia Nacional de Ciberseguridad (E-Ciber) (Brasil, 2025). En la misma lógica, la protección de las IC también ha adquirido mayor relevancia y cuenta con su propia legislación normativa de alto nivel, con la formulación de la Política Nacional de Seguridad de Infraestructuras Críticas (PNSIC) (Brasil, 2018a) y de la Estrategia Nacional de Seguridad de Infraestructuras Críticas (ENSIC) (Brasil, 2020b).

En este contexto, cobra cada vez más importancia el papel que se espera de la comunidad académica nacional, ya sea en su función principal de capacitación de recursos humanos, ya sea en la realización de Investigación, Desarrollo e Innovación (I+D+i), buscando la integración con el sector productivo público y privado, con énfasis en las entidades que conforman la Base Industrial de Defensa (BID). Como se pone de manifiesto en todo este conjunto normativo, esta es una

de las principales vías en la búsqueda de innovaciones tecnológicas cibernéticas, preferiblemente de carácter dual, que ayuden al país a alcanzar la autonomía tecnológica y a fortalecer su posición en el panorama geopolítico global actual y futuro (Barbosa; Caldeira, 2021; Moreira; Galdino, 2024).

Un ejemplo de entorno académico que puede ayudar a cumplir con el papel que se espera de él en el contexto en cuestión es el Laboratorio de Ciberseguridad de Sistemas Ciberfísicos (LaSC) del Instituto Militar de Ingeniería (IME), que entró en funcionamiento a finales de 2021 (Camargo *et al.*, 2022). El LaSC cuenta con una infraestructura que permite la simulación *hardware-in-the-loop* (HIL) en tiempo real de sistemas ciberfísicos sometidos a ataques reales de malware, lo que facilita los estudios y la investigación en Ciberseguridad, como el sistema analizado en Vu *et al*. (2024), por ejemplo.

A finales de 2022, se firmó un proyecto de desarrollo entre la Entidad Financiera para Estudios y Proyectos (FINEP), la Fundación de Apoyo a la Investigación, el Desarrollo y la Innovación del Ejército Brasileño (FAPEB), el Centro Tecnológico del Ejército (CTEx) y el IME, denominado "Innovaciones Tecnológicas para la Ciberseguridad de Sistemas Ciberfísicos Aplicadas a Infraestructuras Críticas y Comunicaciones Estratégicas y Tácticas" (ITSC2ICCOM), con el objetivo de mejorar las capacidades de estudios cibernéticos y ampliar el alcance de actuación del LaSC, incorporando nuevos casos de uso o "verticales" que representan la infraestructura crítica de los sectores eléctrico, de petróleo y gas, de comunicaciones, etc. (FAPEB, 2022). Tras un proceso de selección de un socio estratégico (FAPEB, 2025), en el que el Centro de Investigación y Desarrollo en Telecomunicaciones (CPQD) fue la institución seleccionada, en 2025 se inició el desarrollo más significativo de este proyecto: el sistema CYBEROS, un *Cyber Range* (Lillemets *et al*., 2025) nacional diseñado a medida para incorporar la simulación realista de redes, sistemas e infraestructuras reales. El sistema permite realizar entrenamientos y ejercicios típicos de capacitación en Ciberseguridad, ofreciendo de manera innovadora entornos virtualizados con simulaciones realistas de escenarios de protección de las IC y de redes de comunicaciones militares.

La vertical que atrajo mayor atención inicial fue la de las redes de radios tácticos, compuestas por radios como los de la familia de Radios Definidas por Software de Defensa (RDS-Defesa), en cuyo desarrollo han participado varios miembros de la BID desde hace más de una década (Branco *et al.*, 2014; Redação Tecnologia & Defesa, 2024). Esta prioridad se justifica dado que la aparición de las doctrinas relacionadas con la Ciberseguridad ha generado nuevas preocupaciones sobre la vulnerabilidad de estas redes, además de las ya previstas por las doctrinas militares de Comunicaciones y Guerra Electrónica, como lo ilustra el mapeo de clases de ataques tácticos a las RDS analizado en Silva, Moura y Galdino (2012) y por la metodología propuesta en Kloth *et al.* (2024).

A partir de lo expuesto, se identificó el siguiente problema de investigación: ¿Cómo pueden CYBEROS y sus verticales, en particular la vertical de redes de radios tácticos, contribuir a la Defensa Nacional? Teniendo esto en cuenta, el objetivo de este artículo es demostrar que las contribuciones potenciales de este desarrollo y el contexto en el que se inserta están en consonancia con los principales documentos de orientación de las políticas y estrategias nacionales de defensa, con énfasis en el sector cibernético. Para ello, se realizó una investigación cualitativa centrada en el marco normativo de alto nivel que respalda la Defensa Nacional, con el fin de identificar los objetivos, estrategias y acciones estratégicas con los que se alinea CYBEROS.

La sección 2 describe con mayor detalle el LaSC y el Proyecto ITSC2ICCOM, en el que se enmarcan el sistema CYBEROS y sus verticales. La metodología adoptada en este trabajo se explica en la sección 3. La sección 4 detalla la alineación del sistema en su conjunto con las principales políticas y estrategias pertinentes de la Defensa Nacional. La sección 5 presenta una reflexión más específica sobre las posibles contribuciones de la vertical de redes de radios tácticos. El artículo concluye en la sección 6.

2 LaSC Y EL PROYECTO ITSC2ICCOM

2.1 Historia y antecedentes

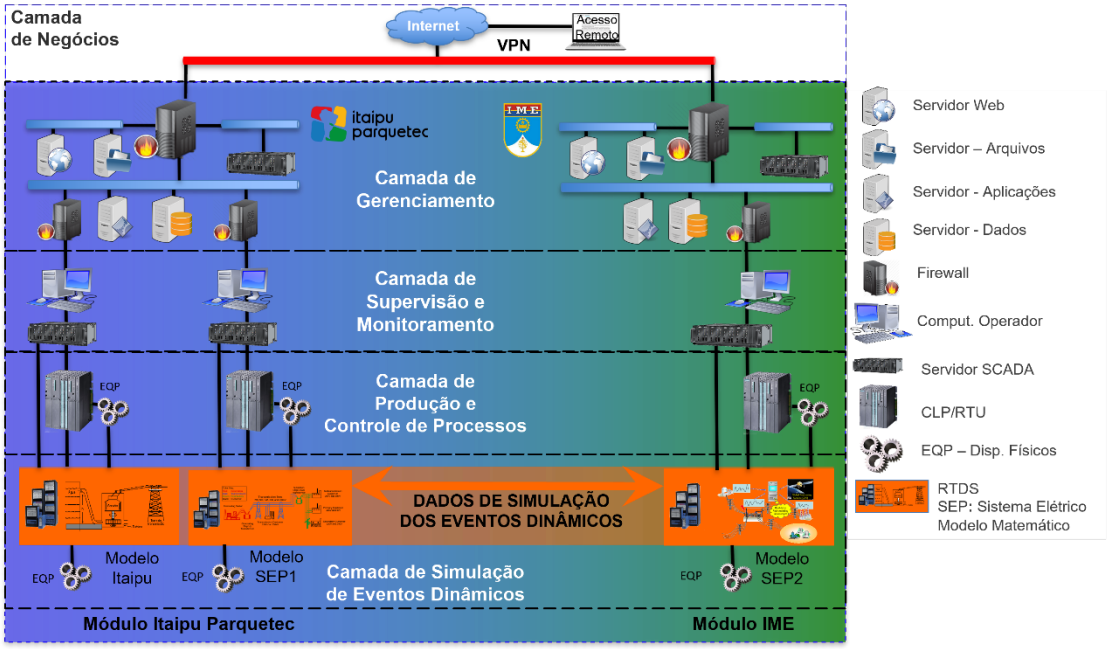
La economía y la sociedad dependen en gran medida de las tecnologías de la información y la comunicación, lo que convierte al ciberespacio en un ámbito crítico que incide en las esferas económica, social y política de los Estados, lo que exige la adaptación de las doctrinas y estrategias de seguridad. Esta dependencia conlleva una serie de vulnerabilidades y amenazas cada vez mayores, como los ataques de *phishing*, los ataques de denegación de servicio, las fugas de datos, el espionaje y el terrorismo cibernético. La difusión indiscriminada de información en el entorno en línea, incluyendo scripts para lanzar ataques cibernéticos, permite que usuarios que no necesitan un alto nivel de conocimiento técnico puedan realizar ataques cada vez más sofisticados. Por ello, la confidencialidad, la integridad, la autenticidad y la disponibilidad de la información se ven constantemente amenazadas. En este contexto, destaca la preocupación por los ataques cibernéticos dirigidos a las IC, cuya interrupción o destrucción de los servicios puede causar graves repercusiones, comprometiendo la seguridad del Estado y de la sociedad (Cravo, 2023; Fontes, 2024; Gomes; Laginestra, 2023; Melo; Albuquerque; Mendonça, 2022; Reis, 2024; Santos Junior *et al.*, 2019).

La creación del LaSC respondió a esta preocupación, permitiendo apoyar la realización de actividades de I+D+i en Ciberseguridad de las IC del sector eléctrico, mediante simulaciones HIL en tiempo real. Las simulaciones incluyen modelos y dispositivos de redes eléctricas (generación, transmisión y distribución), de tecnologías de la información y las comunicaciones, y de tecnologías de automatización, todos ellos integrados y representando con fidelidad el comportamiento de los sistemas reales, tal como se ilustra en la Figura 1. Estas simulaciones de la fase inicial del LaSC consistían en la simulación de incidentes cibernéticos reales, ataques de cualquier tipo, con énfasis en malware y en la contaminación cibernética de entornos industriales, lo que permitió verificar los efectos en las diferentes capas, identificar vulnerabilidades y proponer soluciones.

En este período relativamente corto de existencia, el LaSC ha ido acumulando una capacidad científica, tecnológica y de innovación significativa en materia de ciberseguridad, con resultados importantes en el apoyo a la formación de recursos humanos y a la producción intelectual. En este contexto, cabe destacar en primer lugar la creación, en 2022, del curso de Posgrado en Protección de Sistemas Eléctricos (PGPSE) (IME, 2025). En la misma línea, el LaSC también comenzó a contribuir al desarrollo de investigaciones en los programas de posgrado (maestría y doctorado) del IME.

Otro aspecto en el que ha contribuido el LaSC ha sido el apoyo a la preparación y la formación de equipos militares brasileños para participar en ejercicios cibernéticos nacionales e internacionales. Cabe destacar, en primer lugar, el Cyber Flag de mayo de 2024 (Barros, 2024) y el Cyber Shield de junio de 2025 (Barros, 2025), coordinados por el United States Cyber Command y el United States Department of Defense, considerados los ejercicios de combate cibernético más grandes del mundo. En ambas ocasiones, un mes antes de esos ejercicios, un equipo del LaSC impartió capacitación sobre temas específicos de ciberseguridad relacionados con la protección de las IC a los militares de las tres FFAA que integraban los equipos brasileños. El LaSC también contribuyó a la planificación y participó en el Ejercicio Guardián Cibernético (EGC) de 2024, y también estaba prevista su participación en el EGC de 2025. El EGC es el mayor ejercicio de defensa cibernética del hemisferio sur, en el que participan sectores públicos y privados relacionados con la protección de las IC de Brasil, y está organizado por el Comando de Defensa Cibernética (ComDCiber) (Brasil, 2024b).

Figura 1 – LaSC: diseño lógico inicial de experimentos y simulaciones



Fuente: Integrantes del LaSC (2021).

Tras la puesta en marcha del LaSC, los resultados preliminares apuntaban a un potencial de contribuciones en materia de I+D+i y en la capacitación de recursos humanos mucho más amplio que el alcance inicial, vinculado principalmente a la protección de las IC del sector eléctrico. Para hacer posible la expansión de las actividades del laboratorio y dar mayor visibilidad a sus resultados, el IME solicitó financiamiento a la FINEP, en colaboración con el CTEx y la FAPEB, y firmó un convenio para el desarrollo del proyecto ITSC2ICCOM (FAPEB, 2022). El objetivo del proyecto es desarrollar innovaciones tecnológicas para la ciberseguridad de los sistemas ciberfísicos aplicadas a la protección de las IC y a las comunicaciones estratégicas y tácticas. El desarrollo de estas innovaciones se centra en su aplicación en sistemas de RDS y de comunicaciones destinados a usos militares y civiles, además de otros sistemas ciberfísicos.

2.2 Sistema CYBEROS

Tras un período de maduración sobre las premisas, la metodología, los objetivos y los requisitos, se establecieron los requisitos para la contribución más significativa que se espera del proyecto ITSC2ICCOM: el sistema CYBEROS. Este sistema se desarrolla en colaboración con el CPQD, institución ganadora de la licitación lanzada a principios de 2025 (FAPEB, 2025).

CYBEROS se encarga de la orquestación automatizada de escenarios de ciberseguridad, lo que permite realizar formaciones y ejercicios típicos de este contexto, como el reconocido modelo *Capture the Flag* (CTF) (Švábenský *et al.*, 2021), en entornos virtualizados de simulaciones realistas. Una innovación de este diseño es la integración de módulos complementarios al que sería el núcleo típico de un cyber range, lo que permite operar las verticales en los escenarios específicos

de protección de las IC. Esta solución tiene el potencial de subsanar las brechas identificadas por el LaSC, dada la creciente sofisticación y frecuencia de los ataques dirigidos a sectores estratégicos. Plataformas como la Hack The Box[1] y el TryHackMe[2] no están totalmente adaptadas a aspectos específicos de los escenarios de protección de las IC ni permiten una personalización completa de los escenarios, lo que posiciona a CYBEROS como una solución innovadora y estratégica.

La arquitectura conceptual inicial de CYBEROS se ilustra en la Figura 2. Es modular, escalable y compatible con el entorno existente en el LaSC, lo que incluye el uso de herramientas similares al OpenStack (Adiwal; Misbahuddin, 2023) como pilares para la virtualización y la orquestación. Se basa en tres módulos principales: frontend, orquestador y backend. El *frontend* es la interfaz gráfica a la que tienen acceso los usuarios, diseñada para facilitar la interacción con el sistema, lo que permite configurar escenarios y topologías cibernéticas, dar seguimiento en tiempo real al avance de los ejercicios y visualizar métricas de desempeño.

El núcleo de CYBEROS es el orquestador encargado de automatizar la creación, la configuración y la ejecución de los escenarios simulados. Funciona en una plataforma de computación en la nube equivalente a OpenStack, con funcionalidades que incluyen: administración de máquinas virtuales y contenedores (Tang, 2025); configuración automatizada de redes y dispositivos simulados; soporte para la integración con dispositivos físicos, incluso en formato HIL; y monitoreo continuo del estado de los escenarios y de la asignación de recursos. Por su parte, el *Backend* procesa las solicitudes de los usuarios y las integra al sistema. Entre las funcionalidades que ofrece se encuentran: gestión de usuarios y permisos; gestión de registros (logs) e informes de actividad del sistema; e integración con bases de datos para un almacenamiento seguro y eficiente.

La virtualización es una forma de encapsular y aislar los desafíos cibernéticos, lo que garantiza un entorno consistente y seguro para los participantes en los ejercicios cibernéticos. El orquestador es, en esencia, el sistema operativo de la nube que administra y coordina máquinas virtuales y/o contenedores, así como la infraestructura de red y almacenamiento asociada a gran escala. Esta estrategia se integra en la infraestructura de ejercicios de mayor escala y complejidad, como los CTF modernos, lo que permite crear, administrar y aislar los entornos en los que se desarrollan los desafíos cibernéticos.

Un requisito importante del sistema es buscar la adopción de herramientas de código abierto completas, sin modificarlas (Feller *et al.*, 2005). Cualquier modificación debe realizarse a través de una interfaz de programación de aplicaciones (API) (Bagga, 2023). Además, el sistema debe ser compatible con herramientas de gestión de información y eventos de seguridad (Conti *et al*., 2018) y con herramientas de monitoreo continuo o análisis dinámico de malware (Or-Meir *et al*., 2019), para explorar y visualizar los datos, así como para monitorear el estado de los servidores e identificar comportamientos anómalos.

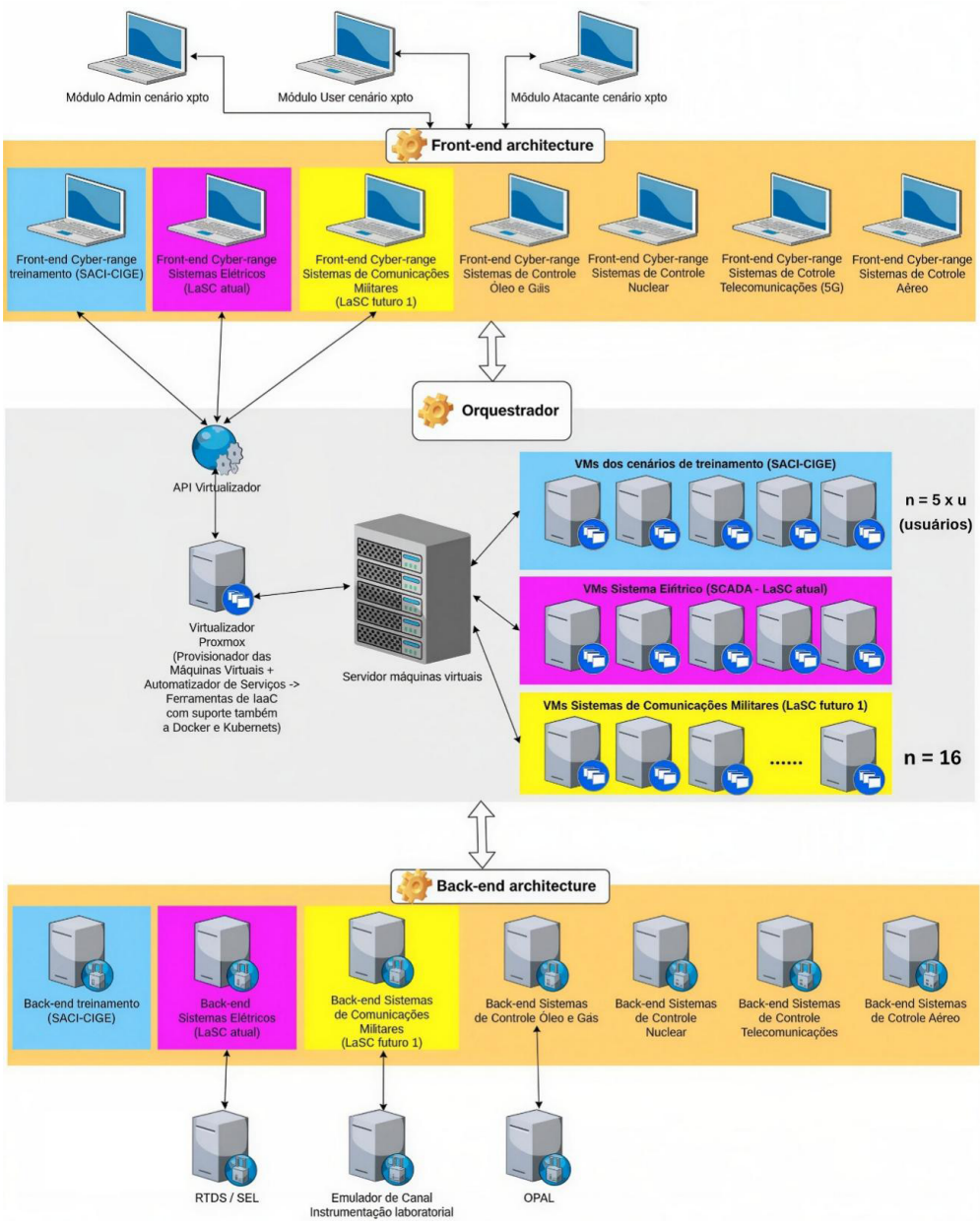
La Figura 2 ayuda a comprender el concepto de las verticales integradas en CYBEROS. Una vertical no es exactamente un módulo en sí misma, sino que solo representa la ejecución de un caso de uso o escenario específico de simulación de un ejercicio de ciberseguridad con sus particularidades. Es un modelo que representa la visión y las necesidades particulares de un perfil específico de usuario en los diferentes escenarios de protección de las IC. Por ejemplo, los elementos resaltados en color magenta en la Figura 2 representan el uso de CYBEROS, complementado con

1 Disponible en: https://www.hackthebox.com/. Consulta: 12 ago. 2025.

2 Disponible en: https://tryhackme.com/. Consulta: 12 ago. 2025.

módulos integrados específicos de apoyo a ejercicios de ciberseguridad en un escenario del sector eléctrico, lo que caracteriza la vertical del sector eléctrico.

Figura 2 – Concepto arquitectónico inicial del CYBEROS



Fuente: Integrantes del LaSC (2024).

Al integrar recursos que permiten la realización de ejercicios cibernéticos en un escenario realista de protección de las IC en cualquier vertical, el mero hecho de contar con este escenario virtualizado e integrado con elementos HIL ofrece otras aplicaciones para la herramienta, como el análisis de aspectos de desempeño y la simulación del uso del propio sistema de esa vertical. Para aprovechar de manera efectiva este

potencial, es necesario incorporar módulos complementarios adicionales, integrados al CYBEROS, cuyas características varían según la vertical. En particular, el desarrollo de esta versión inicial de CYBEROS permitió la aplicación de este método de análisis de desempeño a la vertical de los sistemas de comunicaciones militares o, más específicamente, a las redes de radios tácticos, compuestas principalmente por RDS. Esta forma de utilizar la vertical representa una alternativa para llevar a cabo entrenamientos o ejercicios operativos en un entorno cerrado y controlado, lo cual puede ser útil para apoyar la capacitación y el entrenamiento de las tropas, así como para generar nuevos conocimientos de interés para la doctrina.

2.3 Vertical de redes de radios tácticos

Los sistemas de comunicaciones tácticas militares también están expuestos a ataques cibernéticos y, por lo tanto, también necesitan una protección sólida (Al-Shara; Ahmad, 2018; Heinäaro, 2015; Reis, 2024; Sneps-Sneppe, 2024). El espectro electromagnético se ha convertido en un campo de batalla muy disputado, en el que las exigencias operativas requieren infraestructuras de comunicaciones tácticas especializadas, capaces de garantizar una conectividad continua y un intercambio seguro de información incluso en condiciones adversas (Kloth *et al.*, 2024; Thomas; Fiala, 2020). Las RDS, componentes que están muy presentes en las redes actuales de radios tácticos (Bergstrom *et al*., 2002), aunque ofrecen una notable flexibilidad funcional, también amplían significativamente la superficie de ataque cibernético debido a su dependencia de componentes lógicos y capas de software. Las vulnerabilidades de las RDS incluyen, además, riesgos relacionados con la cadena de suministro de hardware y software, en su mayoría extranjeros, la dependencia de actualizaciones remotas y el uso de bibliotecas de código abierto posiblemente comprometidas (Baldini *et al.*, 2012; Li *et al.*, 2018; Silva; Moura; Galdino, 2012, 2014).

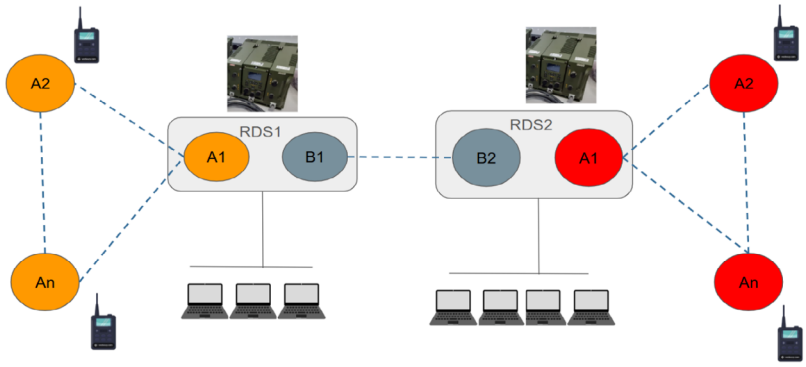
La vertical de redes de radios tácticos integra CYBEROS como un módulo compatible con la familia de RDS-Defesa. Por razones estratégicas, esta integración se inició con la plataforma vehicular, para la comunicación táctica en vehículos y embarcaciones militares, y posteriormente se extenderá al resto de tipos de radios, a medida que estén disponibles (FAPEB, 2025). La RDS-Defesa para vehículos presenta el Módulo de Radiofrecuencia (MRF), de diseño propio y que cumple con la especificación Transceiver Facility de la *Software Communications Architecture*, versión SCA 2.2.2, y el Módulo de Procesamiento (MP), que implementa una arquitectura basada en núcleos de procesamiento Rojo y Negro, separados físicamente e interconectados mediante un Módulo de Seguridad (MSEG) (Branco *et al.*, 2014). Con estos módulos, ofrece una estructura para la ejecución de diversas formas de onda, cada una de las cuales emplea protocolos de comunicación adecuados para distintos escenarios operativos (FAPEB, 2022).

La Figura 3 presenta un caso de uso representativo de la vertical en cuestión. Las redes de radios naranja y roja pueden, por ejemplo, dar servicio a dos batallones, respectivamente, que se encuentran físicamente separados entre sí. Las dos redes están interconectadas mediante las RDS para vehículos, las cuales pueden ejecutar simultáneamente dos formas de onda independientes, por lo que resultan útiles para integrar redes diferentes.

La red de radio que se muestra en la Figura 3, así como otras topologías de comunicación, se pueden configurar íntegramente en CYBEROS. En esta estructura, los MP —instancias virtualizadas en servidores— ejecutan las formas de onda en procesadores emulados por máquinas virtuales. A pesar de la virtualización del procesamiento, la transmisión y la recepción de señales de radiofrecuencia se

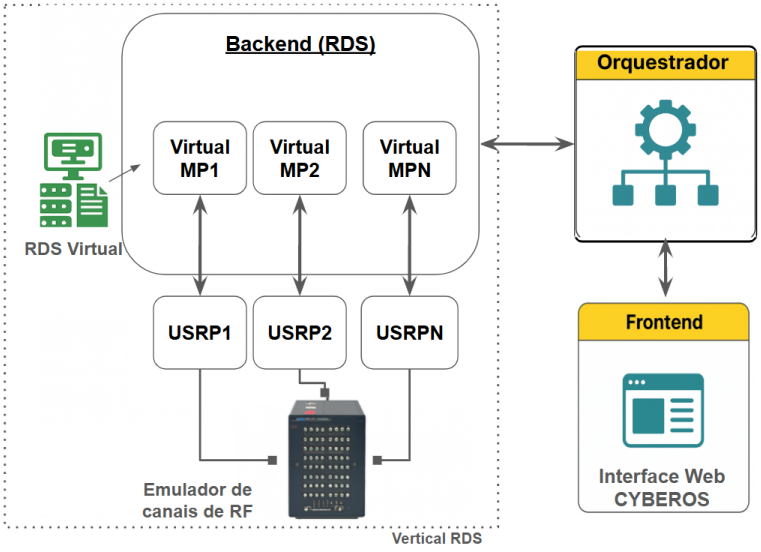
realizan mediante radios físicos comerciales, como dispositivos *Universal Software Radio Peripheral* (USRP)[3] o similares. Estos equipos ofrecen una gran flexibilidad de operación, con una amplia cobertura de frecuencias y anchos de banda, y son adecuados tanto para aplicaciones civiles (como redes 4G, 5G y 6G) como para escenarios tácticos. Esta arquitectura, que se puede identificar de manera genérica como una de las verticales de la Figura 2 (sistemas de comunicaciones militares – bloques de color amarillo), se detalla en la Figura 4, donde se destaca el uso del USRP y del emulador de canales de radiofrecuencia. El emulador de canales puede aplicar degradaciones controladas a las señales entre los diferentes nodos de la red, como atenuación, desvanecimiento y ruido. De esta manera, es posible realizar pruebas de desempeño, interoperabilidad y resiliencia de las formas de onda en condiciones equivalentes a las del campo, pero dentro de un entorno de laboratorio controlado.

Figura 3 – Ejemplo de caso de uso de una red de radios tácticos utilizando RDS



Fuente: Los autores (2025).

Figura 4 – Vertical de redes de radios tácticos basada en RDS virtualizadas del CYBEROS



Fuente: Los autores (2025).

3 Disponible en: https://www.ni.com/en/support/downloads/drivers/download.ni-usrp.html. Consulta: 12 ago. 2025.

3 METODOLOGÍA

Con el fin de aportar una contribución al problema de investigación planteado en este trabajo, se adoptó como metodología una investigación cualitativa. En general, la investigación cualitativa busca comprender los fenómenos en profundidad, explorando aspectos subjetivos y contextuales, y recurre a métodos como entrevistas, grupos focales y análisis de contenido (Lakatos; Marconi, 2017). Para este artículo, se adoptó el análisis de contenido de documentos normativos de alto nivel orientados a la planificación de la Defensa Nacional y de otras referencias bibliográficas pertinentes al tema elegido, con el fin de identificar correlaciones que evidenciaran de qué manera una herramienta de innovación tecnológica como CYBEROS —y, en particular, mediante su vertical de redes de radios tácticos— podría contribuir objetivamente a la Defensa Nacional.

En cuanto al alcance de los documentos normativos examinados, el análisis se limitó a tres grupos, teniendo en cuenta el contexto tecnológico específico de la innovación tecnológica en cuestión (sector cibernético). Con ello, se analizaron inicialmente la PND y la END como documentos normativos de más alto nivel. Para abarcar el alcance más específico del sector cibernético, se tomaron en cuenta la PNCiber y la E-Ciber. A su vez, el contexto de protección de las IC se evaluó a la luz de la PNSIC y la ENSIC. Este análisis, centrado en la alineación normativa, política y estratégica, se presenta en la sección 4, donde se señalan los objetivos, las estrategias y las acciones estratégicas que CYBEROS aborda de manera notable en su conjunto y/o considerando alguna de sus verticales.

La sección 5 se centra en el potencial de contribución de la vertical de redes de radios tácticos. Las reflexiones al respecto buscaron complementar la alineación con los documentos normativos de alto nivel identificados para CYBEROS en su conjunto, señalando también contribuciones de carácter táctico u operativo.

4 ALINEACIÓN CON LAS PRINCIPALES POLÍTICAS Y ESTRATEGIAS RELACIONADAS CON LA DEFENSA NACIONAL

4.1 PND/END

La PND es el documento rector de más alto nivel para la planificación de acciones destinadas a la defensa del país. Centrada principalmente en las amenazas externas, establece ocho OND para la preparación y el empleo de todas las manifestaciones del Poder Nacional, en pro de la Defensa Nacional. A su vez, la END define estrategias y acciones estratégicas que deben guiar a la sociedad brasileña en las acciones de defensa de la patria. En la versión actual, se han previsto 17 ED y 85 AED. Hay ED que se repiten para diferentes OND, así como hay AED que se repiten para diferentes ED (Brasil, 2024a).

En la descripción del diseño estratégico de defensa, hay un punto importante en la END que se relaciona directamente con este trabajo, en el que se señala que los sectores gubernamental e industrial, así como el ámbito académico, enfocados en la ciencia, la tecnología y la innovación (CT&I), deben ser priorizados e integrados para contribuir a garantizar que la satisfacción de las necesidades de productos de defensa (PRODE) se base en tecnologías críticas bajo dominio nacional. La END señala, además, que dichas tecnologías deben obtenerse mediante el estímulo y el fomento del sector industrial y el ámbito académico, de manera sinérgica. También señala que la capacitación de la BID, incluido el

dominio de las tecnologías de doble uso, es fundamental para lograr el abastecimiento de los PRODE, con miras a la autonomía tecnológica del país. Por lo tanto, se observa que el desarrollo del CYBEROS se ajusta a todas estas premisas que sustentan el diseño de la END, dada la participación del IME, el CTEx y el CPQD (una Empresa Estratégica de Defensa – EED), así como la naturaleza dual del sistema.

Entre los fundamentos de la END se destacan las Capacidades Nacionales de Defensa (CND), que se consideran aquellas compuestas por diferentes componentes de las manifestaciones del Poder Nacional. La actual END se basa en nueve CND: Protección; Respuesta rápida; Disuasión; Coordinación y control; Gestión de la información; Logística; Movilidad estratégica; Movilización; y Desarrollo tecnológico de defensa. De estas, dos en particular están relacionadas con el sistema CYBEROS y sus verticales: Protección y Desarrollo tecnológico de Defensa.

Las CND de Protección expresan el OND más relevante: el de garantizar la soberanía, el patrimonio nacional y la integridad territorial. Para reforzar esta CND es necesario adaptar y estructurar los sistemas de vigilancia en las áreas de interés y control, entre las que se incluye el ciberespacio. El sistema CYBEROS tiene el potencial de contribuir indirectamente a esta CND, desde el punto de vista de la protección y el monitoreo del ciberespacio, ayudando a capacitar a personal especializado y facilitando estudios e investigaciones sobre las vulnerabilidades cibernéticas de las IC, lo cual puede orientar a los grupos de interés en los procesos de toma de decisiones que busquen la adaptación y la estructuración de sistemas de vigilancia de este espacio estratégico.

Por su parte, la CND de Desarrollo Tecnológico de Defensa impulsa el desarrollo y/o la modernización de los PRODE, a través de acciones integradas emprendidas por el Estado, la industria y el sector académico, de manera sinérgica, con el objetivo de lograr la actualización y la independencia tecnológica. Por su naturaleza, CYBEROS se inscribe en este contexto, por lo que contribuye directamente a esta CND.

Los fundamentos de la END también abordan el sector de la defensa, detallando el papel de las tres FFAA, así como de los tres sectores tecnológicos estratégicos. La preocupación por el sector cibernético se manifiesta explícitamente para las tres FFAA, con énfasis en el Ejército, que desempeña un papel de liderazgo centralizado en este sentido. En lo que respecta específicamente al sector cibernético, la END señala que las capacitaciones deben incluir, como prioridad, las tecnologías de comunicación entre las unidades de las FFAA, a fin de garantizar su interoperabilidad y la capacidad de actuar de manera integrada y segura. El objetivo es mejorar la Seguridad de la Información y las Comunicaciones y la Ciberseguridad en todas las instancias del Estado, con énfasis en la protección de las IC. Para ello, es necesario fomentar la I+D+i centrada en tecnologías de doble uso que permitan la planificación y la ejecución de actividades cibernéticas en el ámbito del Sector de la Defensa y que contribuyan a la Ciberseguridad a nivel nacional, incluyendo a la comunidad académica. Además, se recomienda fortalecer la colaboración entre el sector de la defensa y la comunidad académica nacional, los sectores público y privado, y la BID. El CYBEROS encaja en estos aspectos fundamentales que sustentan la END.

El Cuadro 1 presenta la lista de OND, ED y AED a los que CYBEROS aporta contribuciones directas o indirectas. La justificación de esta alineación puede entenderse al analizar la relación con las AED, ya que atender a una AED lleva a atender a una ED y, por consiguiente, a atender a un OND. Empezando por la AED 1, el CYBEROS se caracteriza sin duda como un desarrollo estratégico de Defensa del sector cibernético. En cuanto a la AED 2, el papel diferenciado que CYBEROS permite desempeñar a las áreas de protección de las IC y de las redes de radios tácticos contribuye a

la capacitación de personal especializado y a la disponibilidad de herramientas de simulación realista de escenarios de ataques cibernéticos, lo que representa un beneficio indirecto para aumentar el nivel de seguridad de las IC. Esa misma línea de razonamiento se aplica a la AED 10, aunque de manera limitada, ya que CYBEROS puede ayudar a desarrollar las capacidades de monitorear y controlar específicamente el ciberespacio. La contribución a la AED 11 también puede basarse en estos argumentos, especialmente en lo que respecta a la capacidad de exploración del ciberespacio. Por último, la contribución a la AED 52 es evidente y no requiere justificaciones adicionales.

Cuadro 1 – Alineación de CYBEROS con la PND y la END

OND	ED	AED
I – Garantizar la soberanía, el patrimonio nacional y la integridad territorial	1 – Fortalecimiento del poder nacional	1 – Desarrollar los sectores estratégicos de la defensa (nuclear, cibernético y espacial) 2 – Contribuir a aumentar el nivel de seguridad de las IC de los sistemas de captación, tratamiento y distribución de agua; generación y distribución de energía eléctrica; transporte; producción y distribución de combustibles; y comunicaciones, entre otros
	2 – Fortalecimiento de la capacidad de disuasión	10 – Desarrollar las capacidades para monitorear y controlar el espacio aéreo, el ciberespacio, el territorio, las aguas jurisdiccionales brasileñas y otras áreas de interés 11 – Aumentar las capacidades para defender y explorar el ciberespacio
III – Promover la autonomía tecnológica y productiva en el ámbito de la Defensa	9 – Fortalecimiento del área de Ciencia y Tecnología de Defensa	52 – Promover el desarrollo de la tecnología cibernética
VIII – Aumentar la presencia de Brasil en la comunidad internacional y su participación en los procesos de toma de decisiones internacionales	1 – Fortalecimiento del poder nacional	1 – Desarrollar los sectores estratégicos de la defensa (nuclear, cibernético y espacial) 2 – Contribuir a aumentar el nivel de seguridad de las infraestructuras críticas de los sistemas de captación, tratamiento y distribución de agua; generación y distribución de energía eléctrica; transporte; producción y distribución de combustibles; y comunicaciones, entre otros

Fuente: Los autores (2025).

4.2 PNCiber y E-Ciber

En 2018, mediante el Decreto n.º 9.637, se publicó la Política Nacional de Seguridad de la Información (PNSI) (Brasil, 2018b), que establecía objetivos y medios para alcanzarlos en materia de Ciberseguridad, Defensa Cibernética, seguridad física y protección de datos organizacionales. La PNSI preveía su implementación a través de la Estrategia Nacional de Seguridad de la Información (ENSI) y de planes nacionales. Por su parte, se preveía que la ENSI se construyera en cinco módulos, que incluirían las acciones estratégicas y los objetivos relacionados con la Seguridad de la Información, en consonancia con las políticas públicas y los programas del gobierno federal. Los módulos de la ENSI deberían tratar los siguientes temas: Ciberseguridad; Defensa cibernética; seguridad de las IC; seguridad de la información confidencial; y protección contra la fuga de datos.

El módulo de ciberseguridad se desarrolló y publicó en 2020 como la Estrategia Nacional de Ciberseguridad (E-Ciber) (Brasil, 2020a). Esta E-Ciber constituyó la orientación explícita del gobierno

federal a la sociedad brasileña sobre las principales medidas que pretende implementar, tanto a nivel nacional como internacional, en el ámbito de la Ciberseguridad, para el cuatrienio 2020-2023.

La ENSI no se concretó tal como se había planeado originalmente en 2018. En particular, la E-Ciber dejó de estar bajo la competencia de la PNSI y pasó a estar vinculada a la Política Nacional de Ciberseguridad (PNCiber), establecida en 2023, junto con el Comité Nacional de Ciberseguridad (CNCiber), mediante el Decreto n.º 11.856 (Brasil, 2023). El CNCiber es un órgano colegiado vinculado a la Oficina de Seguridad Institucional de la Presidencia de la República (GSI-PR). El Decreto n.º 11.856 estableció que la E-Ciber debía actualizarse en los años siguientes, prorrogando la vigencia de la versión anterior hasta su sustitución. La nueva E-Ciber se publicó en agosto de 2025 (Brasil, 2025).

La PNCiber establece once objetivos en su artículo 3, de los cuales CYBEROS cumple cuatro, en mayor o menor medida, según el caso. Son los siguientes: I) promover el desarrollo de productos, servicios y tecnologías de origen nacional destinados a la ciberseguridad; VII) impulsar la educación y la capacitación técnico-profesional en materia de ciberseguridad en la sociedad; VIII) fomentar las actividades de investigación científica, desarrollo tecnológico e innovación relacionadas con la ciberseguridad; y IX) incrementar la acción coordinada y el intercambio de información sobre ciberseguridad entre la Unión, los estados, el Distrito Federal y los Municipios, los poderes Ejecutivo, Legislativo y Judicial, el sector privado y la sociedad en general.

Los objetivos de la PNCiber deben alcanzarse a través de la E-Ciber, que se estructura en cuatro ejes temáticos: I) protección y concientización de los ciudadanos y la sociedad; II) seguridad y resiliencia de los servicios esenciales y de las IC; III) cooperación e integración entre los organismos y entidades, tanto públicos como privados; y IV) soberanía nacional y gobernanza. Estos ejes temáticos deben implementarse mediante acciones estratégicas específicas, previstas en el Plan Nacional de Ciberseguridad, que aún está por elaborarse. En este sentido, la actual E-Ciber se diferencia estructuralmente de la anterior, de 2020, al sustituir los antiguos objetivos estratégicos por ejes temáticos y dejar el mapeo definitivo de las acciones estratégicas para el Plan Nacional. De todos modos, la actual E-Ciber ya presenta, para cada eje, una lista de acciones mínimas correspondientes.

De las catorce acciones relacionadas con el eje temático I, cuatro están relacionadas, en mayor o menor medida, con CYBEROS: IV – fomento de la capacitación de maestros y administradores, tanto del sector público como del privado, en materia de ciberseguridad; V – fomento de la inclusión de temas relacionados con la ciberseguridad en los planes de estudio de todos los niveles educativos; VI – fomento de la participación en foros y actividades académicas, técnicas y profesionales relacionadas con la ciberseguridad; y IX – fomentar el desarrollo de planes de contingencia institucionales y la realización de pruebas y simulaciones para verificar el nivel de ciberseguridad en el organismo o la entidad. El contexto de desarrollo de CYBEROS en el IME, una institución de educación superior, y su integración en el LaSC, tal como se analizó en la sección 2, justifican la alineación con las acciones IV, V y VI. La acción IX se cumple parcialmente en lo que respecta a las pruebas y simulaciones, dado que CYBEROS y sus verticales se proponen servir como herramienta para la simulación de diversos escenarios de ciberseguridad, con énfasis en la protección de las IC.

El eje temático II, que se refiere a los servicios esenciales y a las IC, especifica un mínimo de once acciones necesarias para su consecución. Curiosamente, a pesar de que CYBEROS destaca los escenarios de protección de las IC, solo se puede señalar una acción como directamente relacionada: VIII – fomentar la realización de ejercicios y simulacros sectoriales y multisectoriales periódicos destinados a mejorar la resiliencia de los servicios esenciales y de las IC. CYBEROS es una herramienta que estará a disposición

no solo del IME, sino de toda la comunidad académica y del sector productivo, y que podrá utilizarse en ejercicios y simulaciones de interés para las instituciones responsables de las IC nacionales.

Asimismo, el eje temático III presenta una sola acción, de entre las cinco enumeradas, a la que CYBEROS y el contexto en el que se inscribe aportan una contribución. La acción I de este eje consiste en impulsar la creación y el desarrollo de equipos de prevención y respuesta ante incidentes de ciberseguridad, centros de análisis e intercambio de información y laboratorios especializados en ciberseguridad. El LaSC, donde se desarrolla y aloja CYBEROS, sin duda se clasifica como un laboratorio especializado en ciberseguridad y, como tal, tiene potencial para formar equipos dedicados a manejar incidentes cibernéticos.

Por último, el eje IV enumera diez medidas mínimas para atender y proteger los intereses de la sociedad brasileña en el ciberespacio y garantizar un entorno cibernético confiable que asegure el crecimiento económico y tecnológico del país. La mitad de estas acciones están en consonancia con el potencial de CYBEROS. Dos de ellas, además, se alinean con el contexto académico en el que se enmarca CYBEROS: III – formación y capacitación técnico-profesional en ciberseguridad a una escala acorde con las necesidades nacionales; y IX – fomentar la creación de líneas de investigación para estudios de grado y posgrado (maestría y doctorado), así como la concesión de becas para la formación de especialistas y profesores brasileños en ciberseguridad. Otras dos iniciativas se refieren al potencial innovador de la herramienta, a la participación de una EED en su desarrollo y al financiamiento obtenido con recursos públicos, principalmente a través de FINEP: IV – reducción del retraso tecnológico del país en tecnologías emergentes y disruptivas mediante medidas gubernamentales afirmativas y progresivas; y X – fomento del desarrollo de productos, servicios y tecnologías nacionales destinados a mejorar la ciberseguridad en el país. Existe además el potencial de CYBEROS para contribuir a la acción: V – fomentar el desarrollo de la capacidad para la evaluación continua de la conformidad en materia de seguridad de los productos, servicios y tecnologías de ciberseguridad, capacidad que se analiza específicamente para la vertical de redes de radios tácticos en la sección 5.

4.3 PNSIC/ENSIC

La atención que el Estado brasileño le ha prestado a la seguridad de las IC se intensificó a finales de la primera década de los 2000, lo cual queda patente en la inclusión de esta preocupación en la primera versión de la END, en 2008. Las discusiones que se han sucedido desde entonces llevaron a la aprobación de la PNSIC (Brasil, 2018a) y la publicación del Decreto n.º 9.819, en 2019, que incluyó la protección de las IC en la lista de competencias de la Cámara de Relaciones Exteriores y Defensa Nacional del Consejo de Gobierno.

La PNSIC define las IC como instalaciones, servicios, bienes y sistemas cuya interrupción o destrucción, total o parcial, provoque un grave impacto social, ambiental, económico, político, internacional o en la seguridad del Estado y de la sociedad. También define la seguridad de las IC como un conjunto de medidas, tanto preventivas como reactivas, destinadas a preservar o restablecer la prestación de los servicios relacionados con las IC. Además, ofrece orientaciones para el esfuerzo conjunto que deben realizar los organismos y entidades de los sectores público y privado en este sentido.

En el decreto que establece la PNSIC se definió la necesidad de crear la ENSIC como uno de los instrumentos para la implementación de dicha política. La ENSIC, publicada en 2020 (Brasil, 2020b), consolida los conceptos e identifica los principales retos para la actividad de seguridad de las IC. En ella se establecieron cuatro ejes estructurales (EE), que constituyen los pilares

fundamentales para la eficacia de la actividad de seguridad de las IC. Estos ejes organizan los desafíos con el fin de crear una estrategia orgánicamente coherente y cohesionada, que debe impulsar el funcionamiento de la actividad de seguridad de las IC. Para cada EE, la ENSIC establece algunos objetivos estratégicos (OE), que se han dispuesto sin orden de prioridad, y que reflejan el enfoque estratégico para orientar los esfuerzos en la implementación de la PNSIC, además de señalar los resultados que se deben alcanzar. También se han desglosado los OE en varias iniciativas estratégicas (IE), que marcan el rumbo para el uso efectivo de dichos esfuerzos.

CYBEROS contribuye con dos EE de la ENSIC. La primera alineación se da con el EE 2 —Concientización y capacitación—, en su OE 2.2 —Fomentar la capacitación y la educación en seguridad de las IC, y, más específicamente, a través de la IE 2.2.1 —Fomentar las acciones de capacitación existentes en materia de defensa y seguridad de las IC. La creación del LaSC se dio precisamente en el contexto de las preocupaciones del Estado por la seguridad de las IC, y el desarrollo de CYBEROS, especialmente al tener en cuenta su adaptación a ese escenario, refuerza esa alineación.

La otra contribución a la ENSIC se da en relación con el EE 4 – Gestión de datos e información, en su OE 4.3 – Fomentar la adopción de recursos y procedimientos orientados a la Ciberseguridad en las IC, y a través de la IE 4.3.2 – Orientar a las IC a cumplir con la E-Ciber, principalmente lo dispuesto en su punto 2.3.5 – Elevar el nivel de protección de las IC nacionales. La contribución de CYBEROS a este trío EE/OE/IE es evidente, ya que el sistema constituye una herramienta de apoyo para estudios y capacitaciones cibernéticas realistas que respaldan la construcción de conocimiento especializado para la elaboración de procedimientos y planes de acción específicos que deberán adoptar las instituciones y el personal involucrado en la seguridad de las IC.

5 APORTES DE LA VERTICAL DE REDES DE RADIOS TÁCTICOS

Una de las principales innovaciones de CYBEROS radica en su vertical de redes de radios tácticos. Esta vertical incorpora un emulador de canal de radiofrecuencia capaz de aplicar degradaciones controladas a la señal, simulando entornos de campo complejos dentro de un laboratorio controlado, para realizar pruebas automatizadas con módulos físicos o virtualizados de RDS. De este modo, la vertical ofrece simulaciones realistas, realizando pruebas de desempeño, interoperabilidad y resiliencia en condiciones equivalentes a las de operaciones reales, ya sean civiles o militares. Además, permite un análisis exhaustivo de las vulnerabilidades, identificando de manera estructurada las amenazas críticas para las redes basadas en RDS. Contribuye a la estandarización y la certificación, ya que los resultados de las pruebas ayudan al desarrollo y la aplicación de un marco normativo para la Ciberseguridad. Amplía la gama de modelos para experimentos mediante el uso de escenarios híbridos que combinan ataques en el espectro electromagnético y amenazas cibernéticas. Por último, brinda apoyo técnico para dar respuesta oportuna a las demandas de seguridad y desempeño, lo que ayuda a preservar la superioridad informativa y la Capacidad de Comando y Control en escenarios altamente disputados.

La vertical de redes de radios tácticos agiliza la identificación de nuevas amenazas y la realización de pruebas de contramedidas para sistemas que dan soporte a las IC, mediante la implementación de funcionalidades para simular y analizar vulnerabilidades. Esto es fundamental para mejorar los dispositivos de seguridad y adoptar otros procedimientos de protección, ya que las amenazas cibernéticas evolucionan a

un ritmo acelerado. Además, la automatización de tareas optimiza los esfuerzos, lo que reduce los costos y el tiempo de respuesta ante incidentes. Dado que gran parte de las IC son operadas por empresas privadas, la vertical de redes de radios tácticos también puede facilitar la colaboración y el intercambio de información estandarizada entre los sectores público y privado, promoviendo así una gobernanza más integrada y eficaz de la ciberseguridad (Cravo, 2023; Gomes; Laginestra, 2023; Reis, 2024).

La experimentación ágil y automatizada que ofrece esta vertical acelera la I+D+i de nuevas capacidades en materia de Comunicaciones y Guerra Electrónica, lo que mantiene a Brasil a la vanguardia frente a posibles adversarios. Un país con capacidades cibernéticas avanzadas y una estrategia de defensa sólida se gana el respeto y destaca en el escenario internacional, lo que fortalece su posición diplomática y de cooperación (Cravo, 2023).

Como ya se ha señalado en la subsección 4.1, CYBEROS y sus verticales contribuyen al desarrollo de la capacitación cibernética en los ámbitos industrial y militar. Más específicamente, en lo que respecta a la vertical de redes de radios, permite la identificación proactiva y la mitigación de vulnerabilidades en el software y los protocolos, actividades fundamentales para mejorar la seguridad de las redes y los sistemas. Se pueden realizar simulaciones tanto de ataques en el espectro electromagnético como de amenazas cibernéticas para identificar vulnerabilidades antes de que se conviertan en incidentes reales, minimizando así las pérdidas y los daños que podrían ser catastróficos. Esto incluye los ataques de denegación de servicio, una de las principales amenazas consideradas, mediante la simulación de interferencia intencional (jamming) de radiofrecuencia o de la interrupción de servicios esenciales. A través de esta vertical de redes de radios tácticos, es posible realizar pruebas de formas de onda en sistemas de RDS virtualizados y físicos, lo que permite a las FFAA y al sector productivo evaluar la efectividad y la seguridad de las nuevas tecnologías de comunicación antes de su implementación. Esto acelera el desarrollo de soluciones nacionales y ayuda a reducir la dependencia tecnológica del exterior. El uso de esta vertical también permite aumentar la frecuencia y el realismo de ejercicios como el EGC, lo que permite poner a prueba la resiliencia de los sistemas tácticos de comunicación de manera continua y eficiente (Cravo, 2023; Gomes; Laginestra, 2023).

Al facilitar la simulación de escenarios complejos y los ejercicios de respuesta ante ataques, la vertical se convierte en una herramienta poderosa para capacitar y entrenar a los escasos recursos humanos, tanto de las FFAA como de otros sectores de la sociedad, en el ámbito de la Ciberseguridad (Fontes, 2024; Cravo, 2023). La vertical también es capaz de potenciar la Inteligencia Estratégica, generando conocimiento útil sobre tendencias y escenarios de amenazas cibernéticas de alta complejidad para técnicos y gestores en el ámbito de la Defensa Cibernética (Melo; Albuquerque; Mendonça, 2022).

Otra contribución de la vertical de redes de radios es su función como herramienta de experimentación y certificación, ya que puede promover una convergencia de esfuerzos más cohesionada entre los diversos actores de la sociedad y facilitar la implementación de políticas, directrices, reglamentos y requisitos específicos para la Ciberseguridad (Cravo, 2023; Gomes; Laginestra, 2023).

6 CONSIDERACIONES FINALES

Este artículo presentó reflexiones sobre las contribuciones de CYBEROS a la Defensa Nacional, un cyber range nacional diseñado a medida para la realización de ejercicios cibernéticos, tomando en cuenta escenarios realistas de protección de las IC, así como el uso de redes de radios

tácticos militares. El propio contexto en el que se desarrolla este sistema fue relevante en esta discusión, por diversos aspectos destacados a lo largo del texto.

Se presentaron CYBEROS y el entorno en el que se inserta, con el fin de destacar las características más relevantes que podrían estar relacionadas con las necesidades de la Defensa Nacional. Para que esta alineación fuera más objetiva, se llevó a cabo una investigación cualitativa centrada en documentos normativos de alto nivel de la Defensa Nacional, pertinentes a los temas principales que contextualizan el sistema en cuestión: Ciberseguridad y Protección de las IC. Con ello, se identificaron y analizaron tres pares de políticas y estrategias nacionales: PND/END; PNCiber/E-Ciber; y PNSIC/ENSIC. También se tomaron en cuenta, de manera complementaria, otras referencias relevantes a nivel táctico u operativo en el análisis de las posibles contribuciones específicas de la vertical de redes de radios tácticos vinculada al CYBEROS.

El sistema analizado en este trabajo contribuye a abordar varios de los principales desafíos para la CT&I en el ámbito de la Defensa, especialmente en el sector tecnológico estratégico cibernético, tales como la dependencia de tecnologías extranjeras, las restricciones tecnológicas y la necesidad de capacitar a recursos humanos calificados. Se pudo señalar con claridad de qué maneras el sistema contribuye o puede contribuir a diversos objetivos, estrategias y acciones estratégicas de los tres pares de documentos de alto nivel más relevantes en materia de Defensa Nacional. También se presentaron varias reflexiones complementarias sobre el potencial específico de la vertical de redes de radios tácticos para contribuir a la Defensa Nacional. En resumen, CYBEROS y sus verticales constituyen una herramienta que ayuda a Brasil a fortalecer su soberanía tecnológica y a posicionarse como un actor relevante en el escenario internacional de la Defensa, en el ámbito de la ciberseguridad.

AGRADECIMIENTOS

Este trabajo se realizó en el marco del proyecto ITSC2ICCOM, con el apoyo financiero de la *Financiadora de Estudos e Projetos* (FINEP) – Instrumento Contractual, Código n.º 01.22.0523.00 (Ref. 1890/22). También queremos dar un reconocimiento especial a los miembros del LaSC que contribuyeron directa o indirectamente haciendo posible este artículo.

REFERENCIAS

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. Disponible en: https://www.defesaemfoco.com.br/instituto-militar-de-engenharia-capacita-militares-para-cyber-flag-24-1/. Accedido en: 6 ago. 2025.

BARROS, M. Cyber Shield 2025: Defesa Cibernética do Brasil em destaque nos EUA. **Defesa em Foco**, 10 jun. 2025. Disponible en: https://www.defesaemfoco.com.br/cyber-shield-2025-defesa-cibernetica-do-brasil-em-destaque-nos-eua/. Accedido en: 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. Disponible en: https://www.eb.mil.br/web/noticias/w/exercito-coordena-maior-exercicio-cibernetico-do-hemisferio-sul. Accedido en: 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. Disponible en: https://lume.ufrgs.br/handle/10183/263232. Accedido en: 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**. ITS2ICCOM – Convênio FINEP-FAPEB Nº 01.22.0523.00**. Rio de Janeiro: FAPEB, 2022. Disponible en: https://fapeb.com.br/its2iccom-convenio-finep-fapeb-no-01-22-0523-00/. Accedido en: 6 ago. 2025.

FUNDAÇÃO DE APOIO À PESQUISA, DESENVOLVIMENTO E INOVAÇÃO DO EXÉRCITO BRASILEIRO – FAPEB. **Chamada Pública nº 05/2025 – ITS2ICCOM**: contratação de serviço de desenvolvimento e entrega de um orquestrador e provisionador de ambientes virtualizados heterogêneos completos. Rio de Janeiro: FAPEB, 2025. Disponible en: https://fapeb.com.br/wp-content/uploads/2025/06/EDITAL-PARA-CHAMADA-PUBLICA-PROJETO-ORQUESTRADOR-ERRATA-DE-CRONOGRAMA.pdf. Accedido en: 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. Disponible en: https://pgpse.ime.eb.br/. Accedido en: 6 ago. 2025.

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. Disponible en: https://tecnodefesa.com.br/rds-rondon-mais-um-integrante-da-familia-rds-defesa/. Accedido en: 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. Disponible en: 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. Accedido en: 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