ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
DIVISÃO DE ENSINO
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2025

CLÁUDIO RODRIGUES DE SOUZA JÚNIOR, Cap Esp Com

Padronização do Ensino em Defesa Cibernética: Estratégia para Integrar as Forças e Potencializar Talentos

Rio de Janeiro
2025

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
DIVISÃO DE ENSINO
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2025

CLÁUDIO RODRIGUES DE SOUZA JÚNIOR, Cap Esp Com

Padronização do Ensino em Defesa Cibernética: Estratégia para Integrar as Forças e Potencializar Talentos

Trabalho de conclusão de curso apresentado à Escola de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-Graduação *Lato Sensu* em Liderança com Ênfase em Gestão no COMAER.
Linha de Pesquisa: Ensino na Força Aérea
Orientador: Eduardo Mendes Marcondes, Maj Av

Rio de Janeiro
2025

CLÁUDIO RODRIGUES DE SOUZA JÚNIOR, Cap Esp Com

Padronização do Ensino em Defesa Cibernética: Estratégia para Integrar as Forças e Potencializar Talentos

Trabalho de conclusão de curso apresentado ao Curso de Aperfeiçoamento de Oficiais da Escola de Aperfeiçoamento de Oficiais da Aeronáutica.

Aprovado por:

_____

Presidente, Eduardo Mendes Marcondes, Maj Av - EAOAR

_____

Durval Aquino Mota, Cap Esp Sup Tec - GLOG-CG

Rio de Janeiro

2025

RESUMO

O ensaio aborda a crescente importância da Defesa Cibernética no cenário global, evidenciada por ataques significativos a países como Estônia, Geórgia e Irã. Diante dessas ameaças no ambiente digital, o Brasil passou a considerar o setor cibernético como prioridade em sua Estratégia Nacional de Defesa (END). Nesse contexto, o Ministério da Defesa (MD) instituiu um grupo de trabalho (GT) com a missão de propor diretrizes para o alinhamento do ensino de defesa cibernética nas Forças Armadas (FA). Com base nessas diretrizes, o trabalho propõe o alinhamento do Curso de Informática, ministrado na Escola de Especialistas de Aeronáutica (EEAR), às propostas sugeridas pelo GT do MD, para o ensino de defesa cibernética nas Forças Armadas, visando à padronização da capacitação, à promoção da interoperabilidade entre as forças e à formação de profissionais altamente qualificados. A implementação dessas propostas traria diversos benefícios à Força Aérea Brasileira (FAB), como maior integração com as demais Forças Armadas, operações conjuntas mais eficazes e a estimulação à qualificação de militares desde o início de suas carreiras. A longo prazo, a iniciativa contribuiria para o fortalecimento da resiliência institucional, o avanço da inovação tecnológica e a ampliação da segurança digital da FAB. Além disso, consolidaria o protagonismo da EEAR no processo de transformação educacional e no desenvolvimento de uma Força Aérea moderna, conectada e apta a enfrentar os desafios do século XXI.

Palavras-chave: defesa cibernética; interoperabilidade; capacitação militar; inovação tecnológica.

1 INTRODUÇÃO

Nunca na história a Defesa Cibernética foi tão debatida como nos dias atuais. Ataques cibernéticos sofridos por diversos países têm gerado um alerta global. Como exemplos desses ataques, podem ser citados o da Estônia, em 2007; o da Geórgia, em 2008 (Lobato; Kenkel, 2015); e o do Irã, em 2010, através do *"worm Stuxnet"*, um vírus que fora introduzido nos computadores da usina nuclear do país, que paralisou totalmente suas centrífugas de enriquecimento de urânio (Bernardes; Ávila, 2021).

A preocupação mundial com os impactos destrutivos dos ataques cibernéticos, seja para espionagem, destruição ou paralisação de ativos, cometimento de fraudes, roubos ou outros crimes cibernéticos, levou diversos países a implementarem ações governamentais para tratar o assunto. No cenário atual, o Brasil estabeleceu, em sua Estratégia Nacional de Defesa, o setor cibernético como essencial para a Defesa Nacional (Brasil, 2016).

Assim, pensando na capacitação de pessoal para atender à estratégia do setor cibernético, Ministério da Defesa, por meio da Portaria Nº 2.735/DIENS/DEPENS/SEPESD/SG-MD, de 14 de agosto de 2020, constituiu um Grupo de Trabalho com a finalidade de elaborar uma proposta para o alinhamento do ensino de defesa cibernética nas Forças Armadas (Brasil, 2020a) e que, em outubro de 2021, produziu um relatório com propostas para este alinhamento.

Neste contexto, a Escola de Especialistas de Aeronáutica, instituição militar encarregada da formação, adaptação e aprimoramento dos graduados do Comando da Aeronáutica (COMAER), pode participar ativamente do processo para atender as propostas e afirmar seu compromisso com a missão estratégica do setor cibernético.

Sendo assim, o presente trabalho defende o alinhamento do Curso de Informática, ministrado na EEAR, às propostas sugeridas pelo GT do MD, para o ensino de defesa cibernética nas Forças Armadas.

Para sustentar a tese, argumenta-se promover a capacitação padronizada em defesa cibernética para garantir a interoperabilidade das Forças Armadas. Essa iniciativa busca maximizar a eficiência dos treinamentos e operações conjuntas realizadas pelas três forças, enfrentando com maior eficácia as crescentes e complexas ameaças no domínio cibernético.

Outro aspecto importante a ser abordado é a estimulação à especialização em defesa cibernética na formação de profissionais qualificados. Essa estratégia também visa despertar o interesse dos egressos da EEAR pelo tema, contribuindo para a capacitação de novos especialistas na área.

2 DESENVOLVIMENTO

A iniciativa do Ministério da Defesa na criação do GT, que culminou na produção das propostas para o alinhamento do ensino de defesa cibernética nas três Forças Armadas, evidencia o reconhecimento da necessidade de padronizar e fortalecer a formação de profissionais militares aptos a atuar de forma coordenada diante das ameaças cibernéticas, cada vez mais sofisticadas e frequentes.

O relatório foi produzido pelos representantes das escolas de formação, aperfeiçoamento e altos estudos das três Forças Armadas, visando promover a integração entre elas no desenvolvimento curricular da defesa cibernética, buscando assegurar uma resposta unificada e eficiente a incidentes que comprometam a soberania nacional no ciberespaço. A criação desse relatório reflete a percepção de que a guerra cibernética já não é uma possibilidade futura, mas uma realidade presente, exigindo preparo técnico, atualização constante e uma doutrina comum para garantir a segurança dos sistemas militares e a resiliência das operações em ambiente digital.

2.1 INTEROPERABILIDADE NAS OPERAÇÕES DE DEFESA CIBERNÉTICA

A evolução constante das ameaças digitais e a crescente dependência tecnológica colocam a defesa cibernética no centro das preocupações estratégicas das nações. Para o Brasil, a proteção do ciberespaço tornou-se um componente essencial da soberania nacional, e as Forças Armadas desempenham papel protagonista nesse cenário.

Contudo, a complexidade das operações cibernéticas exige não apenas investimentos em infraestrutura, mas sobretudo o desenvolvimento de capacidades humanas integradas e padronizadas. Nesse contexto, a interoperabilidade entre os ramos das Forças Armadas é condição indispensável para uma atuação eficaz, e sua consolidação passa, inevitavelmente, pela revisão curricular nas instituições de ensino militar.

A interoperabilidade é definida como a capacidade de diferentes sistemas, unidades ou organizações atuarem em conjunto de forma eficaz. No campo cibernético, essa sinergia se torna ainda mais crítica diante da natureza descentralizada, veloz e assimétrica dos conflitos.

Assim, a Estratégia Nacional de Defesa aponta que a integração operacional é condição essencial à dissuasão eficaz em todos os ambientes de combate (Brasil, 2016). Dessa forma, não se trata apenas de alinhar ferramentas e protocolos, mas de criar uma cultura comum de defesa cibernética desde a formação inicial dos profissionais.

Nesse sentido, destaca-se a importância da atuação do Grupo de Trabalho instituído pelo Ministério da Defesa para tratar especificamente da padronização na formação e capacitação em defesa cibernética. A proposta do GT do MD encontra respaldo no Livro Branco de Defesa Nacional (Brasil, 2020b), que reforça a necessidade de uma capacitação continuada e alinhada entre as Forças Armadas, com vistas a garantir interoperabilidade plena.

Essa padronização curricular proposta tem como objetivo elevar o nível técnico dos profissionais, a fomentação de linguagem comum e doutrinas operacionais compatíveis, e garantir a interoperabilidade das três Forças. Ademais, a Estratégia Nacional de Segurança Cibernética (E-Ciber), lançada em 2020, destaca a formação de recursos humanos como um de seus pilares centrais, reconhecendo que a eficácia da defesa cibernética depende de profissionais preparados para atuar em ambientes de alta complexidade e com constante necessidade de atualização (Brasil, 2020c).

A E-Ciber sugere também a aproximação entre instituições militares e civis, promovendo intercâmbios que favoreçam inovação e maior integração de capacidades. Contudo, a realidade atual mostra que os currículos das escolas de formação militar ainda apresentam disparidades significativas entre os ramos. De acordo com Brasil (2023), essa fragmentação compromete a interoperabilidade e dificulta a atuação coordenada em incidentes cibernéticos reais.

A adoção das propostas do GT do MD representa, assim, uma oportunidade estratégica para superar essa lacuna, ao estabelecer uma base comum de formação, conforme o nível de atuação de seus egressos, que preparem os militares para a cooperação efetiva desde o início de suas carreiras. A interoperabilidade também pode ser fomentada por meio da realização de exercícios conjuntos, simulações e operações coordenadas em ambientes virtuais de guerra.

Conforme argumenta Rocha (2022), a formação em defesa cibernética deve ir além do ensino técnico e abordar cenários estratégicos, análise de risco, direito cibernético e governança digital.

Esses ambientes possibilitam o treinamento prático de equipes mistas, promovendo uma integração operacional mais sólida e fortalecendo a confiança entre os diferentes ramos. A formação em defesa cibernética deve ultrapassar o âmbito técnico, incluindo cenários estratégicos e análises de risco. Ao incorporar governança digital e direito cibernético nesses treinamentos, é possível fomentar uma perspectiva multidisciplinar indispensável para enfrentar a crescente complexidade das ameaças virtuais, garantindo conformidade regulatória

e alinhamento com os objetivos organizacionais.

Segundo Silva (2024), a interoperabilidade em defesa cibernética requer a combinação de doutrina, tecnologia e capacitação conjunta, sob uma lógica de contínuo aperfeiçoamento institucional.

Assim, a combinação de doutrina, tecnologia e capacitação conjunta permite alinhar diferentes áreas e equipes, criando um esforço coordenado contra ameaças. Sob uma lógica de contínuo aperfeiçoamento institucional, essa integração possibilita maior adaptação às rápidas mudanças no cenário de cibersegurança. A doutrina fornece a base estratégica, a tecnologia garante ferramentas avançadas, e a capacitação conjunta aprimora habilidades e fortalece a confiança entre os envolvidos. Essa abordagem abrangente é crucial para enfrentar os desafios dinâmicos da segurança cibernética moderna, promovendo resiliência e eficiência nas operações.

A capacitação padronizada, por meio de uma revisão curricular bem estruturada e abordagens pedagógicas modernas, alinhará o Curso de Informática da EEAR às diretrizes do MD para o ensino de defesa cibernética, promovendo a interoperabilidade e aumentando a eficácia das operações conjuntas das Forças Armadas frente às ameaças cibernéticas.

2.2 A ESTIMULAÇÃO À ESPECIALIZAÇÃO EM DEFESA CIBERNÉTICA

Em um cenário global cada vez mais marcado por ameaças digitais, a formação de especialistas em defesa cibernética tornou-se uma necessidade estratégica. Nesse contexto, as visitas direcionadas a centros de excelência, unidades operacionais e instituições educacionais voltadas à cibersegurança configuram-se como ferramentas eficazes para estimular vocações e promover a especialização na área.

Ao aproximar profissionais em formação dos ambientes reais de atuação, as visitas despertam o interesse, geram senso de pertencimento e ampliam a compreensão sobre a relevância e complexidade do setor. Conjuntamente à capacitação padronizada que visa garantir a operabilidade entre as Forças Armadas, a estimulação à especialização em defesa cibernética através da visita direcionada ao Centro de Defesa Cibernética da Aeronáutica (CDCAER) configura-se como uma ferramenta valiosa para a prospecção de profissionais mais capacitados para atuarem em um cenário cibernético cada vez mais agressivo.

Conhecer a doutrina e as ferramentas existentes de um centro destinado especificamente à defesa cibernética pode trazer benefícios tanto para o alinhamento do ensino nas Forças Armadas, quanto para a identificação de novos talentos. A visita ao

CDCAER possibilita a integração entre o conteúdo teórico ministrado na EEAR e as práticas e tecnologias reais utilizadas pela Força Aérea Brasileira, oferecendo uma experiência mais completa e alinhada aos desafios atuais da defesa cibernética.

Além disso, os alunos têm a oportunidade de observar a aplicação prática dos conceitos de segurança cibernética, compreendendo os protocolos, ferramentas e estratégias empregados na proteção dos sistemas da FAB.

Segundo Araújo e Quaresma (2014), as visitas guiadas possibilitam duas formas de interação dos alunos com o local explorado: uma baseada no conhecimento prévio adquirido em sala de aula, que se amplia com a experiência direta, e outra voltada à construção de saberes por meio da participação ativa, da observação e da percepção do ambiente.

Esse tipo de vivência estimula o interesse vocacional, contribui para a construção da identidade profissional e promove o desenvolvimento de competências específicas. Essas visitas desempenham um papel essencial no processo educativo, ao oferecer experiências que unem teoria e prática. Ademais, são ferramentas valiosas para formar alunos mais engajados e críticos, fortalecendo a conexão entre o ensino e a realidade e favorecendo o desenvolvimento integral do indivíduo.

Para Pessoa (2013), os resultados indicaram que a imersão proporcionada por ambientes virtuais contribui significativamente para o aumento da motivação dos alunos, devido às características de interação, múltiplas perspectivas e relevância das lições no ambiente real.

A prática em ambientes operacionais facilita o aprendizado ao conectar teoria e prática de maneira eficiente. No contexto da segurança da informação, essas vivências ajudam a identificar desafios e desenvolver soluções assertivas. Assim, a imersão ativa incentiva o engajamento e consolida o conhecimento técnico complexo. Essencialmente, essas visitas ajudam a FAB a reconhecer talentos promissores, apoiando sua formação especializada e reduzindo a necessidade de buscar profissionais fora da instituição.

Já para Pavão, Rocha e Bernardi (2019), essa interação facilita o reconhecimento de um grupo de pares mais diversificado do que aquele encontrado na escola regular, incentivando a continuidade dos estudos e o desenvolvimento de suas habilidades.

As visitas direcionadas criam um ambiente de aprendizado dinâmico, permitindo que os alunos interajam com profissionais qualificados e colegas de diversas formações. Essa convivência amplia a diversidade de relações e promove a troca de experiências, estimulando a continuidade dos estudos e o desenvolvimento de habilidades essenciais para o profissional do futuro.

Em vista do exposto, iniciativas como à estimulação à especialização, através da visita direcionada, contribuirá para o alinhamento do Curso de Informática, ministrado na EEAR, às propostas sugeridas pelo GT do MD, para o ensino de defesa cibernética nas Forças Armadas, tornando possível a formação de profissionais qualificados, despertando o interesse dos egressos pelo tema e contribuindo para a capacitação de novos especialistas na área.

3 CONCLUSÃO

Com o avanço das tecnologias e o aumento das ameaças digitais, a defesa cibernética tornou-se prioridade na segurança nacional. O Brasil, atento a essa realidade, incluiu o setor em sua Estratégia Nacional de Defesa e, por meio de um Grupo de Trabalho do Ministério da Defesa, propôs diretrizes comuns às três Forças. Nesse cenário, a EEAR se destaca como peça estratégica, podendo, através do curso de informática, fortalecer a capacidade cibernética da FAB e contribuir para uma doutrina nacional de defesa digital.

A problemática abordada neste trabalho foi à falta de uniformidade curricular entre as escolas de formação das Forças Armadas, fator que compromete a interoperabilidade e a resposta conjunta a ameaças cibernéticas cada vez mais complexas. Assim, a tese defendida propôs o alinhamento do Curso de Informática da EEAR às diretrizes sugeridas pelo GT do MD, como forma de garantir coesão doutrinária e operacional. O primeiro argumento sustentou que uma capacitação padronizada atua para o alinhamento do ensino de defesa cibernética, sendo fundamental para a interoperabilidade entre Exército, Marinha e Aeronáutica, permitindo que essas Forças atuem de forma integrada e eficiente em missões conjuntas.

O segundo destacou a importância da estimulação à especialização para o alinhamento do ensino de defesa cibernética, proporcionando profissionais mais capacitados para atuarem na área. Neste ínterim, experiências práticas em centros de excelência em defesa cibernética, como o CDCAER, despertariam o interesse vocacional, promoveriam o engajamento e facilitariam a identificação de talentos com alto potencial para atuação futura no setor cibernético.

A longo prazo, a proposta poderia ser estendida aos demais cursos ministrados na EEAR, resultando em maior resiliência institucional, capacidade de inovação tecnológica e segurança dos ativos digitais da FAB. Adicionalmente, conferiria à instituição protagonismo no processo de transformação educacional e reafirmaria seu papel como pilar fundamental no desenvolvimento de uma FA moderna, conectada e preparada para os desafios do século XXI.

REFERÊNCIAS

ARAÚJO, G. D.; QUARESMA, A. G. Visitas guiadas e visitas técnicas: tecnologia de aprendizagem no contexto educacional. **Revista Competência**, Porto Alegre, v. 7, n. 2, p. 29–51, 2014. Disponível em: https://www.senacrs.com.br/hotsite/pdf/revista_competencia_2014_2_DEZ.pdf. Acesso em: 4 abr. 2025.

BERNARDES, A. R.; ÁVILA, K. L. B. de. O ato de guerra e o ataque cibernético: o caso STUXNET na visão de Clausewitz. **Defesa em Foco**, 2021. Disponível em: https://www.defesaemfoco.com.br/o-ato-de-guerra-e-o-ataque-cibernetico-o-caso-stuxnet-na-visao-de-clausewitz/. Acesso em: 4 abr. 2025.

BRASIL. **Estratégia Nacional de Defesa**. Brasília: Ministério da Defesa, 2016. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/estado_e_defesa/pnd_end_congresso_.pdf. Acesso em: 23 mar 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Decreto nº 10.222, de 5 de fevereiro de 2020c. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**: seção 1, Brasília, DF, n. 26, p.6, 6 fev. 2020c. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 9 abr. 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Revisão da Capacidade de Defesa Cibernética nas Forças Armadas**. Brasília: GSI, 2023. Disponível em: file:///C:/Users/claud/Downloads/CMM%20report%20Brazil%202023_final_PT%20(1).pdf. Acesso em: 23 mar 2025.

BRASIL. **Livro Branco de Defesa Nacional**. Brasília: Ministério da Defesa, 2020b. https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf. Acesso em: 23 mar 2025.

BRASIL. Ministério da Defesa. Secretaria de Pessoal, Ensino, Saúde e Desporto. Portaria nº 2.735/DIENS/DEPENS/SEPESD/SG-MD, de 14 de agosto de 2020. Constitui o Grupo de Trabalho (GT), com a finalidade de elaborar propostas para o alinhamento do ensino de defesa cibernética nas Forças Armadas. **Diário Oficial da União**: seção 2, Brasília, DF, n. 161, p. 8, 21 ago. 2020a. Disponível em: https://mdlegis.defesa.gov.br/norma_html/?NUM=2735&ANO=2020&SER=A. Acesso em: 28 mar 2025.

LOBATO, L.; KENKEL, K. M. A ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra. **Contexto Internacional (PUC)**, Rio de Janeiro, v. 37, n. 2, p. 629–660, maio/ago., 2015. Disponível em: file:///C:/Users/claud/OneDrive/Documentos/CAP%201%C2%BA%202025/TCC/REFER%C3%8ANCIAS/Lobato%20e%20Kenkel%20(2015)%20-%20(CLARKE%3BKNAKE,2012).pdf. Acesso em: 6 abr 2025.

PAVÃO, A. C. O.; ROCHA, K. M.; BERNARDI, G. (Orgs.). **Tecnologias educacionais em rede**: produtos e práticas inovadoras. Santa Maria: FACOS-UFSM, 2019. Disponível em: Tecnologias-Educacionais-em-Rede-Produtos-e-práticas-inovadoras.pdf. Acesso em: 5 abr 2025.

PESSOA, F. M. M. **Aprendizagem imersiva em mundos virtuais**. 2013. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2013. f . 77. Disponível em: https://repositorio.ufpe.br/handle/123456789/11979. Acesso em: 5 abr. 2025.

ROCHA, H. R. da. **Governança Securitária do Ciberespaço**: Questões sobre Segurança e Defesa. 2022. Dissertação (Mestrado em Ciências Militares) — Escola de Comando e Estado Maior do Exército (ECEME), Rio de Janeiro, 2022. f. 122. Disponível em: file:///C:/Users/claud/OneDrive/Documentos/CAP%201%C2%BA%202025/TCC/REFER%C3%8ANCIAS/Rocha%20(2022).pdf. Acesso em: 9 abr 2025.

SILVA, L. G. L. da. **Segurança Cibernética no Brasil**: Uma Análise dos Fatores Institucionais que Precedem a Política de Segurança Cibernética entre 2008–2020. 2024. Dissertação (Mestrado em Relações Internacionais) – Universidade Federal da Integração Latino-Americana (UNILA), Foz do Iguaçu, 2024. f. 8. Disponível em: https://dspace.unila.edu.br/server/api/core/bitstreams/33f8e929-24b2-4c3e-9641-26deb78dc541/content. Acesso em: 5 abr. 2025.