ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA

DIVISÃO DE ENSINO

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 3º/2024

YÚRI BURLE **ISHIDA**, Cap Inf

Segurança Cibernética para os alunos do Curso de Preparação de Oficiais da Reserva da Aeronáutica

Rio de Janeiro

2024

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
DIVISÃO DE ENSINO
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 3º/2024

YÚRI BURLE **ISHIDA**, Cap Inf

Segurança Cibernética para os alunos do Curso de Preparação de Oficiais da Reserva da Aeronáutica

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: Guerra Cibernética
Orientador: Eduardo Mendes Marcondes, Maj Av

Rio de Janeiro
2024

YÚRI BURLE **ISHIDA**, Cap Inf

Segurança Cibernética para os alunos do Curso de Preparação de Oficiais da Reserva da Aeronáutica

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

Aprovado por:

_____

Presidente, Márcio Henrique Teixeira de Souza, Ten Cel Av - EAOAR

_____

Eduardo Mendes Marcondes, Maj Av - EAOAR

Rio de Janeiro

2024

RESUMO

A expansão do ciberespaço e a crescente dependência da internet trazem desafios significativos para a segurança das infraestruturas críticas, especialmente no contexto das Forças Armadas, onde a proteção de dados e sistemas sensíveis é fundamental. O Departamento de Ciência e Tecnologia Aeroespacial (DCTA) é responsável pelo desenvolvimento de tecnologias aeroespaciais e um alvo potencial de ataques cibernéticos, cujas consequências podem ser incalculáveis para a soberania nacional. Diante do cenário apresentado, este ensaio defende a implementação da disciplina de Segurança Cibernética durante a fase de adaptação do 1º ano do Curso de Preparação de Oficiais da Reserva da Aeronáutica (CPORAer). Para sustentar essa tese, argumenta-se que desenvolver a mentalidade de segurança cibernética nos alunos do 1º ano do ITA ajudará a evitar a cooptação deles como agentes causadores da falha de segurança interna. Além disso, evitará que agentes externos explorem as redes do DCTA. A instrução em segurança cibernética permitirá que os alunos reconheçam ameaças, fortaleçam a segurança dos sistemas internos e disseminem o conhecimento sobre o tema em suas equipes, contribuindo para a proteção das infraestruturas críticas em todo o território nacional e para o fortalecimento da segurança nacional frente às novas ameaças do ciberespaço.

Palavras-chave: soberania nacional; segurança cibernética; ciberespaço; infraestruturas críticas.

1 INTRODUÇÃO

A internet é um sistema de comunicação mundial que não é controlado por uma organização. O seu desenvolvimento, desde a sua criação até os dias atuais, demandou desenvolvimento de protocolos para a comunicação entre redes diferentes (Tanenbaum, Feamster, Wetherall, 2021).

A expansão da internet possibilitou a conexão global, a produção de dados, o acesso às informações de maneira quase que instantânea e o desenvolvimento do ciberespaço, como forma de utilizar o poder de modo a produzir resultados fora do meio tecnológico (Tristão *et al*., 2019). Esse novo cenário coloca em risco toda a Infraestrutura Crítica que, segundo Branquinho e Branquinho (2021), é a infraestrutura que mantém a sociedade e a economia funcionando incluindo as forças armadas, ou seja, todas as atividades que mesmo imperceptíveis são essenciais para o país.

No âmbito do Comando da Aeronáutica (COMAER), o DCTA é o órgão responsável pelo desenvolvimento de tecnologias críticas nos campos de fomento industrial, metrologia, gestão da inovação, propriedade intelectual, transferência de tecnologia compensação comercial, industrial e tecnológica (*offset*), relacionados com os setores aeronáutico, espacial e de defesa (Brasil, 2024).

Anualmente, através do ITA, o DCTA admite nas fileiras da Força Aérea Brasileira (FAB) mais de cem novos alunos nos cursos de engenharia ofertados por aquele Instituto, os quais são matriculados no CPORAer e passam a ter acesso aos mais diversos sistemas da FAB e apesar de poderem acessá-los, eles não possuem qualquer instrução acerca de Segurança Cibernética durante o período de adaptação do curso.

Branquinho e Branquinho afirmam que o ser humano é o elo mais fraco na segurança da informação e que os profissionais das empresas podem se tornar uma ameaça se não tiverem instrução e conscientização acerca de segurança cibernética (2021).

Assim, este ensaio defende a implementação da disciplina de Segurança Cibernética durante a fase de adaptação do 1º ano do Curso de Preparação de Oficiais da Reserva da Aeronáutica (CPORAer).

Para sustentar essa tese, argumenta-se que desenvolver a mentalidade de segurança cibernética nos alunos do 1º ano do ITA ajudará a evitar a cooptação deles como agentes causadores da falha de segurança interna**.** Além disso, evitará que agentes externos explorem as redes do DCTA.

2 DESENVOLVIMENTO

Sistemas conectados à internet trazem agilidade na transmissão de dados, no compartilhamento de informações e na resolução de problemas, em contrapartida deixam expostas portas de entrada para ataques cibernéticos e roubos de informações classificadas, que podem trazer consequências à soberania nacional (Correa, 2021).

A infraestrutura subordinada ao DCTA para o desenvolvimento de sua atividade fim conta com diversos Institutos e Centros, todos interligados, de alguma maneira, pelos sistemas internos, pela rede interna (*intranet*) e pela internet. Muitos projetos desenvolvidos naquele Departamento são classificados por diversos fatores, como segurança e desenvolvimento nacional, fomento industrial entre outros (DCTA, 2023).

2.1 CONHECER SEGURANÇA CIBERNÉTICA PARA EVITAR FALHAS HUMANAS

Anualmente o DCTA admite nos cursos de engenharia do ITA centenas de novos militares nas fileiras da FAB. Conforme preveem os §§ 1º e 2º, do Art. 3º, do Decreto nº 76.323, de 22 de setembro de 1975, todos os alunos que não forem Aspirantes-a-Oficial da reserva das Forças Armadas devem ser matriculados como alunos no Centro de Preparação de Oficiais da Reserva da Aeronáutica de São José dos Campos (CPORAer-SJ) para participarem do CPORAer (Brasil, 2024).

Após a conclusão do período de adaptação do CPORAer, os alunos recém-admitidos passam a ter acesso à rede e aos mais diversos sistemas da FAB, porém, durante a adaptação e ao longo dos cinco anos de formação no CPORAer-SJ, não há previsão de lhes ser ensinada nenhuma matéria que aborde o assunto de segurança cibernética, tornando-os alvos para cooptação e possíveis agentes causadores de falhas internas, ainda que de forma não intencional. Agrava-se o fato de que alguns alunos, após a conclusão do CPORAer no primeiro ano, deixam de ser militares, mas continuam tendo acesso a dispositivos conectados à rede intranet.

Além disso, no início do ciclo básico do ITA (primeiro ano após a conclusão da adaptação) os alunos podem participar das mais diversas iniciativas ofertadas pelo Centro Acadêmico Santos Dumont (CASD), como por exemplo, a ITAndroids e a ITA *Rocket* (CASD, [s.d.]). Essas iniciativas competem constantemente em eventos nacionais e internacionais, como a *Robocup* que, em 2024, ocorreu na Holanda e contou com uma equipe de alunos de todos os anos do ITA (ITAEX, 2024).

Ao participarem deste tipo de evento, normalmente desacompanhados de um militar responsável, os alunos ficam suscetíveis a abordagens do público presente na competição, inclusive podendo receber diversos tipos de brindes, como por exemplo um *pen drive* (unidade *flash usb*). A falta de mentalidade de segurança Cibernética, de não se entenderem como um elo na segurança da informação e como um ativo valioso para os cibercriminosos, pode levá-los a conectarem o equipamento em um computador da biblioteca do Instituto e deixar uma porta aberta no ciberespaço para invasão alheia.

Segundo Mann (2008):

> A segurança da informação está relacionada a pessoas, apesar de, na maioria dos casos, a proteção estar focada em medidas defensivas técnicas. [...] Toda pesquisa séria sobre os métodos usados pelos agressores para comprometer sistemas demonstra que o elemento humano é crucial para a maioria dos ataques bem-sucedidos. Em muitos casos o agressor nem precisou encontrar vulnerabilidades técnicas (Mann, 2008, p. 9).

Depreende-se da afirmação do autor que, tão importante quanto investir nos sistemas de segurança cibernética, é investir na instrução das pessoas que fazem parte deste sistema por serem os elementos cruciais no sucesso dos ataques.

Branquinho e Branquinho (2021) afirmam que os seres humanos podem enfraquecer os sistemas de segurança ao levarem seus próprios dispositivos para o setor de trabalho, e que isso pode ocorrer por desconhecimento ou descuido.

Assim, fica claro a necessidade de fazer os alunos entenderem que passam a ser parte de uma estrutura crítica à sociedade e de se introduzir os conceitos de segurança cibernética logo que são incorporados à FAB e antes de possuírem acesso aos sistemas e à rede interna da Força Aérea.

Esta conscientização fará com que eles se enxerguem como elo da segurança cibernética, conheçam as formas mais utilizadas na cooptação de agentes internos e sejam capazes de identificar possíveis ameaças. Adicionalmente, seriam capazes de desenvolver mentalidade de segurança contra esses ataques, consequentemente, deixando de ser o elo mais fraco na estrutura de segurança cibernética, mesmo quando estiverem desacompanhados em competições internacionais ou quando deixarem de ser militares ao término do primeiro ano do CPORAer.

Diante do exposto, fica claro que a implementação da disciplina de Segurança Cibernética durante a fase de adaptação do 1º ano do Curso de Preparação de Oficiais da Reserva da Aeronáutica (CPORAer) se faz necessária. Este reforço no preparo inicial de desenvolver a mentalidade de segurança cibernética nos alunos do 1º ano do ITA ajudará a evitar a cooptação deles como agentes causadores da falha de segurança interna.

2.2 SEGURANÇA CIBERNÉTICA PARA PROTEÇÃO DO DCTA

Roumani e Alraee (2024) definem Infraestrutura Crítica como a espinha dorsal para o funcionamento da sociedade incluindo a economia, a segurança e a saúde. Pode-se incluir nesse escopo as atividades relacionadas à segurança e à soberania do país como os projetos estratégicos coordenados pelo DCTA e desenvolvidos pelos seus diversos Institutos. Além disso, o DCTA é o órgão da FAB responsável pela coordenação e implantação de sistemas espaciais e pela definição das estratégias de implantação, integração e financiamento de sistemas espaciais relativos à defesa (Brasil, 2024).

Instituições de nível superior se tornaram alvos visados por cibercriminosos por causa de suas pesquisas e dados pessoais sensíveis (Ulven e Wangen, 2021). Segundo notícia publicada no sítio da CISO Advisor (2024), os setores de educação e pesquisa são os principais alvos dos ataques no mundo, seguidos dos setores do governo e das Forças Armadas que, somados, ultrapassam cinco mil ataques por semana, refletindo riscos de espionagem cibernética e interrupção de serviços a nível de Estado.

As consequências de ciberataques podem incluir perdas financeiras, interrupção do funcionamento de infraestruturas críticas e violação da privacidade e da confidencialidade dos dados (Kravchenco, *et al.*, 2024). Alguns projetos desenvolvidos ou gerenciados pelo DCTA possuem algum grau de classificação e o acesso indevido a esses projetos pode culminar em uma perda inestimável de conhecimento e avanço tecnológico, além de comprometer a soberania do Brasil.

Após a conclusão do curso de Engenharia, os Oficiais formados no CPORAer-SJ são distribuídos nas mais diversas organizações da FAB. A turma que se formou em 2023, por exemplo, era composta por 36 engenheiros militares de todas as especialidades ofertadas no ITA. Dos 36, 22 foram designados para organizações que atuam diretamente com o desenvolvimento e a implementação dos sistemas da FAB, os Centros de Computação da Aeronáutica (CCA) ou para Institutos que trabalham com pesquisa e desenvolvimento aeroespacial.

Como forma de exemplificar ataques cibernéticos à Infraestrutura Crítica, podemos citar os ataques ocorridos via e-mail funcional dos militares na plataforma Zimbra. Os ataques consistiram em um tipo de abordagem conhecida como *Phishing*, que consiste no envio de mensagens eletrônicas mal intencionadas, com intuito de enganar o destinatário instalando um software malicioso (*malware)* em seu dispositivo (Silva, 2023).

Com o *malware* instalado, o cibercriminoso pode acessar, não só o equipamento afetado, mas toda a infraestrutura de rede da organização e coletar informações importantes que nela tramitam.

O comprometimento da infraestrutura de rede do DCTA pode levar à perda significativa das inovações tecnológicas e, consequentemente, comprometer não só os sistemas, projetos estratégicos e dados pessoais daquele Departamento, como também de toda a FAB.

A manutenção da segurança, confidencialidade e integridade dos sistemas e projetos desenvolvidos no DCTA depende, entre outras coisas, da capacidade de seus empregados, civis e militares, manterem-se em constante estado de alerta reconhecendo que são fundamentais para a salvaguarda das informações e tecnologias desenvolvidas e aprimoradas naquele Departamento.

Os engenheiros formados no ITA, ao longo de sua formação, passam pelos diversos Institutos do DCTA, inclusive para o estágio obrigatório e trabalho de graduação. Com exceção dos militares do curso de Engenharia de Computação, que tem matéria relacionada à Segurança Cibernética, os demais não têm nenhuma matéria que aborde o assunto, deixando para os militares a responsabilidade de buscar conhecimento que os preparem a não comprometer a rede e fortalecer a cadeia de Segurança Cibernética, bem como impedir a exploração dos recursos da FAB por cibercriminosos.

Além disso, após a sua formação, os oficiais assumem cargos em funções nas quais precisam liderar uma equipe composta por civis e militares. Com o conhecimento prévio de segurança cibernética, eles poderiam atuar como fiscalizadores das ações de seus subordinados e disseminadores do conhecimento a fim de evitar que as redes e sistemas do DCTA sejam exploradas por inimigos externos.

Diante do exposto, podemos verificar que a implementação da disciplina de Segurança Cibernética durante a fase de adaptação do 1º ano do Curso de Preparação de Oficiais da Reserva da Aeronáutica (CPORAer) evitará que agentes externos explorem as redes do DCTA.

3 CONCLUSÃO

A expansão do ciberespaço e a dependência da internet têm gerado uma série de desafios à segurança das infraestruturas críticas, que são fundamentais para o funcionamento da sociedade e do Estado. No contexto das Forças Armadas, a proteção de dados e sistemas sensíveis torna-se ainda mais preocupante diante da crescente ameaça de ataques cibernéticos. O DCTA, por ser o Órgão das Forças Armadas responsável por desenvolver tecnologias

aeroespaciais, é um alvo em potencial e, se afetado, pode refletir em perdas inestimáveis para o Brasil.

Os alunos que ingressam no ITA para realizar a graduação em engenharia, após a conclusão do período de adaptação no CPORAer, têm acesso a diversos sistemas da FAB sem terem sido previamente instruídos sobre segurança cibernética, participam de eventos internacionais, por vezes desacompanhados, tornando-os suscetíveis à cooptação por agentes externos e podendo se tornar o vetor da falha de segurança. Diante desse cenário, este ensaio defendeu a implementação da disciplina de Segurança Cibernética durante a fase de adaptação do 1º ano do Curso de Preparação de Oficiais da Reserva da Aeronáutica (CPORAer).

Para sustentar essa tese, argumentou-se que desenvolver a mentalidade de segurança cibernética nos alunos do 1º ano do ITA ajudará a evitar a cooptação deles como agentes causadores da falha de segurança interna. Foi abordada a vulnerabilidade humana como elo mais fraco na cadeia de segurança e que a falta de preparo dos alunos no que se refere à segurança cibernética os expõe a situações de cooptação, o que pode comprometer a segurança dos sistemas internos. O ensino da disciplina possibilitará que eles reconheçam ameaças e evitem se tornar o vetor de falhas internas.

Além disso, mostrou-se que o ensino da disciplina durante o período de adaptação do CPORAer evitará que agentes externos explorem as redes do DCTA. A instrução em segurança cibernética fortalecerá a capacidade dos alunos em identificar e prevenir tentativas de espionagem e disseminar em suas equipes o conhecimento acerca do assunto.

As discussões levantadas neste ensaio têm implicações que vão além do DCTA. A inclusão da disciplina de segurança cibernética como matéria básica nos cursos de graduação em todo o Brasil promoverá uma cultura de segurança mais robusta em nível nacional, ajudando a prevenir vazamentos de informações classificadas e tecnologias estratégicas, e fortalecendo, assim, a soberania nacional.

Ao capacitar os alunos para reconhecer ameaças, proteger sistemas internos e difundir o conhecimento sobre segurança cibernética em suas equipes, essa instrução contribuirá para a salvaguarda das infraestruturas críticas em todo o país. Além disso, reforçará a segurança nacional frente aos desafios emergentes no ciberespaço.

REFERÊNCIAS

BRANQUINHO, T.; BRANQUINHO M. **Segurança cibernética industrial:** as infraestruturas críticas correm perigo. Aprenda a proteger redes e sistemas de controle com uma metodologia comprovada na prática. Rio de Janeiro: Alta Books, 2021.

BRASIL. [Decreto (1975)]. **Regulamenta a Lei nº 6.165, de 9 de dezembro de 1974**, que dispõe sobre a formação de Oficiais Engenheiros para o Corpo de Oficiais da Aeronáutica, da Ativa e dá outras providências. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1970-1979/d76323.htm#:~:text=DECRETO%20No%2076.323%2C%20DE,Ativa%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Acesso em: 29 set. 2024.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria GABAER n. 1.490/GC3. Aprova o Regulamento do Departamento de Ciência e Tecnologia Aeroespacial. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 157, p. 120-128, 2024. Disponível em: https://www.sislaer.fab.mil.br/. Acesso em: 30 set. 2024

BRASIL. Sobre o DCTA. **DCTA**, 30 ago. 2023**.** Disponível em: https://www.dcta.mil.br/index.php/historico. Acesso em: 4 out. 2024.

CASD. As iniciativas. **CASD**, [s.d.]. Disponível em: https://www.casd.ita.br/iniciativas/. Acesso em: 29 set. 2024.

CISO ADVISOR. **Ataques crescem cerca de 70% no Brasil em um ano**. Disponível em: https://www.cisoadvisor.com.br/ataques-crescem-cerca-de-70-no-brasil-em-um-ano/#:~:text=O%20aumento%20global%20dos%20ataques,ao%20primeiro%20trimestre%20de%202024. Acessado em: 30 set. 2024.

CORREA, J. A. Defesa e segurança nacional no espaço cibernético. **CEDESEN**, São Paulo, 6 abr. 2021. Disponível em: https://cedesen.com.br/defesa-e-seguranca-nacional-no-espaco-cibernetico/. Acesso em: 4 out. 2024.

ITAEX. **ITAndroids mostra potencial e inovação com bons resultados na RoboCup** 2024. Disponível em: https://itaex.com.br/blog/equipe-da-itandroids-mostra-potencial-e-inovacao-com-bons-resultados-na-robocup-2024/. Acesso em 29 set. 2024.

KRAVCHENKO, O.; VEKLYCH, V.; KRYKHIVSKYI, M.; MADRYHA, T. Cybersecurity in the face of information warfare and cyberattacks. **Multidisciplinary Science Journal**, *[S. l.]*, v. 6, p. 2024ss0219, 2024. DOI: 10.31893/multiscience.2024ss0219. Disponível em: https://malque.pub/ojs/index.php/msj/article/view/1938. Acesso em: 29 set. 2024.

MANN, I. **Engenharia social**. São Paulo: Blucher, 2011.

ROUMANI, Y; ALRAEE, M. Examining the factors that impact the severity of cyberattacks on critical infrastructures. **Computers & Security**, v. 148, p. 104074, 2025. DOI: 10.1016/j.cose.2024.104074. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167404824003791?via%3Dihub . Acesso em: 30 set. 2024.

SILVA, M. B. F. da. **Cibersegurança**: uma visão panorâmica sobre a segurança da informação na internet. Rio de Janeiro: Freitas Bastos, 2023.

TANENBAUM, A. FEAMSTER, N.; WETHERAL, D. **Redes de computadores**. 6 ed. Porto Alegre: Grupo Educação S.A., 2021.

TRISTÃO, W. V. M.; CASSIANI A. G.; SANTOS, L. A.; FIGUEIREDO, M. L. S. de; REZENDE, M. C.; PERES, M. B. O Papel da Defesa Nacional em Casos de Ataques Cibernéticos: Uma Análise sobre a Necessidade de Protocolo(s) de Prevenção e Atuação. **Congresso acadêmico sobre defesa nacional**. Rio de Janeiro, 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/ensino-e-pesquisa/copy_of_defesa-e-academia/congresso-academico-sobre-defesa-nacional/artigos-e-palestras-do-16-congresso-academico-sobre-defesa-nacional. Acesso em 30 set. 2024.

ULVEN, J. B.; WANGEN, G. A systematic review of cybersecurity risks in higher education. **Future Internet**, v. 13, n. 2, p. 39, 2021. DOI: 10.3390/fi13020039. Disponível em: https://www.mdpi.com/1999-5903/13/2/39. Acesso em 30 set. 2024