ISSN: 1983 7402 ITA, 26 a 28 SET 2023

Uma Análise de Segurança Cibernética em Sistemas Embarcados de Aeronaves Militares (SEAM)

Tiago Josué Diedrich[1] e Oswaldo Segundo da Costa Neto[1]
[1] Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER), Brasília/DF - Brasil

***Resumo*— Neste artigo, os autores concentram-se na análise do número de ameaças cibernéticas contra aeronaves militares, identificando vulnerabilidades que podem estar associadas a processadores e controladores embarcados, ou Sistemas Embarcados. Assim, propõe-se o termo "Sistemas Embarcados de Aeronaves Militares"(SEAM) para se referir aos sistemas operacionais críticos usados em aviões militares, considerando sua possível vulnerabilidade a ataques cibernéticos durante operações militares em tempos de paz e de guerra. Medidas como criptografia, autenticação e monitoramento em tempo real são destacadas para reduzir as vulnerabilidades dos SEAM. A importância de abordagens regulatórias e adoção de padrões internacionais também são enfatizadas para fortalecer a segurança dos sistemas. Conclui-se que investimentos em tecnologia militar e leis específicas são necessários para proteger os SEAM contra ameaças cibernéticas sofisticadas, visando eficácia das operações militares em geral.**

***Palavras-Chave*— Sistemas Embarcados, Aeronaves Militares e Segurança Cibernética.**

I. Introdução

Os avanços na tecnologia de sistemas embarcados têm impulsionado sua proliferação em várias aplicações críticas, abrangendo setores como transporte, energia, saúde e indústria [1]. Observa-se, assim, que a capacidade de integrar esses sistemas a redes e infraestruturas existentes trouxe benefícios consideráveis em termos de eficiência, automação e tomada de decisões inteligentes. No entanto, essa crescente interconectividade de sistemas embarcados também trouxe consigo um aumento significativo nos riscos de ataques cibernéticos, expondo esses sistemas a ameaças que podem comprometer sua operação segura e confiável.

Para contextualizar, entende-se que um Sistemas Embarcados de Aeronaves Militares (SEAM) é definido como um sistema de computador projetado para executar funções específicas dedicadas, geralmente, sob restrições de computação em tempo real. Ademais, relaciona-se o termo "embarcado" porque é incorporado como parte de um dispositivo ou sistema completo [1].

Nesse contexto, os SEAM desempenham um papel fundamental na segurança e na eficácia das Operações Militares e Forças-Tarefa. Esses sistemas permeiam o ambiente responsável pelo controle de voo, comunicação, sistemas de armas e suporte à decisão nas aeronaves militares [2].

Dada a importância estratégica desses sistemas, entende-se que eles se tornam alvos potenciais para ataques cibernéticos maliciosos, o que pode resultar em consequências graves, como perda de vidas e/ou paralisação nas atividades militares em comento.

Adicionalmente, é comum que muitos sistemas permaneçam em uso por décadas, tornando-se sistemas legados integrados em sistemas críticos, como os sistemas de controle de voo e de controle de tiro.

Para suprir as limitações funcionais de conectividade e facilidade de uso desses sistemas herdados, é comum a utilização de tablets e laptops modernos. No entanto, quando há interconexão e interoperabilidade entre esses sistemas legados e os meios modernos de informação, surgem potenciais riscos de segurança cibernética [3].

De fato, a aplicação de estratégias de proteção cibernética aprimoradas se torna fundamental para fortalecer a segurança dos SEAM. Essas estratégias visam prevenir, detectar e responder a ataques cibernéticos, além de proteger ativos e informações sensíveis envolvidas nos sistemas críticos [4]. Logo, ao implementar medidas robustas de segurança cibernética, é possível garantir o funcionamento adequado, confiável e seguro dos SEAM, mitigando os riscos associados a uma interconectividade mais expandida.

Diante desses desafios, ratifica-se que o artigo está organizado com a Seção II, que destaca a integração de sistemas ciberfísicos (*Cyber-Physical Systems* – CPS) e a necessidade de considerar a interoperabilidade e a proteção contra ataques cibernéticos além da extensão da vida útil de recursos legados nesse contexto. Posteriormente, a Seção III ressalta a crescente preocupação com as ameaças cibernéticas em sistemas militares, exemplificando casos de aeronaves que foram alvo de ataques e enfatizando a necessidade de fortalecer a defesa cibernética para garantir a eficácia e a segurança operacional desses sistemas, especialmente em Operações Militares. Por fim, as Seções IV e V apresentam um apanhado de estudos, propondo estratégias para fortalecer a defesa cibernética de sistemas embarcados além de orientar quanto a medidas importantes, incluindo investimentos, regulamentações específicas e adoção de padrões internacionais, a fim de proteger os sistemas de aeronaves militares e garantir a eficácia das missões do Comando da Aeronáutica (COMAER).

II. Segurança Cibernética em Sistemas Ciberfísicos

O *National Institute of Standards and Technology* (NIST) define CPS como a estreita união e coordenação entre recursos computacionais e físicos. Ademais, esse Instituto Nacional de Padrões e Tecnologia do Departamento de Comércio dos Estados Unidos (EUA) é responsável por promover a inovação e a competitividade industrial, desenvolvendo e promovendo padrões e diretrizes em diversas áreas, incluindo tecnologia da informação e segurança cibernética [5].

Atualmente, o *framework* desenvolvido por este Instituto é amplamente reconhecido e adotado pela indústria, desempenhando um papel crucial na obtenção de segurança cibernética. Observa-se, então, que suas diretrizes e padrões estabelecem

Tiago Josué Diedrich, diedrichtjd@fab.mil.br; Oswaldo Segundo da Costa Neto, netooscn@fab.mil.br.

uma base sólida para proteger sistemas críticos e enfrentar os desafios do ambiente digital.

Nesse contexto, há um revés crítico na alta probabilidade de comprometimento da segurança cibernética por meio da integração de sistemas informacionais e embarcados. A Fig. 1 retrata a interdependência sistêmica, corroborando o conceito de comprometimento da segurança cibernética a partir da interface entre esses sistemas.

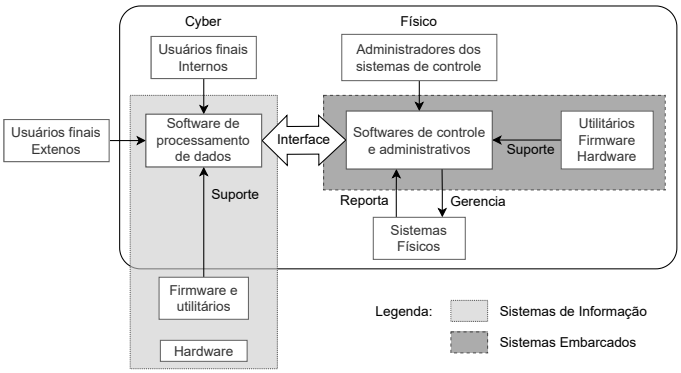

Fig. 1: Componentes Cibernéticos e Físicos de CPS (Adaptado de [6])

É necessário fazer uma distinção entre as aplicações de controle e administração, que são geralmente incorporadas em sistemas embarcados e acessadas por administradores ou operadores quando necessário, dos sistemas de processamento de dados, que são aplicativos desenvolvidos ou adquiridos separadamente e operados por usuários internos ou externos.

Quando esses sistemas operam de forma independente, o risco de ataques cibernéticos é baixo. No entanto, problemas de segurança cibernética surgem quando esses sistemas são interconectados logicamente (como indicado pela seta dupla), especialmente quando a interoperabilidade não foi considerada [3].

Importa mencionar que sistemas embarcados militares legados em tempo real não foram projetados para serem conectados a sistemas de informação modernos, geralmente conectados à Internet. Da mesma maneira, também não foram criados para serem integrados a CPS altamente interligados. Contudo, evidencia-se uma demanda cada vez maior para prolongar a durabilidade de recursos legados que continuam em operação após terem excedido sua vida útil prevista [3] e [7].

Destarte, os CPS são de grande importância para a indústria da aviação [8]. Essa área requer que os sistemas aeronáuticos e aeroespaciais sejam capazes de operar em tempo real e mantenham um elevado grau de confiabilidade. Não obstante, muitos desses sistemas são críticos para a segurança e exigem certificação e forte controle de segurança cibernética [9].

Por outro lado, os futuros sistemas de aeronaves militares incorporarão maior inteligência e autonomia, resultando em sistemas altamente complexos. Dessa forma, entende-se que os avanços na tecnologia de CPS são necessários para compreender e analisar em detalhes as interações entre os componentes físicos e computacionais desses sistemas, a fim de atender e/ou superar os níveis críticos de segurança exigidos para sistemas comerciais [10].

III. Ameaças e Vulnerabilidades Presentes em SEAM

O investimento em tecnologias avançadas para enfrentar novas ameaças em situações de guerra, incluindo aplicações no domínio cibernético, cresce de maneira exponencial [11]. Por exemplo, a implantação de novas capacidades no campo de batalha é uma prioridade, conforme mencionado no relatório nacional de segurança dos EUA [12]. Esses investimentos visam fortalecer a segurança e a eficácia das Operações Militares em resposta aos desafios emergentes nas áreas de defesa cibernética e guerra moderna, onde muitos desses estão relacionados aos conceitos de Força-Tarefa.

Nesse contexto, observa-se que relatórios de Força-Tarefa têm definições relacionadas às ameaças cibernéticas em três classes: profissionais que dependem de terceiros; outros que podem criar ameaças limitadamente; e aqueles que têm muitos recursos e se concentram em vulnerabilidades específicas de certos sistemas críticos [13]. Destarte, a última classe é a mais preocupante, especialmente quando envolve Forças-Tarefa ou operações conjuntas e/ou combinadas.

Segundo [14], algumas evidências apontam que um hacker conseguiu explorar vulnerabilidades em um avião da *United Airlines*, assumindo o controle da aeronave durante o voo. Esse incidente ressalta a realidade das vulnerabilidades cibernéticas em aeronaves e reforça a crescente preocupação com a segurança dos passageiros. Diante desse cenário, é essencial que a indústria da aviação intensifique seus esforços para fortalecer as medidas de proteção cibernética e garantir que sistemas e infraestruturas sejam robustos o suficiente para enfrentar potenciais ameaças no ambiente digital.

Conforme [15], a Força Aérea dos EUA (*United States Air Force* – USAF) planeja corrigir as vulnerabilidades cibernéticas presentes na aeronave F-35, visando assegurar seu pleno desempenho em ambientes de alta complexidade que envolvem questões cruciais de segurança nesse domínio. No artigo, o autor enfatiza a indispensável urgência de abordar e solucionar as potenciais exposições cibernéticas nas aeronaves como um imperativo para salvaguardar a segurança e a integridade do sistema, garantindo, assim, a operação segura e eficiente das aeronaves em todas as missões.

Em outro caso, [16] sugeriu que a China pode ter derrubado um Sukhoi Su-30MKI por meio de artefatos cibernéticos, ressaltando a importância de especialistas em segurança em apontar o investimento do país asiático nesse tipo de tecnologia. Diante disso, torna-se fundamental antecipar e combater as intenções de potenciais oponentes no âmbito cibernético, uma vez que a segurança nesse contexto é de extrema relevância para a estabilidade internacional.

É possível citar que algumas aeronaves militares observam um nível de segurança adequado para as demandas operacionais exigidas. Segundo [17], líderes da *Air Mobility Command* e das Operações Conjuntas da USAF receberam uma demonstração reveladora, destacando a viabilidade de salvaguardar a aeronave KC-46A Pegasus e seus sistemas auxiliares em cenários adversos, garantindo sua utilização segura durante operações de combate. Essa demonstração ressalta a eficácia das medidas de proteção em ambientes desafiadores, ampliando as capacidades estratégicas e táticas da aeronave.

Já o autor em [18] afirma que a USAF fortaleceu sua postura defensiva por meio de duas iniciativas na arquitetura

de operações da Rede de Informações do Departamento de Defesa (do inglês, *Department of Defense Information Network – DoDIN*), buscando equilibrar o custo e o risco entre ataque e defesa. No entanto, identificou-se uma lacuna na proteção dos Sistemas de Tecnologia da Informação (STI) embarcados em plataformas aéreas, que demanda atenção e aprimoramentos para garantir uma defesa completa e robusta.

As preocupações ainda relatadas em [18] vão além quando se considera que as aeronaves militares não possuem uma proteção adequada contra ameaças cibernéticas específicas. Como resultado, indivíduos ou entidades com recursos significativos podem explorar vulnerabilidades em sistemas críticos e projetar ataques precisamente para aproveitar as vulnerabilidades dos SEAM. Portanto, essa questão merece uma atenção especial, pois a proteção cibernética dessas aeronaves deve garantir a segurança operacional e a eficácia nas operações conjuntas.

IV. Abordagens de Redução de Vulnerabilidades em SEAM

É importante mencionar que os autores em [19], [20], [21] e [10] dedicaram-se a pesquisas sobre ataques cibernéticos direcionados a sistemas embarcados e, com isso, apresentaram estratégias de mitigação eficazes que podem ser utilizadas como princípios e conceitos de segurança aos SEAM. Essa sinergia entre conhecimentos é fundamental para fortalecer a proteção e garantir a integridade desses sistemas vitais em diversos setores, principalmente aqueles afetos às Operações Militares.

É fato que [19] abordou um conjunto de perigos cibernéticos direcionados a sistemas embarcados, como ataques de injeção de código, exploração de vulnerabilidades e negação de serviço. No entanto, para preservar esses sistemas, o autor recomendou a implementação de salvaguardas, como criptografia e autenticação robustas, visando fortalecer significativamente sua segurança contra ameaças potenciais.

Da mesma forma, [20] destacou a relevância crucial da integridade e da confiabilidade dos dados em sistemas embarcados. Ele expôs medidas essenciais para detectar e prevenir ataques, utilizando abordagens como redundância de hardware e verificação de integridade de software. Ademais, o autor ratificou que, ao incorporar tais métodos, é possível garantir um funcionamento mais seguro e livre de falhas, essencial para a estabilidade e a eficiência desses sistemas vitais em diversas aplicações tecnológicas.

Por outro lado, o autor em [21] dedicou-se ao estudo minucioso de ataques direcionados aos sistemas de controle industrial, apresentando propostas inovadoras para identificar e combater ameaças. Sua abordagem incluiu a detecção de anomalias e a implementação de técnicas avançadas de monitoramento em tempo real. Tal pesquisa contribuiu significativamente para fortalecer a segurança nesse setor vital, salvaguardando operações críticas e promovendo um ambiente confiável para a indústria.

Destacamos, também, os estudos de [10], que focou na apresentação de um *framework* para análise de vulnerabilidades associadas com CPS utilizados na aviação. Tal abordagem endereça (1) os aspectos de escopo e arquitetura de segurança, definindo o perímetro e a localização das funções e serviços no sistema que necessitam ser protegidos, além das medidas de segurança implementadas; e (2) a avaliação de risco de segurança cibernética, que considera cenários de ameaças, impacto e probabilidade do ataque além de expor os níveis de garantia, classificando o estado do sistema como normal, incerto ou vulnerável.

Dadas as informações apresentadas até aqui, observa-se que os conceitos e as abordagens de proteção cibernética delineados pelos autores supracitados sugerem uma necessidade premente de abordar de maneira mais profunda a segurança cibernética para os SEAM. Isso implicaria na implementação de medidas de segurança robustas, como criptografia avançada, autenticação forte, técnicas de detecção de anomalias e redundância de hardware.

Além disso, há também a importância do desenvolvimento de algoritmos baseados em *frameworks* específicos para vulnerabilidades em SEAM, permitindo o monitoramento em tempo real de vulnerabilidades cibernéticas e protocolos de comunicação seguros para garantir a integridade e a confiabilidade desses sistemas, a fim de mitigar ameaças cibernéticas cada vez mais sofisticadas.

V. Desafios e Abordagens Regulatórias

A segurança cibernética se tornou um desafio que vai além dos sistemas de Tecnologia da Informação [22]. Isso destaca a necessidade de ações por parte dos governos e, indiretamente, pelo alto escalão militar, para abordar as preocupações relacionadas à segurança em suas Forças Aéreas. É evidente que esse problema se estende a todos os países, exigindo uma abordagem mais aprofundada para garantir a segurança cibernética nas Operações Aéreas.

A priorização nos investimentos em tecnologia militar voltada para a proteção cibernética dos SEAM, buscando o apoio conjunto de outros órgãos, a fim de aumentar o orçamento alocado para essa finalidade, também é outro aspecto que pode proporcionar maior capacidade de segurança cibernética para aeronaves militares e, ao mesmo tempo, promover a eficácia das operações conjuntas ou combinadas.

Os autores em [23] e [24] abordam uma relação custo-benefício para investimentos em segurança cibernética para organizações do setor público e privado. Nesses artigos, demonstra-se que os custos de implementação para soluções de medidas contra ataques cibernéticos são proporcionais aos retornos em benefícios, obtendo-se maior resiliência cibernética em infraestruturas críticas para as organizações.

Segundo [25], algumas autoridades dos EUA expressaram publicamente sua posição sobre se as operações cibernéticas se enquadrariam como uso da força nos termos do Artigo 2 da Carta das Nações Unidas [26] e do direito internacional consuetudinário. Além disso, [27], [28] e [29] mencionaram esse mesmo assunto em anos subsequentes, destacando a importância do tema.

Dados os fatos, torna-se latente a possibilidade de ameaças cibernéticas explorarem vulnerabilidades nos SEAM, especialmente em tempos de guerra e Operações Militares, o que sugere a necessidade de autoridades estabelecerem leis e regulamentos específicos para combater ações belicosas no âmbito cibernético.

Ademais, vê-se que, no âmbito militar, tais medidas visam salvaguardar os SEAM, preservar a integridade dos serviços essenciais e proteger os interesses nacionais, pois a ameaça de

um ataque cibernético no domínio aéreo é capaz de comprometer os sistemas aeronáuticos, colocando em risco missões essenciais do Comando da Aeronáutica.

Ao considerar a possibilidade de uma ameaça cibernética dessa magnitude, a FAB poderia se beneficiar da implementação de leis e regulamentos específicos para combater tais ataques, pois um incidente cibernético de grande escala poderia comprometer os sistemas críticos das aeronaves militares, levando-as à destruição, assim como se fossem alvejadas por um míssil. Tal situação representaria um sério risco para o sucesso das missões, impactando negativamente os objetivos operacionais do COMAER.

Dadas as informações apresentadas até aqui, observa-se que a indústria de aviação definiu rigorosos requisitos de segurança de software para aeronaves comerciais em um documento de certificação conhecido como DO-178C [30]. Apesar disso, ainda se observa que, para Aeronaves Remotamente Pilotadas (ARP), geralmente equipadas com sistemas de navegação, sensores, câmeras e, em alguns casos, armamento, essas melhores práticas e diretrizes não são obrigatórias [31].

Portanto, é de suma importância que autoridades governamentais e militares reconheçam a importância desses padrões internacionais e apoiem a adoção e a aplicabilidade de certificação de software, seguindo as diretrizes estabelecidas pelo DO-178C [32] e pelo DO-278A [33]. Isso contribuirá para fortalecer a segurança dos SEAM e garantir a proteção adequada contra ameaças cibernéticas, tanto em operações em tempo de paz quanto em tempo de guerra.

VI. Conclusão

Este trabalho de pesquisa teve como objetivo discutir a importância crucial da segurança cibernética para aeronaves militares durante Operações Militares em tempos de paz e de guerra, propondo um novo conceito denominado SEAM, que abrange os sistemas críticos a bordo de plataformas aéreas e suas vulnerabilidades diante de ataques cibernéticos.

Para fortalecer a proteção cibernética no espaço de interesse, observaram-se serem imprescindíveis a alocação de maiores investimentos em tecnologia militar e a criação de leis e regulamentos específicos voltados à defesa cibernética, especialmente ao tratar dos SEAM. Essa proteção é de suma importância, exigindo o apoio institucional e ação por parte de autoridades governamentais e militares.

O artigo apresenta uma preocupação quanto à segurança cibernética dos SEAM por serem essenciais para garantir a eficácia das operações conjuntas e/ou combinadas bem como das Forças-Tarefa, sugerindo a implementação de medidas que reduzam significativamente o número de ameaças cibernéticas direcionadas às aeronaves militares. Nesse sentido, é possível considerar a adoção das medidas apresentadas por algumas normas e instruções, as quais oferecem diretrizes para combater ameaças cibernéticas direcionadas às plataformas aéreas.

Dada a complexidade das operações militares e o ambiente cibernético cada vez mais hostil, observou-se que a proteção dos SEAM assume um papel central na segurança nacional. Ademais, a implantação de criptografia avançada, autenticação robusta e detecção de anomalias também se mostram fundamentais para salvaguardar os sistemas críticos embarcados. Além disso, a incorporação de redundância de hardware e de técnicas de verificação de integridade de software pode fortalecer ainda mais a segurança dos SEAM, garantindo o funcionamento seguro e confiável das aeronaves em comento.

Desse modo, ao considerar as inovações tecnológicas e o surgimento contínuo de ameaças cibernéticas cada vez mais sofisticadas, é imperativo que as forças militares estejam preparadas para enfrentar esses desafios. Logo, vê-se que a abordagem regulatória, com base nas normas DO-178C e DO-278A, pode proporcionar um marco sólido para estabelecer práticas de segurança consistentes e de alto nível em todo o espectro de Operações Militares.

Por fim, entende-se que a compreensão do conceito de SEAM e a aplicação das diretrizes regulatórias, aliadas a investimentos adequados em tecnologia militar, constituem um enfoque abrangente e robusto para combater ameaças cibernéticas e garantir a supremacia aérea em tempos de guerra e em operações militares críticas. Portanto, tal abordagem integrada e proativa pode proporcionar uma maior proteção de sistemas aéreos militares e resguardar os interesses nacionais em um cenário de crescente complexidade no âmbito cibernético.

Agradecimentos

Os autores deste artigo agradecem ao Comando da Aeronáutica (COMAER), ao Instituto Tecnológico de Aeronáutica (ITA), ao Programa de Pós-Graduação em Aplicações Operacionais (PPGAO), à Diretoria de Tecnologia da Informação da Aeronáutica (DTI) e ao Centro de Computação da Aeronáutica de Brasília (CCA-BR) pelo suporte e infraestrutura oferecidos durante todo o desenvolvimento deste trabalho de pesquisa.

Referências

[1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," *Computer Communications*, vol. 36, no. 1, pp. 1–7, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366412003180

[2] R. M. Fouda, "Security vulnerabilities of cyberphysical unmanned aircraft systems," *IEEE Aerospace and Electronic Systems Magazine*, vol. 33, no. 9, pp. 4–17, 2018.

[3] C. W. Axelrod, "Cybersecurity and modern tactical systems," *CrossTalk*, vol. 28, no. 6, pp. 4–11, 2015.

[4] M. Vai, D. J. Whelihan, B. R. Nahill, D. M. Utin, S. R. O'Melia, and R. I. Khazan, "Secure embedded systems," *Lincoln Laboratory Journal*, vol. 22, no. 1, pp. 110–122, 2016.

[5] National Science Foundation (NSF), "Cyber-Physical Systems (CPS) Program Solicitation NSF 21-551," Posted: January 11, 2021, National Science Foundation (NSF), 2021, acesso em 08 de julho de 2023. [Online]. Available: https://dod.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-june-2015.pdf

[6] C. W. Axelrod, "Mitigating the risks of cyber-physical systems," in *Proc. of the 2013 IEEE LISAT Conf.*, Farmingdale, NY, 2013.

[7] A. Sellars, "Life cycle extension strategies for legacy systems," Nashville, Tennessee, August 2004, submitted to the Faculty of the Graduate School of Vanderbilt University in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE in Management of Technology.

[8] H. Bai, M. Atiquzzaman, and D. Lilja, "Wireless sensor network for aircraft health monitoring," in *Proceedings of Broadband Networks (BROADNETS)*, 2004.

[9] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proceedings of IEEE INFOCOM*, 2007, pp. 1307–1315.

[10] S. A. Kumar and B. Xu, "Vulnerability assessment for security in aviation cyber-physical systems," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. IEEE, 2017, pp. 145–150.

[11] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Computers & security*, vol. 49, pp. 70–94, 2015.

[12] Government of the United States, "National security strategy 2022," Documento governamental, 2022. [Online]. Available: https://nssarchive.us/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[13] Department of Defense (DoD), "Defense Science Board (DSB). Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," Department of Defense, Tech. Rep., 2013. [Online]. Available: https://dsb.cto.mil/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf
[14] Moyer, Justin Wm., "Hacker Chris Roberts told FBI he took control of United plane, FBI claims," The Washington Post, 2015, acesso em 18 de junho de 2023. [Online]. Available: https://www.washingtonpost.com/news/morning-mix/wp/2015/05/18/hacker-chris-roberts-told-fbi-he-took-control-of-united-plane-fbi-claims/
[15] Sprenger, Sebastian, "US Air Force moves to fortify F-35 weak points against hacking," DefenseNews, 2018, acesso em 18 de junho de 2023. [Online]. Available: https://www.defensenews.com/air/2018/11/14/us-air-force-moves-to-fortify-f-35-weak-points-against-hacking/#:~:text=BERLIN%20%E2%80%93%20The%20U.S.%20Air%20Force,to%20a%20key%20service%20official
[16] Nalapat, M.D., "Sukhoi Likely Downed by Cyber Weapons," The Sunday Guardian, 2017, acesso em 18 de junho de 2023. [Online]. Available: https://sundayguardianlive.com/news/9573-sukhoi-likely-downed-cyber-weapons
[17] Eckert, Nathan, "Weapons System Cyber Security: The New Model for Warfighting," Air Mobility Command, 2022, acesso em 18 de junho de 2023. [Online]. Available: https://www.amc.af.mil/News/Article-Display/Article/3022761/weapons-system-cyber-security-the-new-model-for-warfighting-how-the-air-forces/
[18] W. J. Poirier and J. Lotspeich, "Air force cyber warfare: now and the future," AIR UNIV MAXWELL AFB AL AIR FORCE RESEARCH INST, Tech. Rep., 2013.
[19] P. Kocher, R. Lee, G. McGraw, and A. Raghunathan, "Security as a new dimension in embedded system design," in *Proceedings of the 41st annual design automation conference*, 2004, pp. 753–760.
[20] P. Koopman, "Embedded system security," *Computer*, vol. 37, no. 7, pp. 95–97, 2004.
[21] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *ACM Trans. Embed. Comput. Syst.*, vol. 3, no. 3, p. 461–491, aug 2004. [Online]. Available: https://doi.org/10.1145/1015047.1015049
[22] Hadley, Greg, "Air Force Was 'Hyper Focused' on Cybersecurity for IT Networks. Now Other Systems Need Protection." Air & Space Forces Magazines, 2022, acesso em 24 de junho de 2023. [Online]. Available: https://www.airandspaceforces.com/air-force-was-hyper-focused-on-cybersecurity-for-it-networks-now-other-systems-need-protection/
[23] M. A. Roumani, C. C. Fung, S. Rai, and H. Xie, "Value analysis of cyber security based on attack types," *ITMSOC: Transactions on Innovation and Business Engineering*, vol. 1, pp. 34–39, 2016.
[24] A. Arora, D. Hall, C. Piato, D. Ramsey, and R. Telang, "Measuring the risk-based value of it security solutions," *IT Professional*, vol. 6, no. 6, pp. 35–42, 2004.
[25] H. H. Koh, "International law in cyberspace," Legal Advisor U.S. Department of State, USCYBERCOM Inter-Agency Legal Conference, 2012, acesso em 07 de julho de 2023. [Online]. Available: https://2009-2017.state.gov/s/l/releases/remarks/197924.htm
[26] United Nations, "Charter of the United Nations," United Nations, 1945, acesso em 07 de julho de 2023. [Online]. Available: https://treaties.un.org/doc/publication/ctc/uncharter.pdf
[27] C. A. Theohary and A. I. Harrington, *Cyber operations in dod policy and plans: Issues for congress*. Congressional Research Service Washington, DC, 2015, vol. 5.
[28] Department of Defense (DoD), "Law of War Manual," 2015, acesso em 07 de julho de 2023. [Online]. Available: https://dod.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-june-2015.pdf
[29] J. E. McGhee, "Liberating cyber offense," *Strategic Studies Quarterly*, vol. 10, no. 4, pp. 46–63, 2016.
[30] C. Howard, "UAVs, software, and security: An interview with Robert Dewar of AdaCore," Intelligent Aerospace, 2012. [Online]. Available: http://www.intelligent-aerospace.com/articles/2012/06/uavs-software.html
[31] R. Sen, "Challenges to cybersecurity: Current state of affairs," *Communications of the Association for Information Systems*, vol. 43, no. 1, p. 2, 2018.
[32] "DO-178C: Software Considerations in Airborne Systems and Equipment Certification," 2011, Radio Technical Commission for Aeronautics (RTCA).
[33] "DO-278A: Software Integrity Assurance in Air Traffic Services," 2019, Radio Technical Commission for Aeronautics (RTCA).