ESCOLA DE APERFEICOAMENTO DE OFICIAIS DA AERONAUTICA

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1/2021

FREDERICO **AUGUSTO** MARTINS GORI, CAP AV

COMUNICAÇÃO CRIPTOGRÁFICA COMSEC/TRANSEC ENTRE A SCOAM E O PODA

Rio de Janeiro

2021

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1/2021

FREDERICO **AUGUSTO** MARTINS GORI, CAP AV

COMUNICAÇÃO CRIPTOGRÁFICA COMSEC/TRANSEC ENTRE A SCOAM E O PODA

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-graduação em Gestão Pública com ênfase em Gestão de Projetos e Processos.
Linha de Pesquisa: Emprego da Força Aérea.
Orientador: Antonio Pereira **Damasceno** Neto, Maj Av

Rio de Janeiro
2021

FREDERICO **AUGUSTO** MARTINS GORI, CAP AV

COMUNICAÇÃO CRIPTOGRÁFICA COMSEC/TRANSEC ENTRE A SCOAM E O PODA

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica

Aprovado por:

Wellington Azevedo Dos Santos, Maj Inf
EAOAR

Antonio Pereira **Damasceno** Neto, Maj Av
EAOAR

Rio de Janeiro
2021

RESUMO

O COMAE é o orgão do SISDABRA responsável pela execução das atividades de policiamento do espaço aéreo brasileiro, empregando, atualmente, as aeronaves A-29 e F-5. Nesse contexto, verifica-se, no ciclo de acionamento do alerta, vulnerabilidades de segurança, sendo uma delas a ausência de comunicação criptográfica entre a SCOAM e o PODA. Consequentemente, as instruções de acionamento como trigrama do PODA/COAM, canais de comunicação e nível de voo, podem ser facilmente interceptadas. Portanto, este ensaio objetiva defender a tese de que a inserção de comunicação criptográfica entre a SCOAM e o PODA ampliará o nível de segurança e sigilo das instruções de acionamento e maximizará a utilização dos recursos criptográficos existentes nestas aeronaves. Relacionam-se a esse propósito os seguintes argumentos: a inserção de criptografia nas comunicações em VHF entre a SCOAM e o PODA salvaguardará de forma mais profícua e eficiente o sigilo das instruções de acionamento e resguardará as coordenações relativas à situação operacional da aeronave de alerta como: panes logísticas, abastecimento de combustível e demais coordenações. Outrossim, argumenta-se que ao implementar a comunicação COMSEC/TRANSEC incrementará-se o nível de proficiência na utilização dos recursos criptográficos dos rádios Rohde & Schwarz instalados nestas aeronaves, dada a capacidade ociosa, por hora, observada. Desta maneira, este ensaio tem como parecer final a concreta possibilidade de se aprimorar o ciclo de comando e controle da FAB ao impossibilitar que as instruções de acionamento do alerta de defesa aérea estejam suscetíveis de serem auscultadas por sensores de ELINT e COMINT.

Palavras-Chave: Comunicação. Criptografia. Interceptação. Aviação de Caça. SISDABRA.

1. INTRODUÇÃO

A Diretriz do Comando da Aeronáutica 11–45, Concepção Estratégica da Força Aérea 100, define a missão síntese da Força Aérea Brasileira (FAB) como sendo a de manter a soberania do espaço aéreo e integrar o território nacional, com vistas à defesa da pátria.

Nesse escopo, o Sistema de Defesa Aéreo Brasileiro (SISDABRA) é composto pelo Comando de Operações Aeroespaciais (COMAE), nas funções da Alta Autoridade de Defesa Aérea (AADA), do Oficial de Supervisão Operacional (OSO) e do Supervisor de Defesa Aérea (SDA), pelo Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA), nas funções do Chefe Controlador (CC) e do Controlador de Operações Aéreas Militares (COAM), pelas Salas de Controle de Operações Aéreas Militares (SCOAM), como elo, e pelas Unidades Aéreas, na função do Piloto Operacional de Defesa Aérea (PODA).

Ao se constatar a presença de vários atores na cadeia de acionamento do alerta, detectam-se vulnerabilidades de segurança, sendo uma delas a ausência de comunicação criptográfica entre a SCOAM e o PODA, permitindo, assim, que agentes externos ao COMAER consigam espionar e auscultar informações de elevada importância estratégica para o SISDABRA.

Diante do exposto, este ensaio objetiva defender a tese de que a inserção de comunicação criptográfica entre a SCOAM e o PODA ampliará o nível de segurança, sigilo e confiabilidade das instruções de acionamento do alerta, bem como suas coordenações operacionais/logísticas e, adicionalmente, maximizará a utilização dos recursos criptográficos existentes nestas aeronaves.

Nesse contexto, ao inserir-se a comunicação criptográfica, preserva-se a integridade de informações de alto valor estratégico para o SISDABRA, constantes da ordem de acionamento e resguardam-se as coordenações de eminente importância relativas à situação operacional da aeronave de alerta. Além disso, entende-se que, ao implementar a tecnologia COMSEC/TRANSEC, aperfeiçoa-se o nível de proficiência e utilização dos recursos criptográficos instalados nas aeronaves F-5 e A-29, dada a capacidade ociosa, por hora, observada, robustecendo a capacidade do SISDABRA contra medidas de sensores interferidores e passivos com capacidade de ELINT e COMINT.

2 DESENVOLVIMENTO

De maneira geral, Matos (2005) descreve que o início do uso de recursos criptográficos modernos, datam dos anos 20 do século XX, por meio da máquina Enigma, capaz de criptografar e descriptografar códigos de guerra. Conceitualmente, a comunicação criptográfica pode ser resumidamente entendida como práticas e princípios de comunicação sem a presença de agentes externos não autorizados, por meio de autenticação de segurança.

Conforme assevera Netto, comunicação criptográfica é:

> A troca de informações entre emissor e receptor por meio de chave criptográfica cooperativa, com vistas a proteger dados ou informações de fundamental importância estratégica para determinada atividade (NETTO, 2005, p.11).

Lisboa (2008) afirma que as vulnerabilidades de segurança, em setores estratégicos, devem ser constantemente analisadas e progressivamente eliminadas, para que estas não afetem a missão institucional de uma organização. Portanto, no contexto deste ensaio, a vulnerabilidade apresentada pode estar comprometendo os resultados das missões de policiamento do espaço aéreo brasileiro. De acordo com dados estatísticos do ano de 2020, providos pela Divisão de Operações Correntes (DIVOC) do COMAE, foram realizados 04 Tiros de Aviso (TAV) e 00 Tiros de Detenção (TDE) no referenciado ano, tendo sido voadas 250 horas de pela aeronave F-5 Tiger Northrop e 520 horas de A-29 Super Tucano. Complementa-se a estes dados, o fato de terem sido realizados 798 relatórios de tráfegos aéreos desconhecidos (TADREL) pelos 04 Centros Integrados de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA) em 2020.

2.1 Sigilo criptográfico das instruções de acionamento e das coordenações operacionais/logíticas das aeronaves de defesa aérea.

Neste cenário, observa-se que a atual ausência de comunicação criptográfica entre a SCOAM e o PODA é uma vulnerabilidade de segurança do ciclo de comando e controle do SISDABRA, pois, possibilita que agentes externos não autorizados possam estar tendo conhecimento sobre as instruções de acionamento e sobre a situação operacional/logística das aeronaves de defesa aérea.

Em face do exposto, conforme diretrizes apontadas por Moreira (2016), informações essenciais devem ser protegidas com avançados protocolos de segurança criptográficos, como também, por rígidos procedimentos doutrinários de transmissão de informação. Desta forma, com a utilização de recursos criptográficos mitiga-se a probabilidade de interferência por sensores com capacidade de ELINT e COMINT, tanto por parte de narcotraficantes, quanto por países do nosso entorno estratégico em ações de inteligência, como, por exemplo, a Venezuela.

Atualmente, as coordenações de acionamento, operacionais e logísticas sob responsabilidade da SCOAM são realizadas por rádio VHF aeronáutico (118,000 e 136,975 MHz) e estão altamente suscetíveis a serem interceptadas em razão da ausência de chaves criptográficas. Moreira (2003) explica que codificação é a metodologia utilizada para tornar uma informação aceitável e compreensível em um processo estruturado. Evidencia-se que as instruções de acionamento do alerta apesar de codificadas, podem ser facilmente interceptadas e compreendidas.

Por este meio de comunicação tramitam informações como a ordem de acionamento do alerta, contendo trigrama do PODA, do COAM, canais de comunicação, transponder, proa de saída, nível de voo e se a missão é real ou simulada (Rojão de Fogo), como também, reportes logísticos e operacionais, abastecimento de combustível, configuração de armamento, substituição de aeronaves e demais coordenações.

Segundo Pigatto (2012), a proteção de dados sensíveis deve possuir atributos que tornem a comunicação confiável, robusta e não interceptável, devendo-se garantir, mesmo sob condições adversas (interferência eletrônica, Jamming e condições climáticas desfavoráveis), que as informações sejam transmitidas fidedignamente. De acordo com Pigiato:

> Algumas propriedades devem ser garantidas para uma completa e eficaz implementação de segurança como: Confidencialidade, autenticidade, integridade, não repúdio de mensagem e disponibilidade (PIGATTO, 2012, p.14).

Nesse viés, a tecnologia COMSEC pode ser interpretada como uma forma de negar aos receptores não autorizados dados de telecomunicações (dados, vídeo e comunicação) por de chaves criptográficas. Já a tecnologia TRANSEC é a aplicação de medidas protetivas na transmissão das informações por meio de salto de frequências, ou seja, durante a transmissão, a frequência é alterada de forma aleatória dentro da faixa estabelecida para comunicações aeronáuticas (118,000 e 136,975

MHz) na qual somente os detentores da chave criptográfica conseguirão decodificar a informação propagada.

Por fim, demonstra-se que a implementação de comunicação COMSEC/TRANSEC entre a SCOAM e o PODA é tema de grande relevância para o SISDABRA. Desta maneira, adquire-se vantagem operacional em relação ao inimigo ao proteger o SISDABRA contra medidas de ELINT e COMINT, devido à capacidade de salto de frequências, como também contra equipamentos de inteligência de comunicações, capazes de detectar a faixa de frequência e gravar estas comunicações, sanando, desta maneira, as vulnerabilidades elencadas neste tópico.

2.2. Capacidade ociosa na utilização dos recurso criptógráficos dos rádios Rohde & Schwarz nas aeronaves F-5 e A-29.

O Sistema de Vigilância da Amazônia (SIVAM) é um projeto idealizado pelo governo federal, com a finalidade de aumentar a capacidade de fiscalização do estado brasileiro sobre o território amazônico. Consoante Santos (2018), no intuito de reprimir o transporte aéreo de drogas, armas e ilícitos, o congresso aprovou a Lei 9.614/1998 e o decreto 5.144/2004, estabelecendo os protocolos a serem seguidos pelo COMAE, respaldando legalmente a FAB a deter aeronaves hostis ou suspeitas de tráfico de substâncias entorpecentes. Conforme assevera Santos, antes dessa lei:

> Essas aeronaves circulavam livremente, especialmente pelas fronteiras brasileiras, violando, sobretudo, a Soberania do Estado e adentrando com entorpecentes e substâncias proibidas. Tornou-se mais que necessárias medidas com maior contundência para combater os voos ilícitos que transportavam esses entorpecentes e substâncias proibidas para o Brasil (SANTOS, 2018, p.27).

Nesta conjuntura, a Força Aérea Brasileira iniciou em 2000, o processo de modernização das aeronaves F-5 e realizou a aquisição de 78 A-29 Super Tucano, equipando-os com os rádios Rohde & Schwarz V/UHF M3AR Série 6000. A aquisição destes equipamentos representou um importante avanço tecnológico para a Força Aérea Brasileira, ao permitir o início da comunicação criptográfica entre as aeronaves de caça e o CINDACTA. De acordo com Moreira (2016), as principais potências militares (Estados Unidos, Rússia e China) fazem amplo uso de sistemas criptográficos para proteção de dados sensíveis e em suas comunicações estratégicas. Segundo Moreira:

> A necessidade de proteger esse produto da informação, fazendo disso uma vantagem significativa. Isso estaria dentro de um propósito de manutenção do poder, por meio da proteção das suas informações.(MOREIRA, 2016, p. 51).

Deste modo, fazendo o uso da metodologia japonesa Kanban, a qual busca identificar oportunidades de melhoria no fluxo de trabalho, buscando um gerenciamento com melhores resultados, identificou-se uma capacidade ociosa, por hora, na utilização dos recursos criptográficos dos rádios Rohde & Schwarz, visto a possibilidade de realizar-se comunicação segura entre a SCOAM e o PODA.

Outro fator importante a ser destacado, são os diminutos impactos operacionais e econômicos para implementar a comunicação COMSEC/TRANSEC, visto não serem necessárias alterações estruturais nas aeronaves, bastando somente a aquisição de rádios com capacidade criptográfica compatível com o modelo V/UHF M3AR Série 6000 da Rohde & Schwarz.

Adicionalmente, aumentará-se o nível de sigilo e proteção das tripulações do SISDABRA ao evitar a exposição do trigrama do PODA e do COAM, no momento da transmissão das instruções de acionamento. Salienta-se que estes tripulantes possuem uma formação muito especializada, com elevado tempo de formação operacional (7 anos para oficiais e 04 para graduados) e com elevados custos para a união, devendo ser suas identidades protegidas por rígidos protocolos de segurança.

Segundo Moreira (2016), é a complementariedade de sistemas de segurança que tornam a proteção de dados sensíveis eficaz e efetiva, devendo ser uma preocupação constante eliminar progressivamente as vulnerabilidades de segurança em todos os segmentos de transmissão da informação. Ferrua (2010) afirma que a evolução dos métodos e dispositivos de interferência eletromagnética estão em rápida evolução, devendo ser uma obrigação o desenvolvimento de medidas e protocolos de segurança que impossibilitem o vazamento de dados críticos.

Em conclusão, ao aperfeiçoar o nível de proficiência e utilização dos recursos criptográficos instalados nos rádios Rohde & Schwarz, tem-se como consequência a melhora do ciclo de comando e controle do SISDABRA, aprimorando-se o grau de segurança no que diz respeito ao sigilo das instruções de acionamento das aeronaves de alerta, proteção de suas tripulações, assim como suas coordenações operacionais/logísticas.

3 CONSIDERAÇÕES FINAIS

Infere-se, mediante o exposto, que a inserção de comunicação criptográfica é tema de elevada importância para o aprimoramento dos protocolos de segurança e doutrinários do SISDABRA, eliminando-se importantes vulnerabilidades de segurança contra possíveis ações de ELINT e COMINT.

De tal sorte, ao inserir-se meios criptográficos, preservar-se-á, de maneira mais profícua e eficiente, o sigilo das instruções emanadas pelos escalões superiores, assim como, resguardará-se a dinâmica operacional das aeronaves de defesa aérea, por meio da inserção de chaves criptográficas (COMSEC) e de saltos de frequência (TRANSEC).

Outrossim, ao auscultar as instruções relativas ao trigrama do PODA e do COAM, incrementar-se-á o nível de sigilo e de segurança dos militares que compõem as equipagens do SISDABRA, visto que a salvaguarda da integridade dos mesmos é de fundamental observância para a FAB, dado a especificidade da capacitação, erário nacional investido e o elevado tempo de formação até que atinjam a operacionalidade necessária para executar esta atividade.

À guisa de conclusão e diante da vulnerabilidade apresentada, constata-se que ao implementar a comunicação criptográfica, incrementa-se o nível de segurança e confiabilidade do processo de transmissão das instruções de acionamento das aeronaves de defesa aérea e suas coordenações logísticas, adicionalmente, preserva-se a confidencialidade das tripulações que desempenham as atividades de policiamento do espaço aéreo, assim como, utiliza-se mais eficaz e eficientemente os recursos criptográficos disponíveis nos rádios Rohde & Schwarz V/UHF M3AR Série 6000instalados nas aeronaves F-5 e A-29, obtendo como resultado o fortalecimento dos protocolos de segurança nas comunicações entre a SCOAM e o PODA, tornando as instruções de acionamento e suas coordenações menos suscetíveis a dispositivos interferidores e de escuta.

Por fim, o parecer final deste trabalho é que a inserção da comunicação criptográfica entre a SCOAM e o PODA aprimorará o ciclo de comando e controle da FAB ao impossibilitar que informações de alto valor estratégico possam ser auscultadas por sensores com capacidade de ELINT e COMINT, esperando-se ter como consequência a melhora do grau de eficiência dos dados estatísticos referentes as medidas de policiamento do espaço aéreo brasileiro.

REFERÊNCIAS

FERRUA, P. F. M. R. **Dispositivos e métodos de supressão de interferência eletromagnética**. 2010. 140f. Dissertação (Mestrado em Engenharia Aeronáutica e Mecânica). Instituto Tecnológico de Aeronáutica, São José dos Campos. Disponível em: <https://bdita.bibi.ita.br>. Acesso em: 13 de set. 2020.

LISBOA, L. R. P. **Desempenho de redes de comunicação para aeronaves**. 2008. 121f. Dissertação (Mestrado em Engenharia Aeronáutica). Instituto Tecnológico de Aeronáutica, São José dos Campos. Disponível em:< https://bdita.bibi.ita.br.> Acesso em: 15 de set.2020

MATOS, M. A. **Simulação de enlace de dados aeronáuticos em VHF**. 2005. 81f Dissertação (Mestrado em Engenharia Aeronáutica e Mecânica). Instituto Tecnológico de Aeronáutica, São José dos Campos. Disponível em:< https://bdita.bibi.ita.br>. Acesso em: 13 de set. .2020.

MOREIRA, J. B. **Sistema criptográfico com gerenciamento de chaves públicas integrado: uma proposta**. 2003. 180f. Dissertação (Mestrado em Engenharia Eletrônica e Computação). Instituto Tecnológico de Aeronáutica, São José dos Campos. Disponível em:< https://bdita.bibi.ita.br>. Acesso em: 17 de set. 2020.

MOREIRA, W. G. **Atividade de inteligência como ferramenta ideológica**. 2016. 108f. Dissertação (Mestrado em Mestrado em Ciência Política). Centro Universitário Unieuro, Brasília. Disponível em:<http://www.unieuro.edu.br/>. Acesso em: 22 de Out. 2020.

NETTO, J. E. **Segurança em redes de telecomunicações aeronáutica e seu desempenho em canal VDL modo 2.** 2005. 92f. Tese (Mestrado em Engenharia Eletrônica e Computação). Instituto Tecnológico de Aeronáutica, São José dos Campos. Disponível em:< https://bdita.bibi.ita.br>. Acesso em: 13 de set. 2020.

PIGATTO, D. F. **Segurança em sistemas embarcados críticos - utilização de criptografia para comunicação segura**. 2012. 108f. Dissertação (Mestrado em Ciências de Computação e Matemática Computacional). Universidade de São Paulo, São Carlos. Disponível em:<https://www.teses.usp.br.> Acesso em: 15 de set. 2020.

SANTOS, N. J. **A (In) Constitucionalidade Da "Lei Do Abate":** soberania e exceção no estado democrático de direito. 2018. 60f. Monografia (Bacharelado em Direito). Centro Universitário de Brasília, Brasília. Disponível em:<https://repositorio.uniceub.br/>. Acesso em: 22 de Out. 2020.