O EMPREGO DE RÁDIOS MILITARES E OS RISCOS QUANTO À ASSINATURA DO SINAL

Ten **LUCAS HENRIQUE** DE SOUZA RAFAEL
S Ten MÁRCIO **ROBERTO MARTINS** DE ABREU

RESUMO

Assinaturas de sinal em rádios militares referem-se às características específicas de transmissão que distinguem dos demais equipamentos. Essas assinaturas são um elemento chave da inteligência de sinais, permitindo a identificação e a análise de comunicações militares específicas. Portanto, o emprego de equipamentos rádios com tecnologia militares pode oferecer riscos à segurança em combate, conforme as capacidades de análise dos sinais e Guerra Eletrônica do inimigo.

Palavras-chave: INTELIGÊNCIA DO SINAL, GUERRA ELETRÔNICA, ESPECTRO ELETROMAGNÉTICO

1. INTRODUÇÃO

A inteligência do sinal, ou *Signal Intelligence* (SIGINT) em inglês, deriva-se do espectro eletromagnético e atua na coleta de informações focada na interceptação e análise de sinais de comunicação ou de outros tipos de sinais eletrônicos emitidos por dispositivos, pois atua nas atividades de busca, interceptação, identificação e localização de emissões eletromagnéticas.

O emprego de equipamentos de comunicações militares, ainda que acompanhados de sistemas avançados de segurança da informação, acompanha riscos que afetam à segurança das operações militares. Equipamentos militares possuem tecnologias específicas que caracterizam suas transmissões no espectro eletromagnético, como Salto de Frequência e Sistemas de Estabelecimento Automático de Enlace de Terceira Geração, logo essas emissões são evidências de atividades militares. A identificação das emissões, acompanhada pela localização eletrônica, são fatores de grandes riscos.

2 DESENVOLVIMENTO

2.1 ESPECTRO ELETRMAGNÉTICO

Os sistemas de comunicação por rádio-frequência exploram o espectro eletromagnético para suas transmissões. O espectro eletromagnético não é visível a olho nu, mas a utilização de equipamentos específicos permitem sua visualização, análise de transmissões de rádio e até mesmo a identificação de características desses sinais, como tipos de modulação, criptografia, frequência de utilização e até mesmo recursos avançados de segurança como salto de frequência.

Figura 1- Visualização de uma transmissão de rádio.
Fonte: http://appr.org.br:8905/

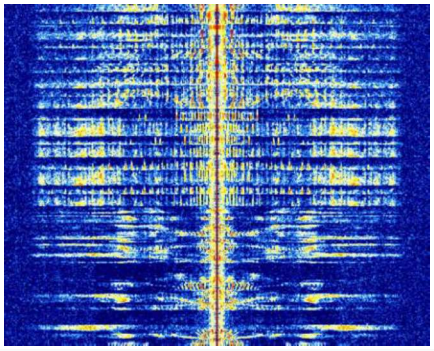
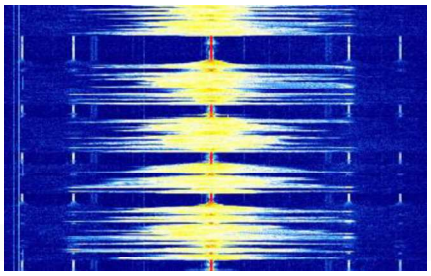


Figura 2L-orFotogrem ipsumafia de uma transmissão em AM.
Fonte: https:www.sigidwiki.com



Fonte: https://www.sigidwiki.com.
Figura 3- Fotografia de uma transmissão em FM.

2.2 DIFERENCIAÇÃO DAS TRANSMISSÕES CIVIS E MILITARES

Através da análise dos sinais no espectro eletromagnético é possível definir se o equipamento transmissor é civil ou um equipamento militar, pois equipamentos militares possuem características específicas. Equipamentos civis utilizam frequências específicas, normalmente são modulações padronizadas como AM (amplitude modulada) ou FM (frequência modulada), suas transmissões não tendem a ser criptografadas ou utilizam criptografia básica (exemplo P25) e não empregam salto de frequência.

Os sinais militares tendem a estar em faixas reservadas para fins militares, utilizam modulações mais complexas, sistemas de estabelecimento automático de link, possuem criptografias complexas e empregam salto de frequência. Além disso, tais sinais possuem padrões de tecnologia proprietária, que são desenvolvidas especialmente para Forças Armadas.

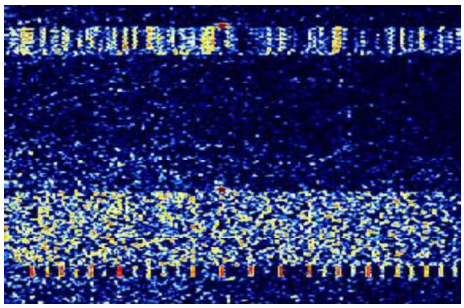


Figura 4 – Fotografia de uma transmissão ALE de Terceira Geração (3G) com padronização military.
Fonte: https://www.sigidwiki.com.

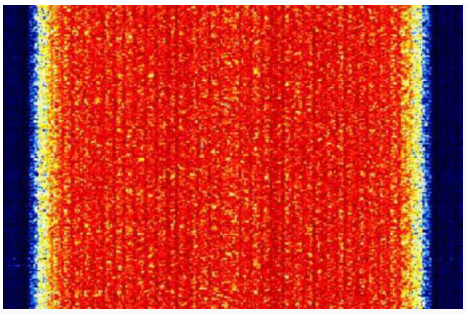


Figura 5 – Fotografia de uma transmissão HF com utilização de protocolos militares.
Fonte: https://www.sigidwiki.com.

2.3 *Direction Finding*: Uma Ferramenta Crucial na Inteligência de Sinais

Direction Finding, ou localização de direção, é uma técnica essencial na guerra eletrônica que desempenha um papel vital na inteligência de sinais . Este processo envolve a determinação da direção de uma fonte de emissão de sinal, como comunicações de rádio, radares ou outras transmissões eletromagnéticas, a partir de um ou mais pontos receptores.

Na guerra eletrônica, a capacidade de identificar a localização de emissores inimigos permite operações militares mais eficazes. Após a confirmação de que o transmissor de RF trata-se de um elemento militar, isso através de confirmações relacionadas à assinatura do sinal, pode-se iniciar medidas para a obtenção de vantagens no Teatro de Operações. Diversas ações podem ser desencadeadas para obtenção de vantagens, como avaliação da capacidade tecnológica inimiga, localização das tropas que operam os equipamentos de comunicações e até mesmo a previsão de planejamentos de contra-ataques inimigos. Esse artigo restringe-se, como exemplo, às ações de localização eletrônica.

A localização eletrônica de transmissores de rádio frequência, tecnicamente conhecida *Direction Finding,* envolve o uso de técnicas e equipamentos especializados para detectar, localizar e identificar a origem de sinais de rádio. Há diversas formas de localizar um transmissor, sendo a triangulação de rádio frequência a mais comum. A triangulação envolve o uso de várias antenas receptoras localizadas em diferentes pontos geográficos. Cada uma dessas antenas mede a intensidade e a direção do sinal recebido do transmissor. Com base nessas medições, as interseções das direções dos sinais indicam a localização aproximada do transmissor.

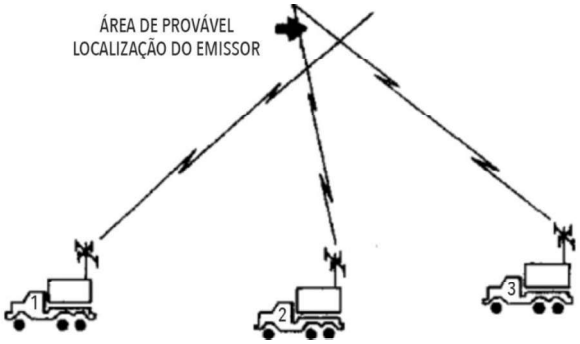


Figura 6 – Ilustração da atividade de *Direction Finding* por triangulação do sinal.
Fonte: https://velhogeneral.com.br/2023/12/04/o-papel-da-guerra-eletronica-de-comunicacao-no-conflito-russia-ucrania/

2.4 RISCOS APÓS A LOCALIZAÇÃO DE ALVOS

Após a localização eletrônica de estruturas militares e alvos compensadores, o que pode ser obtido através da análise de sinais e por sistemas de localização eletrônica, nesse aspecto, os radares são equipamentos muito vulneráveis quanto sua localização eletrônica, devido sua constante emissão de sinais e as características específicas desses sinais. Após as confirmações, diversos tipos de ataques podem ser desencadeados, como ataques aéreos, ataques de artilharia, infiltração, sabotagem de infraestruturas estratégicas e até mesmo a tentativa de captura de materiais de emprego militar.
Um exemplo desse tipo de atuação foi a captura de um Sistema *Krasukha-4* da Rússia, por sua rival Ucrânia, durante o conflito entre os países Rússia e Ucrânia, que se escalou em 24 de fevereiro de 2022.

"Um Krasukha-4 completo consiste em dois veículos, ambos baseados no caminhão KAMAZ-6350 8x8, um com sistema de guerra eletrônica (EW) e outro com módulo de posto de omando."

Figura 7- Sistema russo de radar e posto de commando Krasukha-4.
Fonte: https://galaxiamilitar.es/ucrania-captura-uno-de-los-sistemas-de-guerra-electronica-mas-capaces-de-rusia/

Outro fato que exemplifica, no ano de 2023, militares que operavam em favor da Ucrânia no conflito entre Rússia e Ucrânia decidiram empregar equipamentos civis, pois notaram que a utilização de equipamentos militares resultavam em fogos de artilharia inimiga, segundo depoimento de Leandro Bortolassi, militar que atuou no *front* Rússia-Ucrânia: "A EW no front ucraniano não era consistente, havendo diferenças na intensidade de acordo com a prioridade da região. Em alguns pontos nós mesmos tínhamos rádios designados para captar e ouvir as conversas russas.

Em algumas regiões mais contestadas em que operei, onde haviam combates mais acirrados, o uso dos rádios modelos da Harris como PRC-152 foi deixado de lado.

Esse tipo de rádio apontava um sinal bem específico e intenso para os operadores de Guerra eletrônica russos que entendiam esse sinal como a presença de tropas de operações especiais.

Quando notavam que ali poderiam estar unidades especiais eles intensificavam a vigilância e o ataque sobre nós. Foi aí que boa parte das unidades OpEsp como a nossa decidiu utilizar rádios normais Motorola com criptografia mínima ou nenhuma criptografia.

Era um sacrifício dessa segurança da mensagem para camuflar o nosso sinal em meio as demais unidades convencionais na área de operações.

Ainda com o Motorola, uma técnica básica ainda se valia muito útil: não segurar o PTT continuamente por mais de 5s.

Era nítido que os grupos que não possuíam tal disciplina de rádio eram constantemente alvo de barragem de artilharia e drones FPV.

A complexidade do front se dava pelo fato de que a localização maioria dos Postos de comando nível companhia já era de conhecimento das forças inimigas. Por esse motivo periodicamente o comandante mudava sua posição para tentar evitar atrair atenção". (Bortolassi, 2024)

Figura 8 – Equipamento PRC-152 da L3Harris.
Fonte: https://www.l3harris.com/all-capabilities/falcon-iii-an-prc-152a-wideband-networking-handheld-radio

3 CONCLUSÃO

A utilização de rádios militares em operações táticas e estratégicas, apesar de essencial para a comunicação e coordenação das forças, apresenta riscos significativos devido às características específicas desses equipamentos que podem ser visualizadas no espectro eletromagnético. A principal vulnerabilidade está na possibilidade de detecção dos sinais emitidos, o que pode resultar na localização das tropas e comprometer a segurança e sucesso das operações. Além disso, a suscetibilidade a interferências e a guerra eletrônica adversária pode degradar a qualidade das comunicações ou até mesmo interrompê-las completamente.

Em conclusão, enquanto os rádios militares são ferramentas indispensáveis em campo, sua operação requer uma compreensão profunda dos riscos e a implementação de contramedidas rigorosas para assegurar a eficácia e segurança das comunicações em ambientes hostis.

Abstract

Signal signatures in military radios refer to the specific transmission characteristics that distinguish them from other equipment. These signatures are a key element of signals intelligence, allowing the identification and analysis of specific military communications. The use of military-grade radio equipment can pose security risks in combat, depending on the enemy's signal analysis and electronic warfare capabilities.

Keywords: *SIGNAL INTELLIGENCE, ELECTRONIC WARFARE, ELECTROMAGNETIC SPECTRUM*

4 REFERÊNCIAS

POISEL, Richard. **Introduction to Communication Electronic Warfare Systems**. Boston: Artech House, 2002. 573 p.

BRASIL. Exército. Estado-Maior. EB20-MC-10.207 Inteligência. 1. Ed. Brasília, 2015.

BRASIL. Exército. Estado-Maior. EB70-MC-10.201 A Guerra Eletrônica na Força Terrestre. 1. ed. Brasília, DF, 2019.

BRASIL. Exército. Estado-Maior. EB70-MC-10.247 A Guerra Eletrônica nas Operações. 1. Ed. Brasília, 2020.

BORTOLASSI, Leandro. Depoimento pessoal. Brasília-DF 2024.