O EMPREGO DE RÁDIOS DEFINIDOS POR *SOFTWARE* DE BAIXO CUSTO NO ENSINO DE GUERRA ELETRÔNICA

Major Fernando Henrique Castellani

O Major de Comunicações Castellani é o Chefe da Seção de Doutrina do Centro de Instrução de Guerra Eletrônica (CIGE). Foi declarado aspirante a oficial, em 2004, pela Academia Militar das Agulhas Negras (AMAN). É Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) e especializado em Sistemas de Radiocomunicação pelo Instituto Nacional de Telecomunicações (INATEL). É Instrutor do CIGE e atua nas áreas de Fundamentos, Análise de Sinais Especiais e Organização e Emprego de Guerra Eletrônica. Ao longo de sua carreira, dedicou-se a aprimorar métodos de ensino que permitam ao aluno aplicar prontamente a teoria assimilada por meio de simulações virtual e viva de baixo custo (castellani.fernando@eb.mil.br).

A necessidade de aumentar e melhorar a formação de profissionais de guerra eletrônica (GE) em todos os níveis está se tornando, cada vez mais, aparente, conforme observado nas tropas de países integrantes da Organização do Tratado do Atlântico Norte (OTAN), onde todo soldado em operações possui certo grau de envolvimento ou é afetado por atividades que ocorrem no espectro eletromagnético.

Independente dos sistemas de comando e controle (C2) utilizados, é vital que desde o militar mais moderno até a mais alta autoridade, presente em uma operação militar, possua meios de comunicações que forneçam um nível adequado de serviços, possibilitando o aumento das chances de sucesso das missões das tropas, bem como ampliando a consciência situacional dos comandantes. A constante e permanente utilização do espectro eletromagnético deve ser assegurada às forças amigas ao mesmo tempo em que os enlaces são localizados, explorados e, muitas vezes, negados quando utilizados pelas forças oponentes, cabendo essas tarefas aos especialistas de GE. O ensino dessa ampla gama de conceitos e tecnologias subjacentes de GE, muitas vezes, baseia-se em aulas teóricas sem permitir a prática, negligenciando ao aluno a oportunidade de adquirir vivência e experiência. Quando presente, a formação prática está frequentemente baseada em sistemas de alto custo, o que limita o número máximo de equipamentos disponíveis ou, em alguns casos, utiliza sistemas que, por sua complexidade, desencorajam a experimentação.

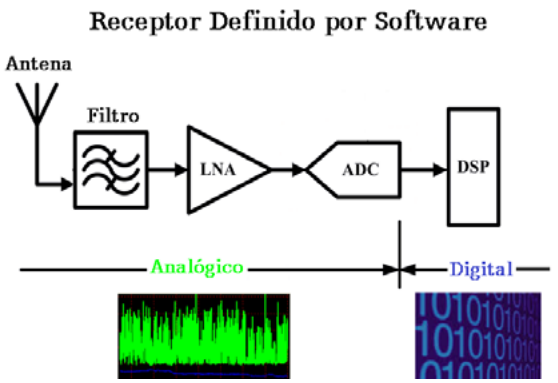
A DIGITALIZAÇÃO DO ESPECTRO ELETROMAGNÉTICO

Assim como o espaço aéreo, naval e terrestre, o espectro eletromagnético é usado como veículo para alcançar metas táticas ou resultados estratégicos. Possuir a superioridade no controle desta dimensão do combate é crucial para atingir a vitória.

Essa declaração, aparentemente simples, esconde a realidade de um ambiente rico em detalhes e extremamente complexo. O perfeito entendimento do espectro eletromagnético pelos profissionais de GE é uma condição *sine qua non* para executar ações de busca de vulnerabilidades, obtenção de informações e geolocalização de emissores por meio da utilização de medidas de apoio a guerra eletrônica (MAGE), assim como a realização de interferências, com o intuito de diminuir a capacidade de C2 ou a eficácia de sistemas de detecção de alvos, tais como radares e optrônicos, por meio do emprego de medidas de ataque eletrônico (MAE).

O foco das MAGE, de natureza totalmente passiva, é o reconhecimento e processamento do espectro eletromagnético, que, normalmente, ocorre por meio de componentes analógicos em equipamentos convencionais, mas que, em rádios definidos por *software*, é substituído pelo tratamento digital. Essa mudança proporciona uma série de vantagens na utilização de *software-defined radio* (SDR) em relação a sistemas tradicionais, como a possibilidade de atualizações, correção de erros e adição de novas funcionalidades apenas pela mudança de *software*, não necessitando substituições em nível de *hardware*.

A popularização de conversores analógicos digitais (ADC) e de processadores digitais de sinais (DSP) possibilitou uma forma ágil e acessível de digitalização do espectro eletromagnético, que depois de captado por uma antena passa por um filtro e um amplificador de baixo ruído (LNA), sendo transformado em *bits*. Esses dados podem ser totalmente manipulados por códigos que são executados em DSPs dedicados ou, como é o caso dos sistemas mais econômicos, mediante a utilização de um computador comum que se conecta ao *hardware* do SDR, usando uma porta USB ou cabo de rede.



O RÁDIO DEFINIDO POR *SOFTWARE* COMO FERRAMENTA DE ENSINO

Um dos objetivos das plataformas SDR é permitir e estimular o rápido desenvolvimento de novos sistemas, muitas vezes, com a livre divulgação dos diagramas de circuitos de *hardware*, bem como dos códigos fonte dos *softwares* envolvidos.

Porém, há exceções, como os receptores de televisão digital, que não têm suas informações amplamente divulgadas, mas que, em virtude do baixíssimo custo (R$ 100,00), são amplamente aproveitados como SDRs.

Esses receptores, conhecidos no mercado como RTL-SDRs por serem baseados no chip da fabricante *Realtek*, apresentam a possibilidade de processar uma largura de banda sem perdas de 2,4 MHz em frequências desde 24 MHz até 2GHz, encontrando uma vasta gama de possibilidades de aplicação nas MAGE.

Como o processamento do espectro digitalizado é todo realizado em um computador comum, os *softwares* podem agregar quase todo tipo de funcionalidades, desde a simples demodulação de sinais de voz em claro até a decodificação e classificação de protocolos digitais, ficando apenas limitados ao nível de conhecimento e à criatividade dos programadores.

Em decorrência da utilização desses pequenos espiões do espectro eletromagnético, vários conceitos podem ser fa-

cilmente identificados, comprovados e, exaustivamente, praticados pelo discente, desde as mais simples medições, como nível de potência e largura ocupada no espectro, até os mais complexos procedimentos, como a caracterização de protocolos de comunicação prioritariamente militares e o acesso a seus conteúdos.

Com a ampla divulgação de vários *softwares* gratuitos compatíveis com os RTL-SDR, como o SDRConsole, HDSDR, SDRUno e SDR#, e a criação, para este último, de *plug-ins* que acrescentam funcionalidades específicas relacionadas ao processamento, demodulação e decodificação, foi possível a criação de uma base de dados de sinais colaborativa que reúne amostras de todo o mundo: a *SIGIDWIKI*.

O Guia de Identificação de Sinais ou *Signal Identification Wiki* é um catálogo online que facilita sobremaneira o ensino da Análise Técnica, cujo foco é identificar características específicas e parâmetros em sinais digitais e analógicos, tais quais largura de banda, modulação, taxa de símbolos e frequência de utilização. Neste ambiente virtual, é possível encontrar amostras que estão divididas de acordo com sua principal finalidade, como sinais de radares, comunicações troncalizadas, rádio amador e outros sistemas militares e civis.

A popularização de Conversores Analógicos Digitais (ADC) e de Processadores Digitais de Sinais (DSP) possibilitou uma forma ágil e acessível de digitalização do espectro eletromagnético, que depois de captado por uma antena passa por um filtro e um amplificador de baixo ruído (LNA), sendo transformado em *bits*

Ao deparar-se com um sinal encontrado no espectro eletromagnético com o auxílio de um SDR, o aluno, futuro operador, planejador ou analista de GE, tem a possibilidade de encontrá-lo no guia e estudá-lo minuciosamente, principalmente, quanto à sua apresentação no espectro eletromagnético, adestrando sua audição e visão para cada família de sinais. Isto é possível devido ao fato de que há características comuns encontradas de acordo com a modulação utilizada, deixando uma espécie de "impressão digital" ou "rastro" do sinal na tela do *software*.

Com um custo um pouco mais elevado, da ordem de U$ 300,00 dólares, o KIWI SDR é uma plataforma dedicada à porção do espectro de HF, que abrange frequências de 3 a 30 MHz, e que opera junto a um processador dedicado, conhecido como *Beagle Bone*, além de possuir um GPS integrado ao sistema. O acréscimo no valor justifica-se pelo fato de não necessitar de um computador, podendo ser diretamente acessado de qualquer lugar do mundo quando integrado a um portal presente na web: o SDR.HU.

Esse SDR é operado por qualquer dispositivo que possua um navegador de internet e sua interface web, o OpenWebRx. Possui também funcionalidades comuns aos *softwares* que operam junto aos RTL-SDR e apresenta um recurso ímpar: a possibilidade de realizar a geolocalização de um emissor de RF utilizando a técnica de *Time Difference of Arrival* (TDoA, na sigla em inglês).

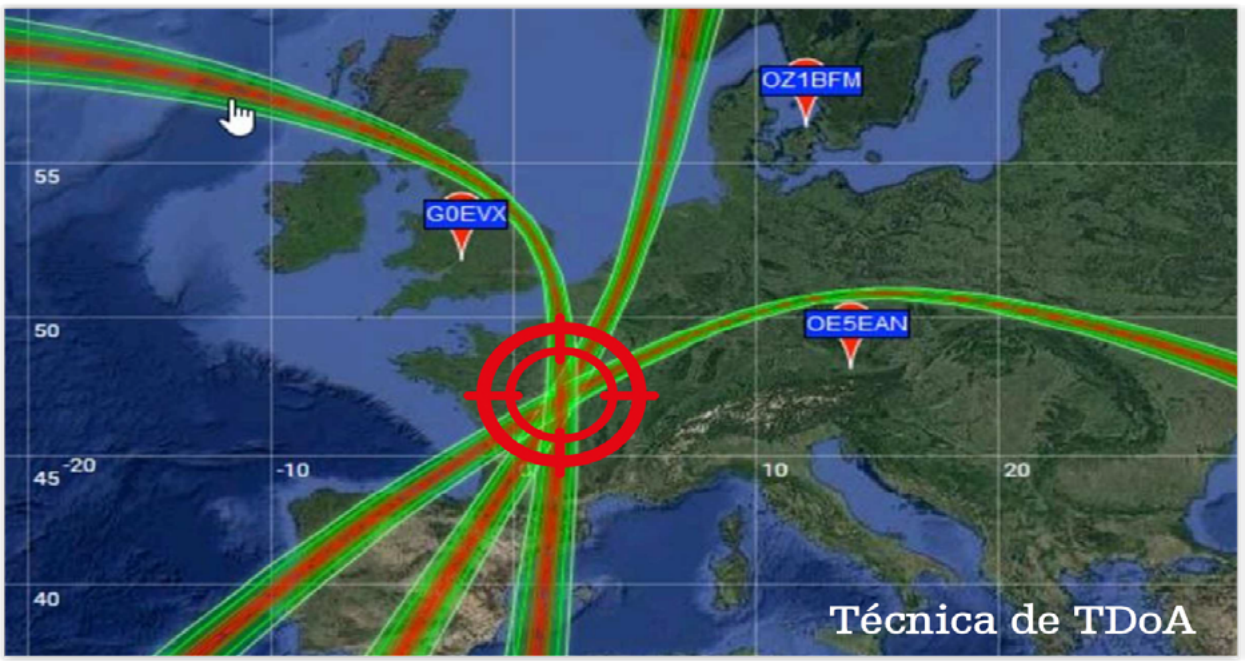
No TDoA, o alvo deve estar dentro de uma área de incerteza, geralmente, na forma de um triângulo, onde cada vértice terá um KIWI e esses três SDR trocarão informações em tempo real traçando três hipérboles que, com certo grau de precisão, irão se transpor e acusar o provável local do transmissor. Essa ferramenta permite o adestramento na técnica de *TDoA* a custo zero, bastando apenas o acesso ao portal presente na internet, mantido por voluntários, pesquisadores e *hobbystas*.

Mesmo o aluno que não é contemplado com um RTL-SDR pode realizar seu adestramento por meio do portal WebSDR.org, que segue a mesma linha colaborativa dos portais apresentados, disponibilizando centenas de SDRs a custo zero.

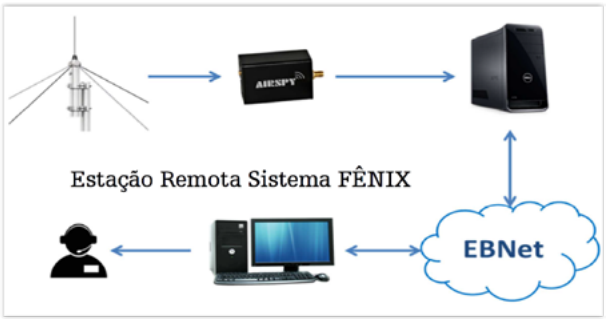
O PROJETO FÊNIX

Uma das tarefas do profissional de GE é manter atualizados os bancos de dados de sinais, alimentando constantemente a base de informações existente. Porém, há necessidade de coletar sinais em regiões que não apresentam uma infraestrutura adequada, além dos gastos com deslocamentos frequentes, o desgaste do pessoal envolvido e a vasta área a ser abrangida, o que torna esse tipo de missão quase que proibitiva.

Dispondo de RTL-SDRs, do *software* SDR# e do sentimento de cumprimento de missão, o 1º Ten Willian Fidêncio, do Núcleo do Centro Regional de Inteligência do Sinal (NuCRIS) do Comando Militar do Sul (CMS) idealizou uma forma de contornar os problemas apresentados,



dispondo sensores em locais distantes e operação remota com recepção das informações obtidas e processamento local centralizado, dando origem ao projeto batizado como FÊNIX.



As estações do FÊNIX são mobiliadas em áreas que dispõem de acesso à intranet do Exército Brasileiro (EBNet) e utilizam uma versão otimizada do chip *Realtek*, o *SDR AirSpy* que possibilita cobrir, em tempo real, uma faixa de 8 MHz do espectro eletromagnético, processando até 30 canais de comunicações simultaneamente. A utilização do *software SDR#* permite a demodulação de sinais digitais e a extração da mensagem de voz em protocolos digitais, como P25, DMR e TETRA, funcionalidade esta imprescindível para os trabalhos de análise realizados.

O custo total de uma estação de monitoração remota desse porte é inferior a seis mil reais, valor que, quando comparado a uma estação que utiliza equipamento militarizado com aplicações similares, é cerca de 250 vezes inferior, gerando grande economia e trazendo excelentes resultados.

O NOVO LABORATÓRIO DE SINAIS

Levando-se em consideração que o treinamento teórico é bastante limitado e não atende plenamente às necessidades do ensino por competências, que prima por desenvolver as capacidades basilares nos profissionais de GE, o CIGE adquiriu junto à empresa *Ettus Research*, que faz parte da *National Instruments*, SDRs da família USRP.

Esses rádios envolvem um custo elevado quando comparados aos citados anteriormente, mas trazem uma nova gama de recursos e capacidade de processamento. A faixa de frequências abrangida é de 70 MHz a 6 GHz, com largura de banda em tempo real até 56 MHz e 4 circuitos de RF simultâneos, sendo dois para recepção e dois para transmissão, com a possibilidade de serem programados e operarem sem a necessidade de um computador dedicado.

CONSIDERAÇÕES FINAIS

Com o novo Laboratório de Sinais do CIGE, além das atividades de adestramento em MAGE, como as conduzidas atualmente, também serão possíveis treinamentos de MAE em laboratório e estudo de medidas de proteção eletrônica frente aos ataques realizados, maximizando a experiência de aprendizado de todos os envolvidos e permitindo, também, a realização de pesquisa científica por parte do corpo docente.

Finalmente, o emprego dos USRPs poderá abrir novas formas de integração da guerra eletrônica e da guerra cibernética, uma vez que esses SDRs poderão ser utilizados para maximizar a eficiência de ataques conjuntos, bem como estender as formas de busca por vulnerabilidades em redes de C2.

REFERÊNCIAS

AIRSPY. **SDR#.** Disponível em: <https://airspy.com/download/>. Acesso em: 6 jun. 2019.

BRASIL, Exército. EB70-MC-10.201: **A Guerra Eletrônica na Força Terrestre**. Brasília, DF, 2019. Disponível em: <http://www.bdex.eb.mil.br/jspui/handle/123456789/3217>. Acesso em: 6 jun. 2019.

Centro de Instrução de Guerra Eletrônica. Disponível em: <http://www.ccomgex.eb.mil.br/index.php/centro-instrucao-guerraeletronica>. Acesso em: 6 jun. 2019.

Ettus Research. Disponível em: <https://www.ettus.com/>. Acesso em: 6 jun. 2019.

National Instruments. Disponível em: <https://www.ni.com/pt-br.html>. Acesso em: 6 jun. 2019.

OpenWebRX Online Receivers. Disponível em: <https://sdr.hu/>. Acesso em: 6 jun. 2019.

RTL-SDR (RTL2832U) and software defined radio news and projects. Disponível em: <https://www.rtl-sdr.com/>. Acesso em: 6 jun. 2019.

Receptor HF online de Brasília. Disponível em :<http://brasilia.proxy.kiwisdr.com:8073/>. Acesso em 19 dez. 2019.

SDR console. Disponível em: < https://www.sdr-radio.com/>. Acesso em: 6 jun. 2019.

Signal Identification Guide. Disponível em: https://www.sigidwiki.com/wiki/Signal_Identification_Guide>. Acesso em: 6 jun. 2019.

SPRECKELSEN, Malte Von. **Electronic Warfare - The Forgotten Discipline**. JAPCC Journal 27. Disponível em: <https://www.japcc.org/electronic-warfare-the-forgotten-discipline/>. Acesso em: 6 jun. 2019.

WebSDR RTL-SDR Online. Disponível em: <http://www.websdr.org/>. Acesso em: 6 jun. 2019.