O PAPEL DA GUERRA ELETRÔNICA DE COMUNICAÇÃO NO CONFLITO RÚSSIA-UCRÂNIA

*Por Jorge Luiz Schwerz**

Imagem conceitual (ELT).

Nos conflitos atuais, a Guerra Eletrônica tem papel cada vez mais preponderante na multiplicação de força dos oponentes – ou da falta dela.

O conflito Rússia-Ucrânia trouxe para o nosso cotidiano um embate clássico entre Estados que há muito tempo não presenciávamos. É um conflito no século XXI, mas que nos remete a guerras mais antigas.

Essa foi a sensação que tive ao ler a reportagem feita pela *BBC*[1], publicada em maio de 2023, sobre o uso, por tropas ucranianas, dos famosos telefones de campanha ligados por fio, reminiscentes das guerras do século XX (Figuras 1 e 2).

Após mais de 600 dias do conflito, algumas realidades começam a se apresentar para os profissionais que estudam a guerra. Hoje, já podemos falar com alguma certeza sobre a guerra invisível travada nos campos europeus: a guerra eletrônica.

A "guerra dos bruxos", como Winston Churchill costumava dizer, continua mais viva do que nunca e a utilização do telefone de campanha em um conflito moderno é apenas um dos indicativos. Vamos entender os motivos pelos quais os ucranianos, em plena era digital, recorrem ao telefone ligado por fio.

[1] ***BEALE**, Jonathan. Ukraine war: How old tech is helping Ukraine avoid detection. BBC, 2023. Disponível em: https://www.bbc.com/news/world-europe-65458263.*

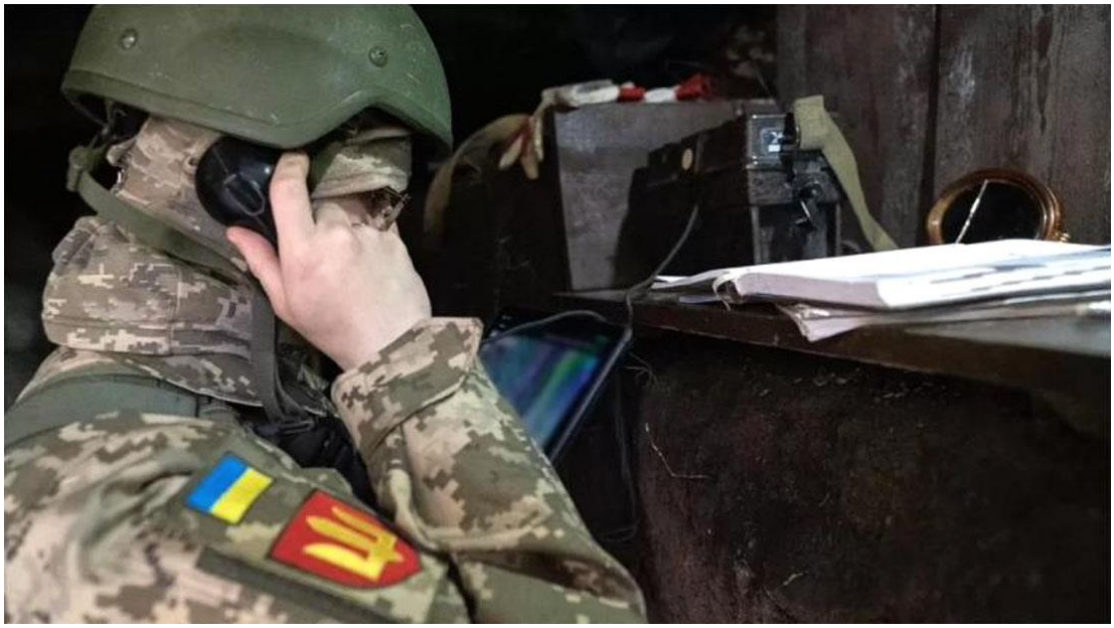

FIGURA 1: Militar ucraniano faz uso de telefone de campanha.

FIGURA 2: Exemplo de telefone de campanha.

Embora muitas vezes não percebamos, a onda eletromagnética faz parte do nosso dia a dia. Quando sintonizamos o rádio em uma estação AM/FM, é uma onda eletromagnética que traz as informações até o aparelho. Quando falamos ao celular, é uma onda eletromagnética que transmite a informação até a torre de transmissão.

Nos teatros de operações atuais, as armas mais modernas utilizam a onda eletromagnética. Desde sistemas de artilharia até mísseis de alta precisão, passando pelos radares das aeronaves de combate, etc. Esses sistemas usam ondas de rádio, ondas milimétricas, infravermelho ou outras frequências que permitem receber e enviar dados para a sua operação.

A guerra eletrônica consiste em usar as ondas eletromagnéticas a favor das forças amigas, protegendo o seu uso das forças inimigas e utilizando-as para reduzir o poder de combate do adversário.

A Guerra Eletrônica (GE) é um campo de estudo complexo que pode ser dividido em três pilares principais para facilitar o entendimento.

O **primeiro pilar** são as Medidas de Apoio de Guerra Eletrônica (MAGE). Essas medidas visam a obter dados e informações a partir das emissões eletromagnéticas utilizadas pelo oponente. Para isso, são usados sensores passivos para receber e analisar as emissões inimigas.

O **segundo pilar** são as Medidas de Ataque Eletrônico (MAE). Essas ações têm como objetivo impedir ou reduzir o uso efetivo do espectro eletromagnético do inimigo. Isso pode ser feito através da destruição, neutralização ou degradação da capacidade de combate do inimigo usando energia eletromagnética ou armamento que empregue a emissão intencional do alvo para seu guiamento. A conhecida interferência eletrônica é um dos seus exemplos.

O **terceiro e último pilar** são as Medidas de Proteção Eletrônica (MPE). Essas medidas buscam garantir o uso efetivo (ativo e passivo) do espectro eletromagnético. Um exemplo disso é o uso do telefone de campanha pelas forças terrestres ucranianas para evitar a interceptação das transmissões pelos russos.

A Guerra Eletrônica das Comunicações (GE Com) é um exemplo de como esses pilares são aplicados na prática.

O primeiro passo das ações de GE Com, dentro das MAGE, é a utilização de receptores passivos especializados para realizar a busca de interceptação. Isso significa “escutar” as frequências usadas pelo inimigo e, ao encontrar uma frequência que esteja sendo usada, interceptar a emissão.

O segundo passo é monitorar a transmissão inimiga interceptada e localizar a sua posição. Para isso, é necessário fazer a triangulação do emissor, utilizando outros postos de escuta eletrônica ou um meio móvel que permita fazer a triangulação (Figura 3). O resultado é uma área provável de localização das emissões inimigas em formato de elipse, que será detalhada no próximo passo.

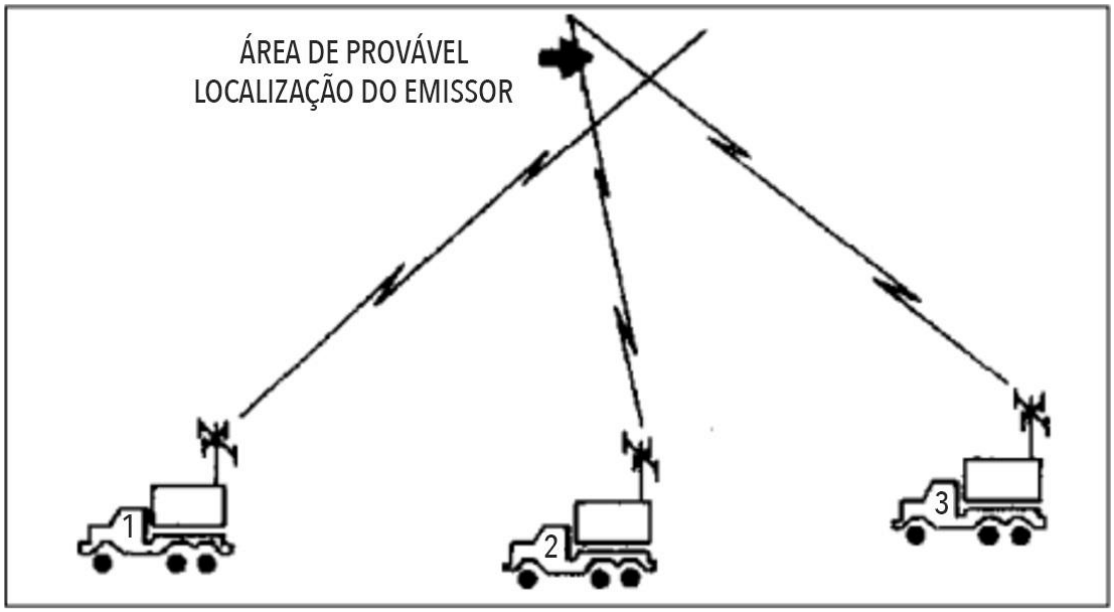

FIGURA 3: A triangulação de uma emissão inimiga permite encontrar a localização do emissor.

O passo seguinte é a fase mais detalhada do trabalho do guerreiro eletrônico, pois analisa quem transmite e quem recebe nos postos inimigos e suas identificações, quais são as mensagens transmitidas e a localização detalhada dos postos de comando, definindo com detalhes:

- Quais transmissores são postos de comando e quais são os subordinados;
- A localização detalhada dos postos inimigos no terreno;
- A composição de cada unidade militar; e
- As possibilidades do inimigo, ou seja, se pretende atacar, se pretende ficar estacionário, etc.

A fase final das ações de GE Com é o registro dos dados coletados e sua difusão para os órgãos que decidirão as ações a serem tomadas a seguir. O resultado do trabalho realizado pelo guerreiro eletrônico pode ser uma ação que destrua fisicamente a unidade militar que faz uso do posto de transmissão, uma ação de ataque eletrônico, bloqueando com interferência para impedir a utilização do equipamento de transmissão ou um despistamento que engane o inimigo.

Atualmente, os russos têm obtido grande sucesso nas operações táticas de GE Com. De acordo com os ucranianos, os russos foram parcialmente bem-sucedidos em destruir os sistemas de comunicação e controle da Ucrânia nos primeiros dias da guerra. Embora algumas redes militares de satélite tenham sido bloqueadas, as comunicações celulares e pela Internet não foram afetadas[2]. No entanto, com a consolidação do Teatro de Guerra do leste da Ucrânia, essa realidade mudou e muitas alternativas de comunicação têm sido negadas ao Exército ucraniano pela grande infraestrutura de GE Com distribuída pela Rússia.

[2] ***ABDURASULOV**, Abdujalil. Ukraine war: How old tech is helping Ukraine avoid detection. BBC, 2023. Disponível em: https://www.bbc.com/news/world-europe-66279650.*

Um dos exemplos mais marcantes é que, no início dos combates próximos às cidades mais movimentadas, o deslocamento de tropas russas era informado ao Exército ucraniano por meio de telefones celulares.

FIGURA 4: Sistema Leer-3 e ARP Orlan-10 e FIGURA 5: ARP Orlan-10 sendo lançado.

FIGURA 6: Sistema Leer-3 e ARP Orlan-10.

Quais são os equipamentos de Guerra Eletrônica de Comunicação utilizados pelos russos[3]?

Não poderíamos deixar de começar pelo "RB-341V Leer-3", que é um sistema de guerra eletrônica construído com base na Aeronave Remotamente Pilotada (ARP) Orlan-10 (Figuras 4, 5 e 6) O ARP é utilizado para ampliar o raio de ação do

[3] ***MAKSIMOV***, *Ilya. Combatentes de guerra eletrônica: porque os sistemas de guerra eletrônica são necessários e como eles funcionam. Disponível em: https://rg.ru/2023/08/28/sredstva-radioelektronnoy-borby-reb-zachem-nuzhny-i-kak-rabotaiut.html.*

equipamento, cuja função é interceptar, monitorar, localizar e analisar comunicações de aparelhos celulares, montando um mapa digital a ser informado aos comandantes da área de operação. Esse sistema pode ser usado para bloqueio, despistamento ou até mesmo para orientar um ataque físico à posição de concentração dos telefones portáteis UHF (300-3000 MHz).

O Orlan-10 também pode realizar reconhecimento por imagens e auxiliar no ajuste de tiro de artilharia.

Exemplos da atuação do Leer-3 podem ser destacados durante a insurgência de 2014–2022 no leste da Ucrânia, quando as forças russas enviaram propaganda e ordens falsas a tropas e civis, sequestrando a rede celular local[4].

E, após o início da invasão russa, houve diversos relatos sobre ataques dos russos a agrupamentos de telefones celulares e muitas dessas informações nasceram do trabalho do Sistema Leer-3.

Da mesma forma, o "RB-301B Borisoglebsk-2", que se diferencia dos demais por ser instalado em blindado sobre lagartas (R-330KMV). Trata-se de um sistema automatizado de inteligência de sinais, responsável por interceptar, monitorar, localizar e analisar as comunicações inimigas. Seu objetivo é bloquear ou despistar as comunicações de rádio nas faixas HF (3-30 MHz) / VHF (30-300 MHz) em frequências utilizadas por tropas terrestres e aeronaves, operando nos níveis tático e operacional[5] (Figuras 7 e 8).

FIGURAS 7 e 8: Sistema de GE russo RB-301B Borisoglebsk-2.

Por outro lado, o conhecido "R-330Zh Zhitel" é um sistema de Guerra Eletrônica com a função de interceptar, monitorar, localizar e analisar as comunicações inimigas. Ele atua no bloqueio ou despistamento de sinais de rádio VHF (30-300

[4] ***CLARK***, *Bryan. The Fall and Rise of Russian Electronic Warfare. IEEE Spectrum, 2022. Disponível em: https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare.*

[5] ***McDERMOTT***, *Roger. Russia's Electronic Warfare Capabilities to 2025 - Challenging NATO in the Electromagnetic Spectrum. ICDS. 2017. Disponível em: https://icds.ee/en/russias-electronic-warfare-capabilities-to-2025-challenging-nato-in-the-electromagnetic-spectrum/.*

MHz) / UHF (300-3000 MHz), incluindo comunicações via satélite, GPS (UHF) e telefonia móvel (UHF), em um raio estimado de 25 km[5] (Figuras 9 e 10).


FIGURAS 9 e 10: Sistema de GE russo R-330Zh Zhitel.

O sistema "R-934B" também faz parte da GE, com a função de interceptar, monitorar, localizar e analisar as comunicações inimigas. Seu foco é o bloqueio ou despistamento de sinais de rádio VHF (30-300 MHz) / UHF (300- 3000 MHz)[5] (Figuras 11, 12 e 13).


FIGURAS 11 e 12: Montagem do sistema de GE russo R-934B.

Além disso, temos o sistema "Torn MDM", que visa a interceptar, monitorar, localizar e analisar as comunicações inimigas atuando no bloqueio ou despistamento de sinais de rádio VHF (30-300 MHz) / UHF (300-3000 MHz). Relatos das forças ucranianas indicam que o sistema conseguiu interceptar e decodificar os rádios portáteis Motorola com codificação de 256 bits[6] (Figuras 14 e 15).

[6] ***WATLING**, Jack; **REYNOLDS**, Nick. Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. RUSI, 2017. Disponível em: https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine.*

FIGURA 13: Sistema de GE russo R-934B.

FIGURAS 14 e 15: Sistema de GE russo Torn – MDM.

Por fim, o renomado "Murmansk-BN" é um sistema de guerra eletrônica russo montado na Criméia, ao sul de Sebastopol[7] (Figura 18). Sua principal função é interceptar, monitorar, localizar, analisar e bloquear as transmissões de HF (3-30MHz) das forças da OTAN, especialmente o Sistema de Comunicação Global dos EUA. Estima-se que tem um alcance de 5.000 a 8.000 km[7], sendo que o grande alcance é obtido pela reflexão ionosférica utilizada pelas transmissões HF. Suas antenas de 32 m de altura são uma característica marcante.

[7] *MURMANSK-BN. Electronic warfare communications jamming system – Russia. Army Recognition, 2023. Disponível em: https://www.armyrecognition.com/russia_russian_military_field_equipment/murmansk-bn_electronic_warfare_communications_jamming_system_data.html#google_vignette.*

Cada complexo Murmansk-BN opera com um conjunto de quatro antenas, podendo trabalhar com outros conjuntos de antenas, perfazendo o máximo de 16 antenas no total (Figuras 16 e 17).

FIGURAS 16 e 17: Caminhões Kamaz, base de uma das antenas de 32 m de altura do Sistema de GE russo Murmansk e conjunto de quatro antenas montado.

Os esforços ucranianos para proteger a comunicação tática ficaram restritos, além da utilização dos telefones de campanha, à incorporação de rádios Motorola com codificação de 256 bits e à adoção do *Single Channel Ground and Airborne Radio System* (SINCGARS), o rádio utilizado pela OTAN. Embora as tropas ucranianas já tivessem treinado com o SINCGARS, o acesso a esse equipamento foi incrementado após a invasão russa.

FIGURA 18: Dois conjuntos de quatro antenas do Sistema de GE russo Murmansk.

O SINCGARS possui criptografia integrada e, para proteger contra interceptação, análise e interferência inimiga, utiliza salto de frequência, podendo mudar de frequência até 100 vezes por segundo na faixa VHF de 30 a 88 MHz[4].

No entanto, o principal esforço das Forças Terrestres ucranianas em Guerra Eletrônica é localizar e eliminar os equipamentos russos que interferem em suas

transmissões e reduzem a precisão dos armamentos guiados por GPS[2]. Para isso, utilizam as MAGE, que envolvem o uso de receptores passivos para interceptar as emissões dos equipamentos russos de Guerra Eletrônica e localizá-los para um possível ataque ucraniano.

Muitos dos equipamentos utilizados pelos ucranianos são antigos sistemas de GE russos, que acabaram virando "Frankensteins" com adaptações de equipamentos eletrônicos e sensores ocidentais (Figuras 19, 20 e 21).

FIGURA 19: Ucranianos montam antena de recepção para interceptação de sinais de comunicação russos, e FIGURA 20: Técnico em GE ucraniano finalizando montagem de sistema de GE.

FIGURA 21: Especialista em GE ucraniano analisa emissões russas interceptadas.

Logo no início da invasão, em março de 2022, as tropas ucranianas capturaram o sistema Torn-MDM e consideram os sistemas de Guerra Eletrônica russos

Borisoglebsk-2, Zhitel e Pole-21[8] (este específico para interferência em sistemas orientados por GPS) como alvos prioritários de alto valor, estando continuamente à procura destes equipamentos.

Alguns questionam por que os países da OTAN não entregam seus equipamentos de Guerra Eletrônica mais modernos à Ucrânia. No entanto, se isso não aconteceu até agora, fica claro que os países que podem fornecê-los não querem permitir que as forças da Federação Russa conheçam as técnicas e capacidades de seus sistemas de GE mais avançados. Esses conhecimentos são tratados como verdadeiros segredos de Estado.

Desta forma, vemos a eterna luta de gato e rato entre Rússia e OTAN, com um dos lados tentando superar o outro a cada nova descoberta. A certeza é que a Guerra Eletrônica tem um papel cada vez mais preponderante na multiplicação da força dos oponentes ou da falta dela, como disse Yaroslav Kalinin, um representante ucraniano da Infozahyst: "Se você está perdendo na Guerra Eletrônica suas forças retornam para um Exército do Século XIX ... você estará dez passos atrás do seu inimigo."[2]

Esta declaração nos remete ao início deste artigo, reforçando a necessidade de as tropas ucranianas utilizarem os antigos telefones de campanha ligados por fio como contraponto ao poderio de Guerra Eletrônica de Comunicação das forças russas.

***Jorge Luiz Schwerz** é coronel-aviador veterano da Força Aérea Brasileira, MsC em Guerra Eletrônica pelo ITA, ex-adido de Defesa e Aeronáutica na França e na Bélgica e coordenador do Canal Ao Bom Combate!*

[8] ***NIKOLOV**, Boyko. Borisoglebsk-2, Zhitel, Pole EW stations are Ukraine's first target. Bulgarian Military, 2023. Disponível em: https://bulgarianmilitary.com/2023/07/23/borisoglebsk-2-zhitel-pole-ew-stations-are-ukraines-first-target/.*