



GUERRA ELETRÔNICA — O episódio Traíra poderia ter sido evitado? (*)

James Correa Caldas

Com base no episódio Traíra, o autor põe em foco a importância da Guerra Eletrônica na defesa da integridade da Amazônia.

INTRODUÇÃO

Aproximadamente às doze horas do dia 26 de fevereiro de 1991, terça-feira, um grupo de 34 homens, supostamente pertencente às FARC (Forças Armadas Revolucionárias da Colômbia) atacou, com fogo de armas automáticas, um destacamento do 3º PelEspFron/1º BtlEspFron (3º Pelotão Especial de Fronteira do 1º Batalhão Especial de Fronteira). Do episódio, três soldados foram mortos e nove ficaram feridos. Os guerrilheiros ainda levaram transceptores rádio, munição, uniformes e armamento leve que estavam em poder dos soldados brasileiros.

(*) Selecionado pelo PADECEME

O ataque foi realizado por três colunas, as quais incursionaram através do Rio Traíra empregando táticas militares. Uma ocupou posição na margem colombiana do rio, enquanto as outras duas progrediram pela selva na direção do acampamento.

Deflui-se do ocorrido que os guerrilheiros planejaram a operação com certo requinte, incluindo um minucioso reconhecimento da área, prevendo rotas de fuga e um conhecimento detalhado da rotina dos soldados brasileiros.

O cenário do episódio é dominado por uma floresta densa, banhada por rios e igarapés encachoeirados. Nesse ambiente, torna-se difícil a condução de uma operação militar sem um adequado suporte de comunicações rápidas e confiáveis.

GUERRA ELETRÔNICA

A operação em tela foi precedido conforme já mencionado, de intensos reconhecimentos na área. Nessas ocasiões, provavelmente, os guerrilheiros fizeram largo emprego do rádio para efetuar suas ligações.

As ligações rádio foram feitas, em grande parte, com equipamentos civis, na faixa de frequência de 3 a 30MHz e, certamente, utilizando a modulação SSB (*Single Side Band*). Pode-se afirmar, ainda, que as comunicações rádio dos guerrilheiros eram feitas em claro ou empregando códigos bastante rudimentares. Com respeito à proteção das emissões rádio, pode-se afirmar, com grande dose de certeza, que os agressores não empregaram as CCME (contra-contramedidas eletrônicas), sejam os procedimentos ou tecnologias, já que os equipamentos civis são desprovidos desses recursos.

Percebe-se, portanto, que as forças clandestinas estavam completamente vulneráveis à ação de Guerra Eletrônica, que poderia: localizar os emissores; monitorar as comunicações; acompanhar os deslocamentos; levantar possibilidades, vulnerabilidades e intenções; impedir o uso do rádio, mediante ações de interferência, e dificultar a coordenação das forças hostis, através de ações de dissimulação eletrônica bem planejadas, prática utilizada no desembarque da Normandia (IIGM) pelos Aliados e, recentemente, na invasão do Iraque pelas forças terrestres da coalizão, lideradas pelos EUA.

As possibilidades da Guerra Eletrô-

nica são incomensuráveis, bastando, tão somente, que o oponente empregue as ondas de rádio. Os equipamentos emissores de ondas eletromagnéticas, particularmente transmissoras de rádio e radares, possuem uma "assinatura eletrônica", tal qual uma impressão digital. É de se supor que uma força mal-adestrada no emprego de meios de comunicações rádio (transmitindo mensagens em claro e longas, usando palavreado típico, sem qualquer codificação, sem o emprego de procedimentos e tecnologias de CCME) forneça grande quantidade de informações pelo rádio, que, se interceptadas, poderão revelar toda a sua ordem de batalha, e, mesmo, o seu plano de operação.

MEDIDAS ELETRÔNICAS DE APOIO (MEA)

As MEA compreendem, entre outras, ações de interceptação, monitoração e localização eletrônicas. Elas constituem o reconhecimento eletrônico que, à semelhança das patrulhas de reconhecimento, estendem os seus ouvidos além da linha de contato e linha de fronteira e auscultam e escutam as emissões adversárias.

A presença de sensores de comunicações no País, voltados para a atividade de MEA, monitorando toda a faixa de HF (High Frequency — 3 a 30MHz), 24 horas por dia, poderiam perceber toda e qualquer ameaça contra o território ou o patrimônio nacional. Naturalmente que, por trás dos equipamentos, há de se ter equipes com

analistas, que sejam especialistas em Guerra Eletrônica, conheçam o idioma do oponente e tenham suficiente preparo para produzir inteligência do sinal a partir das interceptações eletrônicas.

Os sensores para realizar as ações de MEA devem localizar-se em posições estratégicas que lhes permitam interceptar as emissões de interesse em boas condições. A região amazônica, muito cobiçada no momento, deve receber atenção especial nesse particular, a fim de que outros episódios, como o de Traíra, não se repitam.

Sensores em plataformas aéreas são muito eficientes, pois possibilitam a interceptação eletrônica a distâncias mais longas, podendo-se dizer, de antena a antena, porquanto os acidentes de relevo não interferem na ligação terra-avião.

EMPREGO DA GUERRA ELETRÔNICA

Equipamentos de Guerra Eletrônica em instalações fixas, veiculares, portáteis ou em plataformas aéreas, monitorando emissões em qualquer área, podem, a partir de um tempo "T", organizar um banco de dados e, assim, acompanhar todos os passos de um possível oponente.

Por mais adestrada e mais bem doada em meios de comunicações que seja, uma força guerrilheira não consegue dissimular suas intenções após certo tempo de emprego do rádio. As mensagens via rádio, nesse nível, são auto reveladoras. A radiografia das ati-

vidades guerrilheiras será facilitada se os órgãos interessados organizarem um banco de dados do oponente, a partir de hábitos, rotinas, tipo e origem dos equipamentos, doutrina e outros dados afins.

A simples monitoração de uma rede-rádio adversária permitirá ao analista descobrir: como está organizado o seu sistema de comando; quem é o seu Cmt; onde estão as suas principais instalações, e qual a sua direção e a velocidade de deslocamento.

Os próprios radioperadores possuem modos de falar que os individualizam. Associando os operadores com os equipamentos dotados de assinatura eletrônica, pode-se identificar os pessoal e, por conseguinte, o órgão que está por trás de determinado tranceptor rádio. A partir da identificação de um oponente, bem como das suas intenções, é possível neutralizar suas ações, pela interferência eletrônica ou pelos métodos tradicionais do fogo e do movimento.

CONTRAMEDIDAS ELETRÔNICA (CME)

As CME constituem a parte ofensiva da Guerra Eletrônica. Com elas pode-se, por exemplo, interromper as ligações rádio de uma força ou, mesmo, realizar uma dissimulação eletrônica que, se for imitativa, pode provocar um verdadeiro caos no sistema de comando adversário.

Na selva, entretanto, são bastante limitadas, uma vez que as folhagens absorvem grande parte da energia ir-

radiada pelos transmissores. Além do mais, uma ação de interferência, se mal planejada, pode denunciar seu autor e se tornar uma arma contra ele próprio, como efeito bumerangue.

Em plataformas aéreas, as ações de interferência terão alguma eficácia, mas seu emprego nessas condições apresenta, também, algumas restrições.

MEIOS

O Brasil dispõe de meios para produzir inteligência a partir de interceptações eletrônicas?

A resposta é sim.

Com algumas limitações, essa atividade pode ser feita desde já. Basta que o País se apóie nas estações móveis e fixas de alguma rede de monitoragem do atual Ministério da Infra-Estrutura. Os postos seriam posicionados em vários pontos do território nacional, particularmente próximo à fronteira norte. A médio prazo, o País terá, entretanto, que adquirir equipamentos mais modernos e mais confiáveis, que possam vasculhar o espectro eletromagnético de forma ágil, precisa e seletiva.

Para atender à atual conjuntura, uma solução seria instalar estações de monitoragem na fronteira norte, com ênfase nas cidades de Rio Branco, Tabatinga, Vila Bittencourt, São Gabriel da Cachoeira e Boa Vista. A coordenação regional dessas estações poderia ser feita de Manaus. O mesmo raciocínio poderia ser estendido para a parte meridional do país. A coordenação do sistema, como um todo, se-

ria feita em Brasília, que também teria sensores com grande sensibilidade e antenas adequadas para, se possível, interceptar mensagens de qualquer ponto do território nacional.

CONCLUSÃO

O assunto não se esgota neste modesto ensaio. Muito ainda pode ser dito, feito e aprendido. Existem sérios desafios a vencer, particularmente com respeito à aquisição de equipamentos, treinamento de pessoal e o desenvolvimento de uma mentalidade voltada para a produção do conhecimento por meio da interceptação eletrônica.

O Brasil dispõe de um patrimônio de valor inestimável, que é a região amazônica. A Comunidade internacional está, qual tenciona fazer com a Antártica e já o fez com a África, pronta para partilhar a região e assumir, cada qual, um quinhão. A Guerra Eletrônica, se for tratada com prioridade e bem gerenciada, pode, com um mínimo de recursos, face ao nobre objetivo, contribuir sobremaneira para que o maior santuário da natureza permaneça nas mãos do seu verdadeiro dono.

E por que a Guerra Eletrônica pode contribuir de forma tão relevante na solução de outros contenciosos tipo Traíra? Porque é consensual nos dias atuais que mais de 50% das informações produzidas na paz, em situação de crise e na guerra, decorrem da Guerra Eletrônica. Cabe então a pergunta: por que esperar que ocorram outros Traíras?



JAMES CORREA CALDAS, Tenente-Coronel da Arma de Comunicações. Possui os seguintes cursos: AMAN (1970), Básico Pará-queda (1973), Mestre de Salto (1974), Estágio Básico de Salto Livre (1976), EsAO (1979), ECEME (1986), Guerra Eletrônica na Alemanha (1988) e nos EUA (1991). Exerceu as seguintes funções: Instrutor da Escola de Comunicações (1977/1978 e 1981), Cmt da 7ª Cia Com (1982/1983), Membro do EMG da 7ª RM/7ª DE (1987/1988). Atualmente é Instrutor do Centro de Instrução de Guerra Eletrônica (CIGE).

Quem trabalha pela segurança do país tem que ter mais tranquilidade.

Quem trabalha tanto pela segurança do país sabe que a qualquer momento pode contar com a agilidade e eficiência do GBOEX. Planos de saúde, seguros ou pecúlio, faça o seu com a maior empresa de previdência privada da América Latina, ao lado das Forças Armadas há 78 anos. Na hora de pensar no futuro, a experiência do GBOEX é a sua segurança.

GBOEX. CONFIANÇA NO PRESENTE, SEGURANÇA NO FUTURO.



**GRÊMIO
BENEFICENTE**