

# Guerra Eletrônica na Guerra Assimétrica

Capitão-de-Corveta (FN) AUGUSTO FORTUNA BARBOSA  
Instituto Tecnológico de Aeronáutica, ITA, São José dos Campos, SP

**Resumo – Nos tipos de guerra irregular e assimétrico, se processa o rompimento da mais velha convenção: a guerra como assunto exclusivo dos militares, onde se faz o emprego exclusivo de armas militares. Ambas não são conduzidas exclusivamente por militares e não usam, em todos os casos, armamentos militares.**

Objetivo da Guerra Assimétrica – O objetivo da guerra é impor uma vontade. De forma mais clara, o objetivo da guerra assimétrica é o mesmo da guerra irregular, ou seja, exaurir o inimigo, desgastá-lo internamente, de tal modo que, com o correr do tempo, ele estará enfraquecido de tal forma, não só física como psicologicamente, que se mostrará incapaz de uma volição política. O objetivo central é a imobilização operacional do adversário. A imobilização do adversário significa sempre numa guerra o começo da vitória. Assim o é também na guerra assimétrica.

Ao término da guerra assimétrica se tem muito mais uma vitória política do que uma vitória militar. A guerra assimétrica é muito mais a guerra do político. Por isso, quem conduzir uma guerra assimétrica deve procurar evitar testes diretos de poder e buscar e, em vez disso, tirar a estabilidade, surpreender, exaurir o adversário, para desequilibrá-lo. O seu maior objetivo deve ser o de mitigar intelectual e moralmente o adversário.



A guerra eletrônica está se adaptando à guerra assimétrica; por isso, o combate está se tornando diferente do tradicional MAGE-MAE-

MPE devido ao desenvolvimento das comunicações comerciais e de sistemas eletrônicos, atualmente muito utilizados por terroristas e paramilitares. Novos sistemas de controle e *hackers*, bem como dispositivos de controle por celular estão sendo usados. Vários sistemas têm sido desenvolvidos na Europa.



Novos sistemas de guerra eletrônica e de inteligência de sinais em celulares são demonstrados pela *Tadiran Electronic Systems*, uma subsidiária do Grupo Elisra, eu tem desenvolvido tais tecnologias como resultado da luta de Israel contra o terrorismo. Esses novos sistemas permitem os militares e autoridades policiais a rastrear e interceptar ligações de celulares suspeitas. Ao contrário da utilização da guerra eletrônica por “força bruta”, que tem como objetivo interferir em comunicações ou bloquear contra interferências, os novos sistemas empregados são capazes de garantir as ligações das forças amigas ao mesmo tempo em que bloqueia contra telefones celulares suspeitos ou não autorizados. Quando um emissor é considerado suspeito, ele pode ser localizado, interferido e inutilizado pelo Localizador Passivo Portátil Elisra, que ainda é capaz de direcionar os sinais de interferência para a fonte suspeita, ou pode ser utilizado o Collective, um telefone celular de interferência seletivo para atenuar o emissor suspeito sem a necessidade de localizá-lo. Esse novo dispositivo permite a interferência por “intervenção cirúrgica”, ou seja, sem denunciar a

venção cirúrgica”, ou seja, sem denunciar a posição ou interferir no tráfego civil.

Um outro sistema, que pode ser usado como uma Medida de Proteção Eletrônica – MPE, é o Sistema Eletromagnético de Alta Potência (HEPM), fabricado pela Diehl e Rheinmettal Defense. Este sistema é utilizado contra bombas eletromagnéticas ou contra interferidores contendo dispositivos eletrônicos (como em um telefone celular ou outro dispositivo). O HEPM consiste basicamente de um sistema interferidor que causa uma explosão controlada ou uma descarga a uma distância segura de uma viatura. Rheinmettal and Diehl ainda disponibilizam vários módulos, incluindo acessórios que podem ser instalados nas portas ou no painel de viaturas policiais. Esses sistemas possibilitam a interceptação de um veículo suspeito quando se locomovendo lado a lado. Um sistema similar pode ser utilizado para a proteção de um veículo de interferidores. Sistemas diferentes estão sendo desenvolvidos por ambas as empresas para oferecer cobertura de banda extremamente larga, de Megahertz a Gigahertz, bloqueando efetivamente quaisquer sinais de comunicações. Outro sistema é a bateria operacional DS-110, que destrói qualquer módulo de dispositivo diretor de tiro, neutralizando o alvo. O sistema é basicamente omni-direcional mas pode ser configurado a irradiar em uma determinada direção.



### Inteligência no Combate em Localidade



Guerrilhas urbanas têm aprendido a utilizar os benefícios de um Centro de Comunicações, com tecnologias modernas como redes sem fio, celulares e internet. Suas comunicações fundem o tráfego comercial com monitoragem de sinais. Conforme acordos comerciais e legais, especialistas em inteligência de sinais podem monitorar ligações comuns para alimentar um banco de dados. A inteligência de sinais requer um equipamento especial que simula uma ligação de telefone celular, discriminando o tráfego comercial sem o conhecimento do assinante, e então a ligação é analisada e inserida no tráfego comercial novamente. Esse processo possibilita a monitoragem, identificação e o acompanhamento de ligações de usuários específicos, interceptando determinadas ligações.

Outros meios para interceptação estão



disponíveis nos troncos e nas centrais telefônicas, permitindo agências de inteligência monitorar milhares de ligações e interceptar a comunicação entre suspeitos baseados na assinatura da voz, ou na utilização de determinadas palavras, nomes, ou localidades. Atividades similares realizadas na Internet permitem a análise de correios virtuais por filtros ou pelo aumento do tráfego. A filtragem pode incluir palavras específicas como “bomba” ou “interferidores”. O controle do tráfego aborda a utilização de determinados padrões, comunicações entre IP suspeitos e localização da origem ou do destino da troca de mensagens.

Ativação de explosivos por controle remoto é uma outra atividade comum em guerrilhas urbanas. Telefones sem fio, equipamentos de

controle remoto, e controles remotos por infravermelho têm sido utilizado com frequência por elementos no leste da Europa nas últimas décadas. As Forças Armadas têm utilizado MPE com raios de alcance cada vez maiores, para se colocar à frente das ameaças. Conseqüentemente, assim como Operações de Informações de Guerra, na qual interferidores são utilizados somente por unidades especialistas em guerra eletrônica, elementos de combate urbano utilizam interferidores em quaisquer veículos de combate ou de patrulha. Essa função tem orientado o desenvolvimento de interferidores do tipo “ligue e esqueça”, que são capazes de combater sem atenuação do sistema de comunicações portátil ou veicular. Esse tipo de guerra eletrônica tem criado inúmeros desafios para a engenharia.

## Conclusão

Com a unipolaridade de forças no âmbito mundial, e a supremacia de tecnologia no emprego de armamento militar, cada vez mais se acentua a assimetria nos conflitos deste milênio. Para combater, do mesmo modo que para se utilizar de táticas desenvolvidas para esse tipo de guerra, deve ser avaliado o emprego da guerra eletrônica em outros tipos de ambientes. Para tal, deve ser levado também em consideração as medidas de proteção – MPE e de ataque eletrônico – MAE – doutrinárias.

O objetivo deste artigo não se resume em apresentar o desenvolvimento de uma tecnologia ou de apresentar novas tecnologias possíveis neste tipo de conflito, mas incentivar o desenvolvimento de novas táticas e de novos equipamentos para fazer frente às inovações e características inerentes a este tipo de confronto

## REFERÊNCIAS

- [1] Montgomery, C. Meigs, General (Res) do Exército dos EUA, “Idéias pouco ortodoxas sobre a Guerra assimétrica”, traduzido da revista “Parameters”, Maio 2006.
- [2] Brummel Vázquez Bermúdez, Capitão-de-Fragara da Marinha do Equador, A Guerra Assimétrica a Luz do Pensamento Clássico, Escola de Guerra Naval, 2004
- [3] Costa. Darc, Visualizações da Guerra Assimétrica, Escola Superior de Guerra, Dezembro 2001.
- [4] Electronic Warfare in Asymmetric Warfare, Defense Update - International Online Defense Magazine, Fevereiro 2006.