A GUERRA ELETRÔNICA NA ERA DA INFORMAÇÃO

Cap Alexandre Barboza ROCHA
Capitão de Artilharia da turma de 1995. Atualmente, desempenha a função de Instrutor de Guerra Eletrônica de Não-Comunicações na EsACosAAe

"Se conhecemos o inimigo e a nós mesmos, não precisamos temer o resultado de uma centena de combates"

Sun Tzu

RESUMO

Os conflitos mais recentes têm deixado clara a importância dos avanços científicos no campo militar. A interação da guerra eletrônica (GE) com o ambiente eletromagnético ocorre de três maneiras básicas: a primeira delas é levantando informações acerca dos equipamentos e sistemas de interesse e suas características; a segunda é impedindo que o inimigo utilize o espectro eletromagnético com sucesso; a última é evitando que o oponente tanto leve dados dos nossos equipamentos e sistemas quanto nos impeça de utilizar plenamente o espectro eletromagnético. Sendo a GE um dos pilares da guerra da informação, a utilização de equipamentos voltados para este fim constitui-se em importante ferramenta para obtenção de dados sobre o inimigo. Dessa forma, o uso correto da GE está intimamente relacionado à capacitação dos recursos humanos e a uma maior interoperapilidade entre as três Forças do Ministério da Defesa.

Palavras-chaves: Guerra Eletrônica (GE), Guerra da Informação, interoperabilidade.

1. INTRODUÇÃO

Historicamente, buscar informações sobre o inimigo para levar vantagem tática e estratégica no campo de batalha tem sido um objetivo constante. A guerra moderna tem como características o largo emprego da tecnologia, a assimetria e a velocidade das ações, tornando cada vez mais disseminado o uso de sistemas eletrônicos para comunicações e sensoriamento, muitos deles baseados na radiação de energia eletromagnética.

A atual era da informação produziu uma explosão na quantidade de dados que está (ou estará) disponível para o comandante em diferentes níveis. Desta forma, a proteção dos nossos sistemas de comunicações e não-comunicações torna-se fundamental.

Uma das vertentes para obtenção de informações sobre sistemas e possibilidades do oponente, que será aqui abordada, refere-se a atividades de Guerra Eletrônica (GE) no campo das não-comunicações, ou seja, aquela que está relacionada ao emprego de equipamentos destinados a produzir informações, como radares, sensores infravermelhos e LASER.

2. DESENVOLVIMENTO

Segundo Nunes (1999) o conceito de guerra da informação pode ser descrito pela *utilização da informação e do equipamento que a manipula como ferramentas (ar-*

mas) contra adversários. Neste contexto, ela está diretamente ligada ao combate dos sistemas de comando e controle (C2), segurança operacional, ciberguerra, guerra eletrônica, bloqueio de informação, guerra baseada na informação ou mesmo guerra psicológica.

A Portaria Normativa Nr 333/MD, de 24 de março de 2004 define a Política de Guerra Eletrônica e orienta as atividades de GE no âmbito das Forças Armadas, nos níveis estratégico, operacional e tático, determinando e atribuindo responsabilidades a diferentes segmentos da Estrutura Nacional de Defesa.

Desta forma, podemos definir Guerra Eletrônica como o conjunto de ações que:

a) utilizam a energia eletromagnética para destruir, neutralizar ou reduzir a capacidade de combate do oponente;
b) buscam tirar proveito do uso do espectro eletromagnético pelo oponente, e
c) visam a assegurar o emprego eficiente das emissões eletromagnéticas próprias.

A GE pode ser dividida em três grandes ramos: Medidas de Apoio de Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE) e Medidas de Proteção Eletrônica (MPE).

As Medidas de Apoio de Guerra Eletrônica objetivam a obtenção de dados e informações a partir das emissões eletromagnéticas utilizadas pelo oponente.

As Medidas de Ataque Eletrônico envolvem as ações para impedir ou reduzir o uso efetivo do espectro eletromagnético pelo oponente, bem como destruir, neutralizar ou degradar sua capacidade de combate, usando energia eletromagnética ou armamento que empregue a emissão intencional do alvo para seu guiamento.

As Medidas de Proteção Eletrônica buscam assegurar o uso efetivo (ativo e passivo) do espectro eletromagnético pelas forças amigas, a despeito de formas de interferências não intencionais e das ações de GE empreendidas pelo oponente.

A era da informação está transformando a guerra clássica centrada em plataformas para a Guerra Centrada em Rede (NCW), que pode ser definida com um conceito de operações com predomínio na informação, que gera crescente poder de combate por meio de uma rede de sensores, tomadores de decisão e operadores de sistemas de armas.

Segundo o Plano de Modernização e Integração do Sistema de Comando e Controle da Força Terrestre (2003/2005), busca-se a inserção do Exército Brasileiro na nova era do campo digital, em especial quanto à interoperabilidade dos vários meios de telemática .

Nesse contexto, defini-se o Sistema de Comando e Controle do Exército como sendo *um conjunto de recursos humanos , instalações, normas e processos que possibilitam ao Comandante planejar, dirigir e controlar, por intermédio de uma estrutura de telemática e de um fluxo de informações, forças e operações (organizações e atividades), na paz e na guerra, no preparo ou emprego da Força Terrestre.*

O acesso às nossas informações, facilitado com o advento da *internet*, torna imperativo o desenvolvimento de sistemas de proteção e autenticação das nossas emissões. O Projeto C2 em Combate da FTer (Exército Brasileiro), que tem como gerente executivo o Cmt do CIGE, está centrado na transmissão de dados entre os comandos visando aumentar as possibilidades de sucesso no campo de batalha, auxiliar no processo de tomada de decisão bem como o controle da execução das decisões tomadas.

Criptografia de sinais, adoção de pro-

tocolos e *links* seguros, recursos técnicos dos equipamentos, criação de uma mentalidade quanto a segurança além do gerenciamento das informações são algumas das medidas adotadas, visando a negar nossos dados para o oponente.

O conceito de ciberguerra, ainda que por vezes seja referido de uma forma diferenciada, em relação ao conceito de guerra eletrônica, pode ser considerado como parte integrante do mesmo. A ciberguerra envolve, assim, a utilização de todas as "ferramentas" disponíveis ao nível da eletrônica e da informática para derrubar sistemas eletrônicos e de comunicações inimigos e manter os nossos próprios sistemas operacionais.

Muitas das ações a serem desenvolvidas nesta área encontram-se ainda pouco definidas, devido, fundamentalmente, ao aparecimento contínuo de novos equipamentos e ser recente a descoberta pelos militares dessa área tecnológica, como uma nova forma de guerra.

Verificamos na figura a seguir uma visão da Guerra de Informação Estratégica, que por intermédio de uma ampla organização, produz conhecimentos técnicos e operacionais a partir dos sinais interceptados (Inteligência do Sinal – SIGINT). No nível estratégico de comando a Inteligência do Sinal atua, normalmente, sem a pressão do tempo, o que possibilita uma análise profunda sobre os dados coletados. Em função de sua natureza, o trabalho e os produtos por ela desenvolvidos requerem um elevado nível de segurança.

O fundamental a ser compreendido por todos os usuários do sistema de transmissão de dados é que sempre haverá um operador e equipamento de MAGE tentado estabelecer nossa Ordem de Batalha Eletrônica (OBE), ou seja, todos os nossos equipamentos eletrônicos presentes em uma operação. Por meio dos parâmetros que são coletados pode-se determinar o tipo, a função e o emprego dos equipamentos. A tabela abaixo mostra um exemplo recente de levantamento de informações dos meios empregados pelo Iraque na Guerra do Golfo em 1991.

Radar	Tipo	Banda	PRF [pps]	Pot Pico	Alcance [nm]	Plataforma
Alerta Antecipado-Estratégico/Defesa Aérea						
P-35M/37 Bar Lock	GCI/EW	E-F	375	650/beam	125	trailer
PRV-11 Side Net	HtF	E	-	-	95	trailer
Aquisição de alvos						
P-12 Spoon Rest B	EW/Acq	A (VHF)	310-400	180-350	100-150	Zil-157
P-12M Spoon Rest C	EW/Acq	A (VHF)	310-400	180-350	100-150	Ural-375

Ordem de Batalha Eletrônica do Iraque – 1ª Guerra do Golfo (Extrato)

3. CONCLUSÃO

A Guerra Eletrônica faz uso de grande parte ou de quase a totalidade do espectro eletromagnético(EEM). Diariamente, fazemos uso do EEM para produção ou trânsito de informações.

O advento de novas tecnologias e o uso mais constante das mesmas cresce numa velocidade assustadora. Os usuários dos diversos sistemas, militares ou não, devem estar preparados para fazerem uso dessas ferramentas de forma racional e segura.

Assim, mais importante do que a adoção de medidas de proteção dos nossos sistemas e equipamentos, faz-se necessária a implementação de uma mentalidade de Guerra Eletrônica desde o início da formação militar, o que será conseguido através da capacitação de recursos humanos altamente especializados, padronização de procedimentos, contínuo aperfeiçoamento, redução da dependência externa, além de estimular o desenvolvimento de tecnologia, materiais e equipamentos que reduzam as emissões e assinaturas eletromagnéticas das diversas plataformas.

REFERÊNCIAS

[1] Nunes, Paulo Fernando Viegas. Impacto das Novas Tecnologias no Meio Militar, artigo da Aerospace Journal, 1999.

[2] Brasil,. Ministério da Defesa. Secretaria de Tecnologia da Informação. Plano de Modernização e Integração do Sistema de Comando e Controle da Força Terrestre. 2003/2005

[3] _____,. Ministério da Defesa. MD32-P-01.Política de Guerra Eletrônica de Defesa, 1. ed., DF, 2004

[4] Phister Jr, Paul W. e Plonisch, Igor G. Aplicações militares das tecnologias da informação, artigo da Aerospace Journal, 4 trim, 2004.