MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
GUERRA ELETRÔNICA

TRABALHO DE CONCLUSÃO DE CURSO

GUERRA ELETRÔNICA NAS COMUNICAÇÕES SATELITAIS: Conceitos e Vulnerabilidades

1º Ten MATHEUS CORDEIRO WILHELM DA COSTA

Rio de Janeiro
2021

1º Ten MATHEUS CORDEIRO WILHELM DA COSTA

GUERRA ELETRÔNICA NAS COMUNICAÇÕES SATELITAIS: Conceitos e Vulnerabilidades

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica.

Orientador:
CT Renato da Silva Martins

CIAW
Rio de Janeiro
2021

FOLHA DE APROVAÇÃO

1º Ten MATHEUS CORDEIRO WILHELM DA COSTA

GUERRA ELETRÔNICA NAS COMUNICAÇÕES SATELITAIS: Conceitos e Vulnerabilidades

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica.

Aprovada em _____

Banca Examinadora:

CT Renato da Silva Martins – CIAW _____

CT Daniel Gama de Souza – CIAW _____

Marco Antônio Grivet Mattoso Maia, PhD – PUC Rio _____

CIAW
Rio de Janeiro
2021

Dedico este trabalho, em especial, a todos as pessoas envolvidas direta ou indiretamente com o Curso de Aperfeiçoamento em Guerra Eletrônica do Centro de Instrução Almirante Wandenkolk e a todos os profissionais do mar, que labutam os conveses da nossa Marinha.

AGRADECIMENTOS

À Deus, em primeiro lugar, por estar junto comigo em todos os momentos, dos mais fáceis e prazerosos aos mais árduos e difíceis.

A minha esposa, por ser a minha maior companheira e ter se transformado na pessoa mais importante da minha vida.

Aos meus pais, por terem me dado a parcela mais importante da educação que tenho, aquela que vem de casa, e terem sido fundamentais para eu entrar, me manter na Marinha e poder, assim, estar realizando este trabalho de conclusão de curso.

Aos meus avós e minha irmã, por sempre me prestarem todo o apoio de que necessitei.

E aos meus amigos, que sempre me acompanharam, principalmente nos momentos mais difíceis, e me deram valorosos conselhos ao longo da jornada trilhada até o dia de hoje.

“Não é preciso ter olhos abertos para ver o sol, nem é preciso ter ouvidos afiados para ouvir o trovão. Para ser vitorioso você precisa ver o que não está visível.”

Sun Tzu

GUERRA ELETRÔNICA NAS COMUNICAÇÕES SATELITAIS: Conceitos e Vulnerabilidades

Resumo

As comunicações por satélite contribuem positivamente para diversas qualidades de um sistema de Comando e Controle (C^2) no âmbito de uma operação naval, tais como flexibilidade, amplitude, confiabilidade, rapidez e continuidade. Sendo assim, nos dias de hoje, representam um grande avanço tecnológico na área das comunicações e são de grandiosa importância para o eficiente funcionamento do referido sistema, tendo em vista as suas principais características e as consequentes possibilidades que podem ser proporcionadas. No entanto, por conta de fazerem uso da propagação eletromagnética, a qual ocorre num meio altamente compartilhado, como é o caso do ar, as comunicações por satélite são suscetíveis de serem atingidas com ações atinentes ao campo da Guerra Eletrônica (GE), que acarretam em certas vulnerabilidades, que, por sua vez, podem comprometer alguns dos princípios do C^2. Dessa forma, é fundamental que sejam executadas medidas de proteção, pautadas em procedimentos e tecnologias para que um sistema de comunicações por satélites se contraponha a essas ameaças.

Palavras- chave: Comando e Controle, Guerra Eletrônica, Vulnerabilidades.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTAS DE SIGLAS E ABREVIATURAS

AGE	Atividades de Guerra Eletrônica
APEL	Aprestamento Eletrônico
CGE	Capacidade de Guerra Eletrônica
C^2	Comando e Controle
CT&I	Ciência, Tecnologia e Inovação
DBM	Doutrina Básica da Marinha
EHF	*Extra High Frequency*
FFAA	Forças Armadas
GE	Guerra Eletrônica
GMDSS	*Global Maritime Distress and Safety System*
GPS	*Global Positioning System*
INMARSAT	*International Maritime Satellite Organization*
HF	*High Frequency*
MAE	Medidas de Ataque Eletrônico
MAGE	Medidas de Apoio à Guerra Eletrônica
MB	Marinha do Brasil
MGE	Medidas de Guerra Eletrônica
MPE	Medidas de Proteção Eletrônica
RETRON	Reconhecimento Eletrônico
SGDC	Satélite Geoestacionário de Defesa e Comunicações Estratégicas
SHF	*Super High Frequency*
SISCOM	Sistema de Comunicações da Marinha
SISCOMIS	Sistema de Comunicações Militares por Satélite
$SISMC^2$	Sistema Militar de Comando e Controle

TI	Tecnologia da Informação
UHF	*Ultra High Frequency*

SUMÁRIO

1 INTRODUÇÃO

Ao se observar a missão da Marinha do Brasil (MB), observa-se como ponto de partida a preparação e o emprego do Poder Naval[1] a fim de que sejam cumpridas as suas atribuições. Inevitavelmente, o sucesso dessa missão está ligado à capacidade de realizar operações navais de forma eficiente.

Diversos fatores contribuem para esse sucesso, mas, sem dúvidas, eficientes comunicações são um dos mais importantes dentro desse conjunto, já que possibilitam a troca de informações de cunho tático, estratégico ou até mesmo logístico tanto entre navios, situados próximos ou afastados uns dos outros, quanto entre navios e estações em terra, muitas vezes afastadas por centenas de milhas náuticas ou até uma distância maior.

A comunicação é fundamental por ser um importante componente da parte física de uma estrutura de Comando e Controle (C^2). Como uma autoridade pode tomar uma decisão se não recebe informações para lhe subsidiar? O que pode acontecer se as recebe e elas estão alteradas pelo inimigo. Ou ainda, como um Comandante vai transmitir as ordens aos seus subordinados se a estrutura de C^2 não lhe garante a sua transmissão de forma segura e confiável?

No caso da comunicação entre estações bastante afastadas umas das outras, a dificuldade para estabelecer o enlace entre a transmissora e a receptora é maior, por diversos motivos, se comparado com estações próximas. Principalmente para melhorar não só esse como também outros aspectos, os sistemas de comunicação por satélite são importantíssimos e podem até ser imprescindíveis para o sucesso de uma operação naval.

1.1 Apresentação do Problema

Provavelmente por conta de as comunicações satelitais serem bastante eficientes, muitos usuários do Sistema de Comunicações da Marinha (SISCOM) as caracterizam como totalmente seguras e não enxergam certos riscos, o que não é a verdade. Pois, uma vez que é

[1] "Parte integrante do Poder Marítimo capacitada a atuar militarmente no mar, em águas interiores e em certas áreas terrestres limitadas de interesse para as operações navais" (BRASIL, 2007, p. 200). Ou seja, é a parcela armada do Poder Marítimo, que, por sua vez, é "resultante da integração dos recursos de que dispõe a Nação para a utilização do mar e das águas interiores" (BRASIL, 2007, p. 200).

empregado o espectro eletromagnético, de forma indissociável, certas vulnerabilidades provenientes de ações pertencentes ao campo da Guerra Eletrônica (GE) incidem sobre o sistema de comunicações utilizador.

1.2 Justificativa e Relevância

Os avanços tecnológicos estão possibilitando cada vez mais o emprego de satélites de telecomunicações. Nos dias de hoje, é difícil de encontrar um navio que não disponha de um terminal móvel naval pertencente a um sistema de comunicações satelitais. Por tal revolução tecnológica, também estão passando os meios da MB.

A enorme eficiência desses sistemas pode fazer com que muitos usuários do SISCOM possam não enxergar as "invisíveis" vulnerabilidades existentes. No entanto, deve-se estar consciente que ao passo que a tecnologia dos tempos de hoje possibilita o emprego cada vez maior desses sistemas, ela também é capaz de gerar ameaças aos mesmos.

1.3 Objetivos

O objetivo deste trabalho é incitar uma discussão sobre os conceitos, características e vulnerabilidades dos sistemas de comunicações satelitais dentro da MB e, com isso, obter um incremento da consciência situacional dos usuários do SISCOM.

1.3.1 Objetivo Geral

Conforme já dito, as comunicações por satélites, por fazerem uso do espectro eletromagnético, estão suscetíveis a ações pertencentes ao campo da GE. Sendo assim, o objetivo geral deste trabalho de conclusão de curso é mostrar como as comunicações por satélites podem ser ameaçadas por conta de determinadas ações de GE e, consequentemente, como o sistema de C^2 de uma operação pode ser influenciado, bem como o que pode ser feito para fazer frente a essas ameaças.

1.3.2 Objetivos Específicos

A fim de atingir ao objetivo geral deste trabalho de conclusão de curso, alguns objetivos específicos precisam ser alcançados, de forma que seja criado um encadeamento lógico e conceitual entre as suas seções.

Inicialmente, a intenção é formar um entendimento sobre a atividade de C², abordando seus principais conceitos e princípios.

Após, são apresentadas as principais características das comunicações satelitais, de modo que seja possível conhecer em que pontos elas se relacionam com a execução do C² e seus princípios.

Em seguida, o trabalho se volta para a GE propriamente dita, quando é conceituada e apresentada a estrutura da GE na MB, bem como é explicitado como um sistema de comunicações por satélites pode ser ameaçado por conta de Medidas de Apoio à Guerra Eletrônica (MAGE), atividades de Reconhecimento Eletrônico (RETRON) e de Medidas de Ataque Eletrônico (MAE). Em sequência, é explicitado como é possível se contrapor a essas ameaças por meio de Medidas de Proteção Eletrônica (MPE), durante a realização da operação.

E, por fim, é apresentado o avanço operacional advindo da ativação do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), lançado em 2017, de forma a exemplificar uma importante atividade de Aprestamento Eletrônico (APEL) desempenhada pelo Brasil recentemente.

1.4 Etapas do Trabalho

Este trabalho está dividido de forma a atender aos objetivos citados na seção anterior. Sendo assim, além das seções INTRODUÇÃO, METODOLOGIA, REFERENCIAL TEÓRICO E CONCLUSÃO, constam desta monografia as seguintes:

- O COMANDO E CONTROLE (C²);
- O SISTEMA DE COMUNICAÇÕES POR SATÉLITES, subdividido nas seguintes subseções: Características e Relações com os princípios de C²;
- A GUERRA ELETRÔNICA E SUAS IMPLICAÇÕES EM UM SISTEMA DE COMUNICAÇÕES POR SATÉLITES, subdividido nas seguintes subseções:

Estrutura da Guerra Eletrônica na MB, Medidas de Apoio à Guerra Eletrônica (MAGE) e Reconhecimento Eletrônico (RETRON), Medidas de Ataque Eletrônico (MAE), Tabela Resumitiva e Medidas de Proteção Eletrônica (MPE); e

- O SATÉLITE GEOESTACIONÁRIO DE DEFESA E COMUNICAÇÕES ESTRATÉGICAS (SGDC).

2 REFERENCIAL TEÓRICO

Houve a necessidade neste trabalho de conclusão de curso de, inicialmente, criar um embasamento teórico a respeito dos principais conceitos do C² e da GE, além das principais características das comunicações satelitais. A partir disso, puderam ser entendidas como e quais ações de GE podem trazer ameaças ou proteções para sistemas de C² que fazem uso desse tipo de comunicação.

No sentido de compreender os principais conceitos do C² e da GE, foram utilizadas, principalmente, definições e outras informações constantes de artigos e normas oficias das FFAA, onde destacam-se a Doutrina Básica da Marinha, o Glossário das Forças Armadas e a Doutrina para o Sistema Militar de Comando e Controle. Nesse contexto, figuram nesse conjunto de conhecimentos o funcionamento de um sistema de C² e quais são seus princípios mais importantes, além de algumas definições e da estrutura da GE no âmbito da MB.

As principais características das comunicações satelitais puderam ser compreendidas a partir de pesquisas a artigos com notável credibilidade, onde destaca-se o artigo “As vulnerabilidades das redes de Comando e Controle baseadas em comunicações por satélites”.

3 METODOLOGIA

O método empregado neste trabalho de conclusão de curso foi o dedutivo, pois partiu-se do conhecimento de que as comunicações satelitais fazem uso do espectro eletromagnético para se depreender que os sistemas que as empregam estão suscetíveis a sofrer certas ameaças atinentes ao campo da GE, bem como podem empregar a GE para fazer frente a essas ameaças.

3.1 Classificação da Pesquisa

3.1.1 Quanto aos fins

Visando analisar aspectos qualitativos do tema em questão, não é objetivo do presente trabalho levantar dados numéricos a respeito do problema abordado, nem a respeito das alternativas para superá-lo, mas sim descrevê-lo. Sendo assim, a pesquisa realizada no âmbito deste trabalho é classificada, quanto aos fins, como explicativa e descritiva.

3.1.2 Quanto aos meios

Os objetivos deste trabalho foram alcançados, principalmente, por meio de pesquisas a diversas normas pertencentes às Forças Armadas (FFAA), bem como a artigos com notável credibilidade. Esse conjunto de fontes de pesquisa, de caráter notadamente descritivo e normativo, fazem a pesquisa realizada no âmbito deste trabalho ser classificada, quanto aos meios, como bibliográfica.

3.2 Limitações do Método

O tema do trabalho, por ser bastante atual, possui uma vasta gama de informações a seu respeito e que aumenta a cada dia. A GE é, sem dúvida, uma das vertentes da guerra que mais cresce na atualidade, ao passo que o emprego de satélites para telecomunicações também vem sendo cada vez maior. No entanto, devido a questões temporais o trabalho não pode ser mais abrangente. Ainda assim, os pontos abordados foram suficientes para atingir os objetivos desejados.

3.3 Coleta e Tratamento de Dados

Para a elaboração deste trabalho, foi realizada uma extensa pesquisa bibliográfica concentrada em artigos, teses, dissertações e normas oficiais disponíveis em meio digital. Os dados obtidos foram empregados de modo a produzir as informações necessárias para que fossem alcançados os objetivos específicos, a partir dos quais buscou-se criar um encadeamento lógico e conceitual para que o objetivo principal fosse, então, atingido.

4 O COMANDO E CONTROLE (C²)

O C² constitui-se no exercício da autoridade e da direção que um Comandante tem sobre as forças sob o próprio comando, para o cumprimento da missão designada. Viabiliza a coordenação entre a emissão de ordens e diretrizes e a obtenção de informações sobre a evolução da situação e das ações desencadeadas. É entendido no Brasil como a ciência e a arte que trata do funcionamento de uma cadeia de comando.

Nesta concepção, envolve, basicamente, três componentes: a autoridade legitimamente investida, apoiada por uma organização, da qual emanam as decisões que materializam o exercício do comando e para onde fluem as informações necessárias ao exercício do controle; a sistemática de um processo decisório que permite a formulação de ordens, estabelece o fluxo de informações e assegura mecanismos destinados à garantia do cumprimento pleno das ordens; e a estrutura, incluindo pessoal, equipamento, doutrina e tecnologia necessários para a autoridade acompanhar o desenvolvimento das operações (BRASIL, 2007, p.65).

O processo de tomada de decisão envolve a obtenção de dados, a conjugação de fatores intervenientes, a obtenção e a manutenção da consciência situacional, até a decisão propriamente dita (BRASIL, 2015, p.15).

Figura 1 – Ciclo OODA ou Ciclo de Boyd

Fonte: CARDOSO (2015)

O ciclo de C², também conhecido como ciclo OODA ou ciclo de *Boyd*, é composto pela seguinte sequência de ações em combate, desenvolvidas de forma cíclica: observação, orientação, decisão e ação, conforme mostrado na figura 1. Na primeira etapa, é percebida uma mudança no curso dos acontecimentos; na segunda, é produzida uma imagem mental da nova situação; na terceira etapa, chega-se à decisão da conduta a ser desenvolvida; e na última, são executadas as ações decorrentes da decisão tomada, voltando-se à etapa da observação para um novo ciclo. Deve-se buscar realizá-lo por completo de forma mais rápida que o oponente (BRASIL, 2014a, p. A-5).

Portanto, fica evidenciada a importância de um adequado sistema de comunicações, de modo a garantir um rápido, seguro e confiável, ou seja, um eficiente fluxo de informações entre cada uma dessas fases e os componentes da estrutura.

Um sistema de comunicações por satélites, ao ser parte componente de um sistema de comunicações, pode contribuir para que isso seja alcançado, uma vez que traz consigo uma série de vantagens e contribui para que se atinjam os objetivos apontados por vários dentre os princípios de C², os quais "são os pressupostos básicos que devem ser observados no planejamento e na execução de atividades de C²" (BRASIL, 2015, p.17).

Todavia, uma vez que utiliza radiofrequência em suas transmissões, esse sistema faz uso do espectro eletromagnético e, consequentemente, alguns dos referidos princípios podem ficar vulneráveis a certas ameaças se não forem executadas as MPE adequadas. Dessa forma, torna-se interessante conhecer as principais características de funcionamento do sistema, de modo que se entendam quais são suas vulnerabilidades, as quais se dividem, principalmente entre monitoramento, interrupção do serviço e simulação de comunicações falsas. Sendo assim, para que se compreenda como essas ameaças podem se concretizar em problemas para o sistema de C², ganha relevância, sem dúvidas, o entendimento dos principais aspectos da GE.

5 O SISTEMA DE COMUNIÇÕES POR SATÉLITES

5.1 Características

Os satélites, sem dúvida, são uma das invenções mais engenhosas realizadas pela humanidade. O início de sua concepção se deu a partir de meados do século XX. Mais precisamente, pode-se dizer que o marco do nascimento da ideia de colocar um satélite em órbita, a fim de prover telecomunicações, foi a publicação de um artigo científico chamado "*Can Rocket Stations Give Worldwide Radio Coverage?*" pelo inglês Arthur Charles Clarke, em 1945, na revista *Wireless World*, quando foi proposto o conceito de satélite de órbita geoestacionária[2].

Em comparação com sistemas terrestres, os satélites possuem a vantagem de serem capazes de prover rapidamente imensas áreas de cobertura, o que é particularmente interessante quando o acesso a zonas do globo com baixas densidades populacionais ou baixos níveis de desenvolvimento não justifica os sistemas terrestres e quando é necessária a difusão de um elevado número de informações para um universo alargado de utilizadores individuais. O seu uso é ainda essencial em áreas devastadas por catástrofes ou conflitos que destruíram a estrutura de comunicações (GORDON; MORGAN, 1993, p.3-4, apud CARDOSO, 2015, f.20).

Além disso, prover cobertura a áreas marítimas é uma grande vantagem proporcionada pelos sistemas de comunicação por satélite, seja pelas aplicações comerciais, militares, dentre outras. Em qualquer uma dessas atividades, a segurança é um aspecto fundamental. E tal aspecto é bastante favorecido pelas comunicações por satélite, que são consideradas elementos importantes do GMDSS (do inglês, *Global Maritime Distress and Safety System*), que é um sistema empregado internacionalmente para navios conduzirem as comunicações essenciais para a sua própria segurança, bem como de navios próximos (BRASIL, 2011, p. 81).

Os satélites possuem uma grande importância para um sistema de comunicações do qual fazem parte, uma vez que possibilitam a comunicação de forma confiável entre

[2] Tipo de órbita na qual os satélites são posicionados a 35.786 Km de altitude em um plano próximo ao Equador. Sua velocidade de rotação é a mesma da Terra, o que os faz ficar parado em relação a um ponto da superfície do planeta. Em face de ser única, uma posição geoestacionária é muito disputada entre os países. Disponível em: https://pt.wikipedia.org/wiki/Órita_geoestacionária.

estações localizadas a longas distâncias entre si e permitem que sejam trafegados diversos tipos de informações, tais como voz, dados, imagem e vídeo, o que confere grande versatilidade a um sistema de C².

A versatilidade supracitada se deve, principalmente, às elevadas faixas de frequências utilizadas: UHF (do inglês, *Ultra High Frequency)*, SHF (do inglês, *Super High Frequency)* e EHF (do inglês, *Extra High Frequency)* (BRASIL, 2011, p. 18). Uma outra nomenclatura, um pouco confusa e herdada das divisões de banda dos sistemas radar e de televisão por satélite, diria que os satélites operam nas bandas L, S, C, X, Ku, K e Ka.

As divisões do espectro eletromagnético conforme as bandas de frequências supracitadas constam das tabelas 1 e 2, apresentadas logo a seguir.

Tabela 1 – Espectro de Radiofrequências

VLF (Very Low Frequency – Frequência Muito Baixa)
Esta faixa inclui todas as frequências rádios menores que 30 kHz, sendo usada em comunicações a média e longa distância e radiodifusão.
LF (Low Frequency – Frequência Baixa)
Esta faixa vai de 30 a 300 kHz, sendo usada em comunicações a média e longa distância, sendo também aplicada em radiofaróis (radiogoniometria) e radiodifusão.
MF (Medium Frequency – Frequência Média)
Faixa que vai de 300 kHz a 4 MHz, sendo usada em comunicações a média distância, por radiofaróis (radiogoniometria), radiodifusão, radiotelefonia e NAVTEX.
HF (High Frequency – Frequência Alta)
Faixa de 4 MHz a 30 MHz, sendo usada, principalmente, em comunicações a média e longa distância, radiotelefonia e radiotelex.
VHF (Very High Frequency – Frequência Muito Alta)
Faixa de 30 MHz a 300 MHz, sendo usada em comunicações a curta distância, televisão e AIS SART.
UHF (Ultra High Frequency – Frequência Ultra Alta)
Faixa de 300 MHz a 3.000 MHz, sendo usada em comunicações a curta distância, comunicações via satélite, televisão, EPIRB e radar.
SHF (Super High Frequency – Frequência Super Alta)
Faixa de 3000 MHz a 30.000 MHz, sendo usada em comunicações via satélite, radar e SART.
EHF (Extremely High Frequency – Frequência Extremamente Alta)
Faixa de 30.000 MHz a 300.000 MHz, sendo usada em comunicações via satélite e radar.

Fonte: BRASIL, 2012, p. 18.

Tabela 2 – Bandas de frequências empregadas nas comunicações por satélite

Banda de frequência	Faixa de frequência	Aplicações
L	1 GHz até 2 GHz	Serviço móvel por satélite (MSS)
S	2 GHz até 4 GHz	Usado pela NASA e para MSS
C	4 GHz até 8 GHz	Serviço fixo por satélite (FSS)
X	8 GHz até 12,5 GHz	Satélites meteorológicos e militares
Ku	12,5 GHz até 18 GHz	FSS e MSS
K	18 GHz até 26,5 GHz	FSS e MSS
Ka	26,5 GHz até 40 GHz	FSS

Fonte: STROSKI, 2018.

O uso dessas frequências bastante altas possibilita a transmissão de sinais com largura de banda, isto é, a parcela do espectro de frequências utilizada pelo sinal eletromagnético para transmitir a informação desejada, consideravelmente maior se comparada com sinais de frequências inferiores.

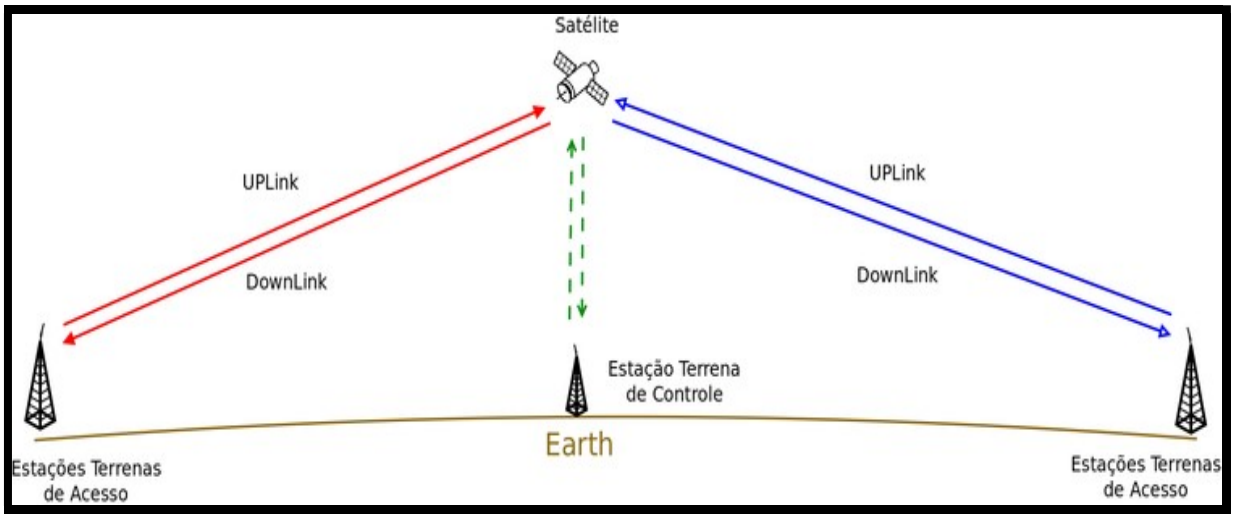
Dito isso, percebem-se, claramente, algumas das vantagens do emprego de satélites em telecomunicações ao serem comparados com os sistemas de rádio operados em HF (do inglês, *High Frequency)*, por exemplo, que, por sua vez, são uma comum alternativa para a comunicação entre estações localizadas em regiões muito afastadas umas das outras, quando não se dispõe de equipamentos satelitais ou se está fora da área de cobertura dos satélites.

Os transmissores que operam nessa faixa de frequências, muitas vezes, possuem potência necessária para que o sinal irradiado chegue até pontos situados em lugares muito distantes, no entanto de acordo com Domínguez, “a propagação em HF é altamente dependente de condições ionosféricas e de terreno, causando desvanecimentos, o que torna a torna pouco confiável” (1990, p. 137, apud CARDOSO, 2015, f.19). Além disso, tais sistemas até conseguem transmitir dados, mas com uma capacidade de transmissão muito baixa. Se os arquivos a serem transmitidos precisarem de muita banda de transmissão em um curto espaço de tempo, esse sistema torna-se ineficaz.

Segundo Gordon e Morgan (1993, p.3-4, apud CARDOSO, 2015, f.20), um sistema de comunicações por satélite funciona como um retransmissor. Uma estação que deseja se comunicar envia para o satélite a mensagem por meio de um enlace ascendente (*uplink*). Este a recebe, executa os processamentos necessários e realiza a retransmissão para outra estação, agora pelo enlace descendente (*downlink*), conforme mostrado na Figura 2.

Ainda nesse contexto, cabe ressaltar que essas frequências são distintas a fim de se evitar interferência entre os sinais ascendentes e descendentes.

Figura 2: Topologia básica do sistema de comunicações por satélite



Fonte: MONQUEIRO, 2010.

Para que o estabelecimento do enlace seja possível, o sinal propagado deve conseguir atravessar extensas regiões e camadas atmosféricas de diferentes características. A fim de chegar ao receptor de uma forma que possa ser inteligível, a transmissão deve ser realizada com altas potências e em elevadíssimas frequências, que por sua vez tornam o sinal seja bastante diretivo, portanto com alta capacidade de manter sua direção de propagação independente das condições ionosféricas que encontrar.

5.2 Relações com os Princípios de C²

As características apresentadas contribuem muito para a confiabilidade, que é a capacidade de um sistema de proporcionar credibilidade aos seus usuários. Um sistema confiável deve sobreviver e manter sua eficácia, mesmo quando exposto a eventos desestabilizadores, sobretudo provenientes do ambiente operacional, de danos internos ou de casos fortuitos (BRASIL, 2015, p. 19).

Um sistema de comunicação por satélite, sendo uma parcela de um sistema de C², contribui para uma maior rapidez, “pois uma vez colocado em órbita, possibilita a implementação de uma rede de comunicações em prazo reduzido” (SOUSA, p.38). “Os

enlaces devem ser estabelecidos por oportunidade, a fim de possibilitar o acesso imediato às informações de interesse" (BRASIL, 2015a, p. 19). Por ser mais uma possibilidade, ou seja uma redundância para se estabelecerem enlaces, contribui, também, para a continuidade, que é a sua capacidade de funcionar ininterruptamente (BRASIL, 2015, p. 19).

Ao incorporar produtos e conceitos derivados de inovações tecnológicas, sem dúvidas, um sistema de comunicações por satélite, confere, também, ao sistema de C^2 flexibilidade, que é definida como sua capacidade de modificar sua organização e suas funcionalidades, de modo a atender aos ditames impostos pela evolução da situação operacional (BRASIL, 2015, p. 18). Além disso, proporciona amplitude, também chamada de universalidade, por possuir uma cobertura bastante abrangente (SOUSA, p.38).

Ainda que existam todos esses pontos positivos, que acabaram de ser apresentados, os usuários de um sistema de comunicações por satélite não devem esquecer que é empregada para a transmissão de informações a propagação eletromagnética. O sinal utiliza o ar como meio de transmissão, um ambiente altamente compartilhado, e por isso está suscetível de ser interceptado e, consequentemente, monitorado. A partir daí, o inimigo pode obter informações altamente sensíveis, tais como os códigos e indicativos utilizados, além dos procedimentos operacionais adotados nas comunicações. Com isso, há a chance de que sejam simuladas pelo inimigo comunicações falsas.

Esses dois riscos ora apresentados comprometem o princípio da segurança, que "consiste em negar, dificultar ou identificar o acesso não autorizado às informações das forças amigas, restringindo a liberdade de ação do oponente para ataques aos pontos sensíveis do sistema de ao sistema de C^2" (BRASIL, 2015, p. 18).

Há, ainda, a ameaça de interrupção do funcionamento do sistema, por meio de bloqueio realizado pelo inimigo, que acaba impedindo ou dificultando a recepção do sinal em algum ponto do sistema. Neste caso, são comprometidos os princípios de confiabilidade, rapidez e continuidade.

6 A GUERRA ELETRÔNICA E SUAS IMPLICAÇÕES EM UM SISTEMA DE COMUNICAÇÕES POR SATÉLITES

Com base no que foi apresentado no tópico anterior deste trabalho, tornou-se possível conhecer as principais características de um sistema de comunicações por satélite e, consequentemente, entender como elas podem ser favoráveis ou desfavoráveis no que tange aos princípios de C^2. Dessa forma, é bem lógico compreender que a GE está indissociavelmente ligada a essas questões, ao passo que é a responsável não só por gerar as referidas vulnerabilidades, mas também por proporcionar formas de se contrapor.

6.1 Estrutura da Guerra Eletrônica na MB

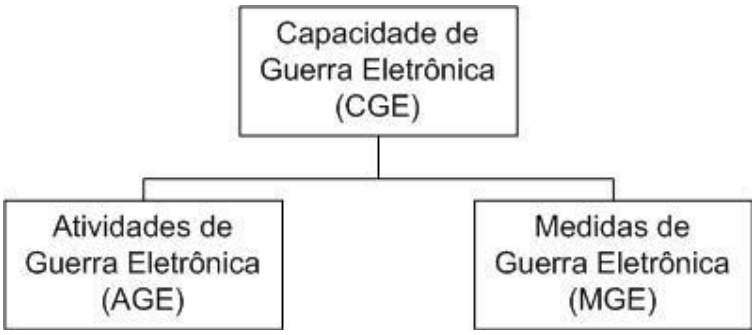
> O emprego militar da eletrônica diz respeito às ações que envolvem o uso de energia eletromagnética para determinar, explorar, impedir, reduzir ou prevenir o uso efetivo pelo inimigo do espectro eletromagnético e para assegurar o uso deste espectro pelas próprias forças.
> A guerra eletrônica (GE) engloba todo o espectro eletromagnético, cujo controle, ou seja, a capacidade de seu uso sem interferências inaceitáveis e a negação do seu uso ao adversário, contribui, sempre em escala crescente, para o resultado favorável das interações. Para ser capaz de conduzir as Ações de GE, o Poder Naval precisa desenvolver uma ampla capacidade de guerra eletrônica (CGE). A CGE é o somatório de meios e recursos de toda ordem que permite a uma Força empreender eficazmente Ações de GE em proveito de suas operações. Ela compreende o desenvolvimento de todo o processo de construção, de avaliação e de manutenção e engloba as atividades e as medidas de guerra eletrônica (BRASIL, 2014a, p. 3-23).

As Atividades de Guerra Eletrônica (AGE) são as de "caráter estratégico, tático e logístico ou de pesquisa que contribuem para o estabelecimento, para a exploração, para a reformulação ou verificação da capacidade de guerra eletrônica" (BRASIL, 2014b, p. 37) e são divididas em Reconhecimento Eletrônico (RETRON) e Aprestamento Eletrônico (APEL).

> As medidas de guerra eletrônica (MGE) abrangem as ações efetivamente realizadas no decorrer de uma operação naval. A sua natureza é fundamentalmente tática e seu emprego deve estar amparado por um planejamento e pela adequabilidade das táticas e equipamentos utilizados. As MGE são divididas em três ramos: Medidas de Apoio à Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE) e Medidas de Proteção Eletrônica (MPE) (BRASIL, 2014a, p. 3-23).

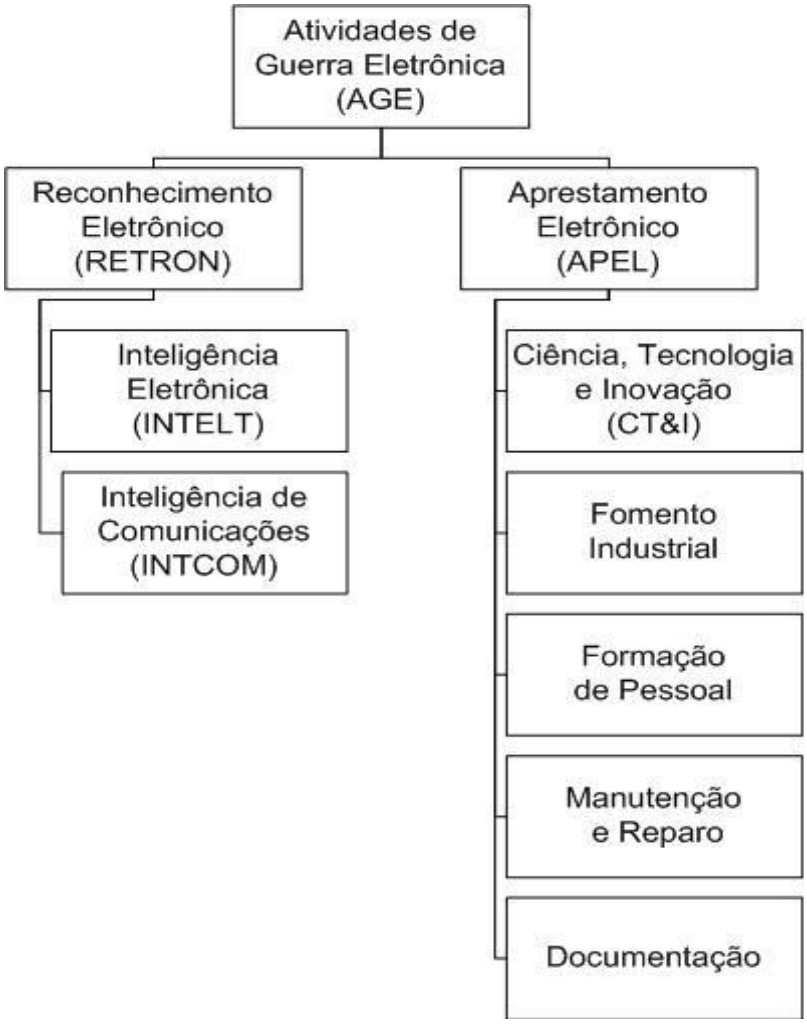
As formas como estão estruturadas a CGE, as AGE e as MGE estão ilustradas a seguir, nas figuras 3, 4 e 5.

Figura 3: Estrutura da Capacidade de Guerra Eletrônica



Fonte: o autor

Figura 4: Estrutura das Atividades de Guerra Eletrônica



Fonte: o autor

Figura 5: Estrutura das Medidas de Guerra Eletrônica

Fonte: o autor

Em se verificando as definições acima e uma vez que, como já foi dito neste trabalho, os sistemas por satélite fazem uso do espectro eletromagnético, torna-se evidente a importância do entendimento dos conceitos de GE para quem projeta ou opera os referidos sistemas.

6.2 Medidas de Apoio à Guerra Eletrônica (MAGE) e Reconhecimento Eletrônico (RETRON)

> As MAGE são um conjunto de ações visando à busca, interceptação, identificação e localização eletrônica das fontes de energia eletromagnética irradiadas no ambiente eletrônico, a fim de permitir a análise, o imediato reconhecimento de uma ameaça ou sua posterior exploração. (BRASIL, 2014b, p. 3-23)

Cabe, ainda, ressaltar que existem ações desempenhadas, dentro do conjunto das AGE, com um propósito muito semelhante ao das MAGE, mas que se diferenciam destas por não serem realizadas no decorrer de uma operação naval, mas sim num momento anterior, com o objetivo de obter conhecimentos estratégicos a fim de contribuir para o desenvolvimento cada vez maior da CGE ou para o planejamento de uma operação futura, como é o caso da atividade de RETRON (BRASIL, 2007, p.223).

Seja uma atividade de RETRON, executada antes da operação, seja uma das MAGE, executada durante a operação, o mais relevante nessa análise é que ações dessa natureza têm o objetivo de monitorar as comunicações do inimigo. Isto dá agilidade ao ciclo de C^2, uma vez que não é necessário o início da ação do oponente para se conhecer as suas intenções. “Permite, ainda, analisar e entender o processo cognitivo do oponente, possibilitando, em conjunto com as possibilidades do inimigo, que o comando esteja melhor preparado para antecipar as ações do adversário” (CARDOSO, 2015, f. 30).

Relembra-se que o enlace nas comunicações por satélite se dá por meio de *uplinks* e *downlinks*. Logo, para ocorrer o monitoramento, uma dessas transmissões deve ser interceptada. Nesse sentido, segundo Cardoso (2015, p.32), monitorar um *uplink* é uma atividade muito mais complexa, pois depende de aeronaves ou satélites, ao passo que no caso do *downlink*, a tarefa é menos complicada e precisa-se de uma estação de monitoragem na área de cobertura do sinal descendente.

> Uma vez que um sistema é capaz de interceptar uma comunicação do satélite, já é possível realizar a análise técnica. A partir dela, poderá ser identificada a modulação e a codificação. Nesse caso, será possível fazer a análise da mensagem, ou seja, do seu conteúdo e também a análise de tráfego. Mesmo que o conteúdo possa estar criptografado, muitas vezes o endereçamento é feito em claro para permitir o roteamento das mensagens e a análise de tráfego poderá ser feita independentemente da análise da mensagem. (CARDOSO, 2015, f. 33)

Por fim, para obter a localização da fonte emissora, podem ser empregados três métodos. Um se dá por meio da triangulação de transmissões ascendentes. Outro, por meio da medição das reflexões secundárias da transmissão em outros satélites geoestacionários, que usa uma lógica matemática parecida com a do GPS (do inglês, *Global Maritime System)*. O terceiro se aproveita dos dados de posição transmitidos por estações de usuários, conforme previsto pelo protocolo de funcionamento de diversos sistemas (CARDOSO, 2015, f. 34).

Em se analisando o que foi apresentado neste tópico e o que já foi comentado sobre a segurança de um sistema de C², fica claro que esse princípio pode ser comprometido se as comunicações estiverem sendo monitoradas por meio de interceptação de transmissões. Logo, é imprescindível que sejam executadas ações para se contrapor a esses riscos. “As medidas de segurança deverão ser continuamente revisadas, a fim de manter sua eficácia contra qualquer ameaça e de ações adversas aos sistemas de C² das forças amigas” (BRASIL, 2015, p. 18).

6.3 Medidas de Ataque Eletrônico (MAE)

“As MAE são um conjunto de ações tomadas para evitar ou reduzir o uso efetivo, por parte do inimigo, do espectro eletromagnético e, também, degradar, neutralizar ou destruir sua capacidade de combate por meio de equipamentos e armamentos que utilizem este espectro” (BRASIL, 2014b, p. 3-24).

Sendo assim, as comunicações por satélite, principalmente por conta de sua importância, podem ser alvos de ataques eletrônicos, sendo o bloqueio eletrônico e o despistamento os mais comumente empregados contra as comunicações por satélite.

O primeiro deles é baseado na irradiação, reirradiação ou reflexão deliberada de energia eletromagnética, impedindo ou, pelo menos, dificultando a recepção dos sinais, com a finalidade de reduzir ou anular o desempenho dos equipamentos do inimigo. (BRASIL, 2007, p.44).

Há o bloqueio de ponto, quando é utilizado um transmissor de faixa estreita de frequência "empregado individualmente sobre a largura de banda ocupada, no espectro, pelo receptor do oponente cuja eficiência depende diretamente da obtenção da frequência exata de operação" (BRASIL, 2007, p.44). Em contrapartida, existe o de barragem, que emprega uma transmissão em larga faixa ao ser comparada com a banda de recepção do oponente. Há, também, o bloqueio de varredura, que emprega um ruído de faixa estreita e variável no tempo, o qual possui a vantagem sobre o anterior de conseguir atingir uma larga faixa de frequências sem a necessidade de dividir a sua potência por toda essa faixa que se deseja atingir (BRASIL, 2007, p.44). A literatura, ainda, apresenta a possibilidade de realizar bloqueio com outros tipos de transmissões.

Portanto, várias são as formas que podem ser empregadas para tentar atrapalhar a recepção dos sinais em algum ponto do enlace, com a finalidade de, segundo Poesel, "interromper as comunicações em determinado momento o que poderá inviabilizar o uso daquele sistema, ou causar retardos sensíveis para que as comunicações aconteçam" (2004, p. 2, apud CARDOSO, 2005, p. 28), o que pode impactar diretamente sobre os princípios confiabilidade, rapidez e continuidade de um sistema de C^2.

Como já citado, além do bloqueio, faz parte desse conjunto o despistamento, que, por sua vez é caracterizado pela "deliberada irradiação, reirradiação, alteração, absorção ou reflexão de energia eletromagnética, com o propósito de induzir o inimigo a erro na interpretação ou no uso da informação recebida pelos seus sistemas eletrônicos" (BRASIL, 2007, p. 82).

Em muitas ocasiões, é realizado o despistamento imitativo, quando são enviadas mensagens falsas na rede como se fizessem parte do tráfego inimigo, causando, obviamente, prejudiciais consequências a quem as recebe, as interpreta e as considera para algum propósito (BRASIL, 2014b, p. 2-2). Para tal, é necessário "um grande conhecimento das comunicações do oponente, não só das suas características técnicas, mas também dos seus

procedimentos, a fim de que a comunicação simulada possa ser crível e atenda o seu efeito desejado" (CARDOSO, 2015, p. 28).

Claramente, o princípio da segurança fica comprometido, se o sistema de C² sofre a ação desse tipo de MAE.

> O despistamento imitativo causa confusão, prejudicando o aspecto cognitivo do processo de tomada de decisão nos diversos níveis de uma operação, prejudicando o princípio da segurança. [...] Tem o efeito secundário de, ao ser descoberto, afetar a credibilidade de todo o julgamento executado até aquele momento. Isso também retardará o Ciclo de C2 para que se possa reavaliar os fatos conhecidos (CARDOSO, 2015, p. 28).

Ao se estabelecer um paralelo entre o bloqueio eletrônico e o despistamento imitativo, percebem-se as semelhanças entre esses dois tipos de MAE, já que ambos possuem o objetivo de fazer com que, de alguma forma, sinais indesejáveis sejam captados pelo receptor do inimigo, seja por um satélite ou por uma estação terrena. Já as diferenças entre eles ficam por conta da forma e o consequente objetivo dos ataques. O primeiro emprega ruídos e visa a interrupção do funcionamento do sistema de comunicações do inimigo, ao passo que o segundo busca interferir no seu processo cognitivo, ao serem utilizadas comunicações falsas.

Por fim, um sistema de comunicações por satélite, que, como já foi dito, pode ter um papel fundamental na capacidade de C² de uma operação naval, pode, sem dúvidas, ser alvo de MAE.

6.4 Tabela Resumitiva

Os dois tópicos anteriores mostraram como determinadas ações desempenhadas no campo da GE podem acarretar em certas vulnerabilidades a um sistema de comunicações por satélite e, com isso, afetar alguns princípios de C². Então, com o objetivo de correlacionar, de uma forma resumida e de fácil visualização, algumas ações realizadas, pertencentes ao conjunto de MAGE, RETRON e MAE, com as ameaças geradas e com os princípios de C² afetados, é apresentada a tabela 3, logo a seguir.

Tabela 3: Correlação de ações realizadas com ameaças geradas e princípios de C² afetados

Ação realizada	Classificação da ação	Ameaça gerada	Princípios de C² afetados
Interceptação de mensagens	MAGE/RETRON	Monitoragem	Segurança
Bloqueio Eletrônico	MAE	Interrupção ou deterioração do funcionamento	Confiabilidade
			Continuidade
			Rapidez
Despistamento Imitativo	MAE	Simulação de Comunicações Falsas	Segurança

Fonte: o autor

6.5 Medidas de Proteção Eletrônica (MPE)

Inicialmente, ressalta-se a importância de um sistema de comunicações ter a capacidade de fazer frente às ameaças, tais quais as apresentadas nos tópicos anteriores. Portanto, é com essa finalidade que são adotadas as MPE, as quais são definidas como o "conjunto de ações tomadas para a proteção de meios, sistemas, equipamentos, pessoal e instalações, a fim de assegurar o uso efetivo do espectro eletromagnético, a despeito do emprego de MAE por forças amigas e inimigas" (BRASIL, 2014a, p. 3-24).

Apesar de essa ser a definição encontrada na Doutrina Básica da Marinha (DBM), norma oficial usada como referência na conceituação acima, as MPE englobam, também, ações para proteger os sistemas contra as MAGE inimigas. Sendo assim, existe dois tipos de MPE: anti-MAE e anti-MAGE. Contudo, essa subdivisão serve muito mais para fins didáticos do que práticos, uma vez que, geralmente, uma mesma medida pode alcançar as duas finalidades.

> Um exemplo é a utilização da tecnologia de salto de frequência que, quando utilizada na transmissão entre dois equipamentos-rádio, irá dificultar a interceptação e monitoração pelos sistemas MAGE. Contudo, essa tecnologia também impede ou diminui a eficiência de uma ação de bloqueio pelas MAE oponentes, sendo classificada, portanto, como Anti-MAGE e Anti-MAE (BRASIL, 2014b, p. 1-3).

No universo das MPE voltadas para as comunicações, há outra subdivisão: entre as voltadas a impedir a interceptação das transmissões, como é o caso do salto em frequência, da transmissão por salvas e do controle de potência, dentre outras; e aquelas com a finalidade de impedir o entendimento, a interpretação e o consequente uso das informações interceptadas

para produção de conhecimento, por parte do inimigo. Nesse segundo grupo, podem ser incluídas a criptografia e a esteganografia.

Bastante conhecida, a criptografia é “uma técnica de converter mensagens de sua forma original para outra ininteligível, de maneira que possa ser conhecida (decriptografada) apenas por seu destinatário” (BRASIL, 2014b, p. 2-8).

Já a esteganografia, da qual muito menos se ouve falar, se baseia em ocultar a existência de mensagem dentro de outra, de modo que a mensagem que se deseja transmitir, seja ela texto, imagem, áudio ou vídeo, é mesclada, *bit* a *bit*, em outro arquivo digital sem importância para a situação envolvida (BRASIL, 2014b, p. 2-9).

Evidentemente, essas duas tecnologias conferem ao sistema maior segurança, na medida em que ajudam na proteção contra as ameaças de monitoragem e simulação de comunicações falsas.

Outra medida que pode ser adotada é o emprego da técnica de transmissão por salvas, que é baseada na compressão da mensagem e no seu posterior armazenamento em pacotes, caso apenas um não seja suficiente, antes de transmiti-la, aumentando, assim, a dificuldade de interceptação por parte do inimigo (BRASIL, 2014b, p. 2-10).

O controle de potência é um procedimento que preconiza o uso da menor potência de transmissão necessária para o estabelecimento das comunicações. Porém, o aumento da potência de transmissão pode ser empregado para suplantar a ação de bloqueio. (BRASIL, 2014b, p. 2-5). As transmissões com potências mais baixas dificultam a interceptação e as consequentes possibilidades de monitoragem e simulação de comunicações falsas. Já as com potências mais altas dificultam a chance de haver uma interrupção do funcionamento do sistema de comunicações.

Sendo assim, ao lado da já citada e explicada técnica de salto em frequência e do uso de antenas direcionais, este por uma razão um tanto lógica, o controle de potência pode aumentar a imunidade do sistema tanto a interceptações, como a bloqueios.

Outros procedimentos, tais como a execução de manobras que posicionem os meios fora do alcance dos equipamentos do inimigo, a exploração correta dos recursos de comunicação e o uso de artifícios como mudanças de indicativos, mensagens preestabelecidas e códigos de nomes, podem ser MPE muito eficazes, seja contra MAE ou MAGE.

Cabe ressaltar, ainda, que as MPE só são usadas quando há necessidade de se contrapor a ameaças. Tais medidas só fazem sentido num ambiente em que as MAE ou MAGE estejam ocorrendo ou quando haja considerável probabilidade de ocorrência. Caso contrário, seriam impostas complicações desnecessárias aos procedimentos do sistema de

comunicações, prejudicando o princípio da simplicidade, segundo o qual “um sistema de C^2 deve ser o mais simples possível e atender aos requisitos para os quais foi concebido” (BRASIL, 2015, p. 18).

7 O SATÉLITE GEOESTACIONÁRIO DE DEFESA E COMUNICAÇÕES ESTRATÉGICAS (SGDC)

Como foi ilustrado na figura 4 deste trabalho, as AGE são divididas entre as atividades de RETRON e APEL, as quais possuem as suas respectivas subdivisões. A conceituação de RETRON já foi abordada, mas a de APEL e ainda não. Sendo assim, o APEL reúne o conjunto de atividades que visam a proporcionar todos e quaisquer recursos necessários ao estabelecimento, verificação, manutenção ou reformulação da CGE (BRASIL, 2007, p. 28). Subdivide-se: Ciência, Tecnologia e Inovação (CT&I); Fomento Industrial; Formação de Pessoal; Manutenção e Reparo; e Documentação.

Nesse sentido, uma importante atividade executada pelo Brasil recentemente, foi o lançamento e a posterior ativação do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), ilustrado na figura 6, apresentada a seguir.

Figura 6: O SGDC

Fonte: PADILHA, 2017.

O satélite foi lançado ao espaço em maio de 2017 e ficou pouco mais de dois anos inoperante por conta de um imbróglio judicial que travava a parceria entre as duas empresas responsáveis pela sua operação (OLIVEIRA, 2019).

As inovações trazidas pelo SGDC proporcionam um grande incremento na capacidade do Sistema de Comunicações Militares por Satélite (SISCOMIS), principal canal de comunicação de dados militares operacionais nas forças armadas brasileiras, e, consequentemente, na CGE.

O SISCOMIS compõe a estrutura do Sistema Militar de Comando e Controle (SISMC²) e possui uma infraestrutura de Tecnologia da Informação (TI) completa para enlaces digitais, por meio de satélites de comunicação geoestacionários, através da qual provê a conectividade segregada necessária para o estabelecimento de ligações de voz, dados e imagens que integrem e assegurem um fluxo de informações em tempo real entre os Centros de C², permitindo sua interligação para atendimento às necessidades das operações conjuntas e singulares de interesse do Ministério da Defesa (BRASIL, 2015, p. 32).

> Apesar das limitações existentes, o SISCOMIS tem atendido satisfatoriamente as necessidades de C² das Forças Armadas, entretanto, com a evolução tecnológica dos armamentos e das comunicações, a necessidade do compartilhamento da informação de forma rápida e oportuna tem tornado os sistemas de C² cada vez mais exigentes (LUIZ, 2017, f. 10).

Sendo assim, a ativação do SGDC foi uma forma de aumentar não só a capacidade do SISCOMIS, por conta do aumento da largura de banda e da potência utilizada, mas também a sua soberania, uma vez que o Ministério da Defesa é o responsável pela gerência da carga útil de banda X, faixa de frequências de uso exclusivo militar.

No entanto, o funcionamento desse satélite tem por objetivo, também, levar *internet* de banda larga a todo o território nacional, inclusive a pontos onde as redes de fibra óptica não alcançam, contribuindo para o desenvolvimento regional de áreas do território brasileiro e para a inclusão digital de sua população.

Cabe, ainda, ressaltar que durante o projeto, houve uma preocupação com transferência de tecnologia e capacitação profissional, acarretando em um significativo avanço da indústria espacial brasileira, o que proporcionou uma evolução em duas vertentes da atividade de APEL: Fomento Industrial e Formação de Pessoal.

8 CONCLUSÃO

Ao se entender o que é importante para que se disponha de um eficiente sistema de C² e conhecer as principais características de um sistema de comunicações por satélite, ficou evidenciada ao longo deste trabalho a fundamental importância de um sistema como este dentro de uma estrutura de C².

Foi possível não somente analisar e compreender como diversos requisitos e princípios da atividade de C² podem ser melhorados a partir do emprego de tecnologias de transmissão via satélite, como também verificar que tais tecnologias não são isentas de serem afetadas por Medidas de Ataque Eletrônico e Medidas de Apoio à Guerra Eletrônica.

Nos dias de hoje, em que inovações tecnológicas são cada vez mais desenvolvidas e os seus resultados são por vezes impensáveis, não há de se imaginar que no campo da Guerra Eletrônica isso não esteja ocorrendo. De fato, o que ocorre é exatamente o contrário e a GE, sem dúvidas, é uma das áreas da guerra que mais se desenvolve. Por conta disso, é de se esperar que as forças navais precisem operar, cada vez com maior frequência, em um ambiente eletromagnético hostil, onde o inimigo pode realizar diversas ações de GE, empregando os mais variados métodos para obter distintas vantagens táticas ou estratégicas.

8.1 Considerações Finais

Tão importante quanto empregar a tecnologia de comunicação por satélites é entender os riscos a que se está submetido num ambiente onde ocorre a propapação eletromagnética e, com isso, aplicar as medidas necessárias para mitigá-los. Portanto, indispensáveis são a boa capacitação dos equipamentos utilizados no que tange às MPE, seu uso racional de modo que sejam empregados no menor número possível, além do treinamento dos seus operadores, a fim de que possam explorar da maneira mais segura as suas capacidades.

8.2 Sugestões para Futuros Trabalhos

No momento atual, em que se verifica o enriquecimento cada vez maior das CGE dos países e, consequentemente, das ameaças a que um meio naval pode estar sujeito ao operar num ambiente eletromagnético cada vez mais hostil, está sendo desenvolvido o projeto das fragatas da classe Tamandaré, apontado como um marco da revolução tecnológica da Esquadra brasileira. Dessa forma, seria interessante um trabalho futuro abordar seu sistema de comunicações e sua CGE.

REFERÊNCIAS

ARTHUR C. Clarke. **Wikipedia**, 2020. Disponível em: https://pt.wikipedia.org/wiki/Arthur_C._Clarke. Acesso em: 12 mar. 2021.

BRASIL. Comando de Operações Terrestres. **EB70-CI-11.403 Caderno de instrução: Medidas de Proteção Eletrônica**. 1. ed. Brasília, DF, 2014b. 44 p. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/119/1/EB70-CI-11.403.pdf. Acesso em: 09 ago. 2020.

_____. Diretoria de Portos e Costas. **EROG Especial de Radioperador Geral**. 2. ed. Rio de Janeiro, RJ, 2011. 184 p. Disponível em: http://www.aquaseg.ufsc.br/files/2011/07/EROG_2011_socorro_salvamento.pdf. Acesso em: 09 abr. 2021.

_____. Estado-Maior da Armada. **EMA-305 Doutrina Básica da Marinha**. 2. Rev. Brasília, DF, 2014a. 102 p. Disponível em: http://www.consultaesic.cgu.gov.br/busca/dados/Lists/Pedido/Attachments/418525/RESPOSTA_PEDIDO_EMA-305_2014.pdf. Acesso em: 05 ago. 2020.

_____. Ministério da Defesa. **MD-35-G-01 Glossário das Forças Armadas**. Brasília, DF, 2007. 274 p. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em: 05 ago. 2020.

_____._____. **MD-31-M-03 Doutrina para o Sistema Militar de Comando e Controle**. Brasília, DF, 2015. 44 p. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/doutrina_militar/lista_de_publicacoes/md31a_ma_03a_douta_sismca_3a_eda_2015.pdf. Acesso em: 03 ago. 2020.

CARDOSO, Caio Germano. **As vulnerabilidades das redes de Comando e Controle baseadas em comunicações por satélite**. 2015. 51f. Monografia, ESCOLA DE GUERRA NAVAL, Rio de Janeiro, 2015. Disponível em: https://www.repositorio.mar.mil.br/bitstream/ripcmb/843297/1/00000bc2.pdf. Acesso em: 12 ago. 2020.

LUIZ, André Vinícius Pinho. **A evolução tecnológica e sua influência no Sistema Militar de Comando e Controle: impactos e consequências das novas tecnologias e do SGDC na capacidade do Sistema Militar de Comando e Controle**, 2017. 30f. Monografia, ESCOLA DE GUERRA NAVAL, Rio de Janeiro, 2017. Disponível em: http://www.redebim.dphdm.mar.mil.br/vinculos/00001b/00001b95.pdf. Acesso em: 22 jul. 2020.

MISSÃO e Visão de Futuro. **Marinha do Brasil**, 2016. Disponível em: https://www.marinha.mil.br/content/missao-e-visao-de-futuro-da-marinha#:~:text=%22Preparar%20e%20empregar%20o%20Poder,o%20apoio%20%C3%A0%20Pol%C3%ADtica%20Externa%E2%80%9D. Acesso em: 17 abr. 2021.

MONQUEIRO, Julio Cesar Bessa. Enlaces via satélite. **Hardware.com.br**, 2010. Disponível em: https://www.hardware.com.br/tutoriais/jubarte/pagina7.html. Acesso em: 11 abr. 2021.

OLIVEIRA, A. J. Satélite brasileiro leva banda larga a 1 milhão de alunos da rede pública. **Galileu**, 2019. Disponível em: https://revistagalileu.globo.com/Ciencia/noticia/2019/06/satelite-brasileiro-leva-banda-larga-1-milhao-de-alunos-da-rede-publica.html. Acesso em: 14 abr. 2021.

ÓRBITA geoestacionária. **Wikipedia**, 2020. Disponível em: https://pt.wikipedia.org/wiki/Órita_geoestacionária. Acesso em: 11 mar. 2021.

PADILHA, Luís. Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC) opera parcialmente. **Defesa Aérea & Naval**, 2017. Disponível em: https://www.defesaaereanaval.com.br/naval/satelite-geoestacionario-de-defesa-e-comunicacoes-estrategicas-sgdc-opera-parcialmente. Acesso em: 14 abr. 2021.

SOUSA, R. A. F.; SILVA, C. R. P. **Reflexões sobre o uso de satélites como infraestrutura complementar ao Programa Nacional de Banda Larga**. 9f. Disponível em: http://repositorio.ipea.gov.br/bitstream/11058/5418/1/Radar_n15_Reflex%C3%B5es.pdf. Acesso em 09 mar. 2021.

STROSKI, Pedro Ney. Introdução a satélites de comunicações. **ElectricalLibrary.com**, 2018. Disponível em: https://www.electricalelibrary.com/2018/02/16/introducao-satelites-de-comunicacoes/. Acesso em: 11 abr. 2021.