ESCOLA DE GUERRA NAVAL

CC CAIO GERMANO CARDOSO

AS VULNERABILIDADES DAS REDES DE COMANDO E CONTROLE BASEADAS EM COMUNICAÇÕES POR SATÉLITE

Rio de Janeiro

2015

CC CAIO GERMANO CARDOSO

AS VULNERABILIDADES DAS REDES DE COMANDO E CONTROLE BASEADAS EM COMUNICAÇÕES POR SATÉLITE

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CMG(RM-1) Luiz Carlos C. ROTH

Rio de Janeiro
Escola de Guerra Naval
2015

AGRADECIMENTOS

Agradeço a Deus pela força que me permite continuar lutando a despeito das dificuldades e por me dar a fé para saber esperar o Seu tempo e Sua vontade em transformar os sonhos em realidade.

À minha esposa Carla, agradeço a paciência e o apoio que me permitiram concluir esta e inúmeras outras demandas da carreira naval. Aos meus filhos, Gabriel e Leticia, por serem minha fonte de inspiração e por me fazerem querer ser uma pessoa melhor a cada dia.

Aos meus pais Artur e Neusa, por todas as lições de vida recebidas.

Ao meu orientador, CMG(RM-1) Roth, e ao meu orientador metodológico, CF(RM-1) Nagashima, agradeço os ensinamentos que aprimoraram e fizeram este trabalho uma realidade.

Aos meus amigos do Centro de Guerra Eletrônica da Marinha, em especial CC Paim, CC Alessandro Santos, CT(T) Eclenice e 1T(T) Caroline Branco, por todas as horas e lições compartilhadas e por dividirem o sonho de uma Marinha melhor.

RESUMO

O Comando e Controle (C2) é uma conjunção de ciência e arte, essencial ao sucesso de uma operação militar. Uma parcela do componente físico de seus sistemas são as comunicações, por satélite. Existe uma cultura disseminada entre um grande número de pessoas de que esse canal é completamente seguro. Para avaliar tal assertiva, foram apresentados, explicados e analisados alguns conceitos de C2 e de comunicações por satélite e identificadas as possíveis fragilidades desses sistemas. Algo análogo foi feito, ainda, com relação à Guerra Eletrônica (GE), suas componentes e capacidades. Foi, então, estabelecido o confronto entre as possíveis vulnerabilidades do C2 e a GE, empregando o método hipotético-dedutivo. A análise de documentação ostensiva comprovou a insegurança das comunicações por satélite à GE e a presença de artifícios para minimizar tal ameaça. Espera-se, com isso, que seja ampliada a consciência das vulnerabilidades das comunicações satélite e que elas possam ser consideradas no gerenciamento de risco operacional dos planejamentos militares, minimizando os riscos e aprimorando a probabilidade de sucesso da empreitada militar.

Palavras-Chave: Comando e Controle. Guerra Eletrônica. Comunicações por satélite. Gerenciamento do risco operacional. Planejamento militar.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ASAT -	Armamento Antissatélite
C2 -	Comando e Controle
EUA -	Estados Unidos da América
GE -	Guerra Eletrônica
GEO -	Órbita Geoestacionária
GPS -	Sistema de Posicionamento Global
INTCOM -	Inteligência de Comunicações
INTSAL -	Inteligência de Sinal
LEO -	Órbitas Baixas (*Low Earth Orbit*)
MAGE -	Medidas de Apoio à Guerra Eletrônica
MAGE-COM -	Medidas de Apoio à Guerra Eletrônica de Comunicações
MAE -	Medidas de Ataque Eletrônico
MB -	Marinha do Brasil
MPE -	Medidas de Proteção Eletrônica
NSA -	Agência de Segurança Nacional (*National Security Agency*)

SUMÁRIO

1 INTRODUÇÃO

É inegável a importância de um grande Comandante no sucesso de uma empreitada militar. A atuação desse líder nas ações de seus subordinados é realizada pelo que modernamente é chamado de Comando e Controle (C2). É indispensável que essa sistemática de C2 esteja adequada e permita que toda a estrutura hierárquica possa funcionar o mais harmonicamente possível, contribuindo com o cumprimento da missão.

O C2 possui vários componentes, dentre os quais encontra-se a estrutura de comunicações. Ela precisa atender a necessidades estratégicas/operacionais, táticas e logísticas, a curtas e longas distâncias. Para tal, empregam-se diversos sistemas, inclusive aqueles baseados em satélites.

Um dos principais requisitos das comunicações é a segurança. Existe uma cultura disseminada entre um grande número de pessoas de que as comunicações por satélite são completamente seguras. Esta pesquisa visa a responder a seguinte questão: será que as comunicações por satélite são completamente seguras como se imagina?

O propósito desta pesquisa é avaliar conceitualmente a segurança das comunicações por satélite. Para tal, objetiva-se descrever e explicar os conceitos básicos de C2, que incluem, entre outros tópicos, as comunicações por satélite, e de Guerra Eletrônica (GE) e da análise, comparação e contraste entre eles, com vistas a avaliar conceitualmente a segurança do referido canal de comunicações.

Para a condução desta pesquisa foi formulada a hipótese de que se as comunicações por satélite empregam o espectro eletromagnético, e este é vulnerável à GE, então as comunicações por satélite são vulneráveis. A negação dessa hipótese confirmaria o senso hoje vigente, porém a sua confirmação indicará que, pelo menos em alguns casos específicos, as comunicações por satélite também são vulneráveis. Essa comprovação é essencial, pois permite criar a mentalidade de que a vulnerabilidade desse canal de

comunicações deve ser sempre analisada dentro do Gerenciamento do Risco Operacional do C2 dos planejamentos militares. Acreditamos que, por isso, a pesquisa é relevante para a Marinha do Brasil (MB).

Outro ponto indispensável desta pesquisa é a ausência de sigilo. Ao decidir-se por delimitá-la às referências ostensivas é assegurado que o conhecimento possa ser disseminado sem as restrições dos documentos sigilosos.

Esta pesquisa é composta por seis seções. Esta introdução, a primeira delas, tem como propósito proporcionar uma visão geral do problema e da pesquisa.

A segunda seção apresentará a metodologia de estudo para responder à questão da pesquisa. Ela apresentará a linha de raciocínio que permitirá o atendimento do propósito estabelecido de avaliar conceitualmente a segurança das comunicações por satélite.

Na terceira seção será descrito, explicado e analisado um referencial teórico de C2 e de comunicações que permitam compreender as peculiaridades das comunicações por satélite.

Já a quarta seção, de maneira análoga, serão descritos, explicados e analisados os conceitos básicos da GE, que é a ameaça estudada na pesquisa.

Na quinta seção, as comunicações por satélite e a ameaça da GE serão analisadas, comparadas e contrastadas permitindo avaliar a hipótese formulada pelo estudo.

Por fim, a sexta seção concluirá este estudo indicando quais as implicações operacionais decorrentes da análise realizada, bem como quais pesquisas poderiam ser desenvolvidas para aprofundar algumas descobertas desta pesquisa.

Conforme mencionado anteriormente, a próxima seção apresentará a metodologia que orientará o estudo.

2 METODOLOGIA

O método empregado nesta análise é o hipotético-dedutivo. Ele prevê que a partir de conhecimentos e expectativas prévios seja identificado um problema. Para a solução deste problema é estabelecida uma nova teoria por meio de uma conjectura ou uma hipótese obtida por meio de dedução e passível de teste. Ela será então falseada, ou seja, haverá uma tentativa de refutá-la por meio da observação de fatos (POPPER, 1975, *apud* MARCONI; LAKATOS, 2010, p. 77-78).

No que tange a esta pesquisa, conforme já mencionado, as expectativas prévias existentes entre várias pessoas indicam que as comunicações por satélite são totalmente seguras. A questão formulada é: elas são tão seguras como se imagina?

O raciocínio dedutivo nos indica que as comunicações que empregam o espectro eletromagnético são vulneráveis à GE. Ora, as comunicações por satélite empregam o espectro eletromagnético; logo, elas estão vulneráveis às ações da GE. Essa é a hipótese elaborada na presente pesquisa. Para permitir a elaboração desse raciocínio, serão descritos, explicados e analisados os conceitos básicos de comando e controle, incluindo as redes de comunicações por satélite, e de GE nas duas seções seguintes.

A tentativa de falseamento dessa hipótese se dará posteriormente e em duas etapas. Na primeira, será realizada uma análise conceitual para confirmar se os pressupostos teóricos discutidos permanecem válidos no caso das comunicações por satélite. Em seguida, será empregado o método indutivo. A partir de casos observados na literatura ostensiva, poderá ser induzida a vulnerabilidade das comunicações por satélite. Ainda que seja uma indução incompleta[1] e mesmo que seja sabido que os pressupostos das capacitações tecnológicas dos potenciais oponentes não permanecem válidas para qualquer adversário,

[1] A indução incompleta ou científica é aquela que permite a partir de apenas alguns casos observados adequadamente afirmar ou negar para as demais ocorrências daquela categoria (MARCONI; LAKATOS, 2010, p. 71).

ainda assim o propósito desta pesquisa terá sido atendido.

Isso se deve pelo fato de que doutrinariamente, para o planejamento de operações militares, devem ser consideradas as possibilidades do inimigo (BRASIL, 2011, p. 28, 2006, p. 4-31). A compreensão clara da possibilidade do oponente dispor dessa capacidade já obrigará o planejador a considerar tal problema no seu gerenciamento do risco operacional (BRASIL, 2015, f. 7). Servirá, ainda, para a mitigação do risco e para a identificação da sua componente residual, ampliando a segurança das comunicações.

A seguir será apresentado o referencial teórico básico de C2 e das comunicações por satélite.

3 COMANDO E CONTROLE E COMUNICAÇÕES POR SATÉLITE

Conforme mencionado, serão descritos, explicados e analisados, a seguir, os conceitos básicos referentes ao C2. O C2 é um elemento essencial para a condução das operações militares.

Para abordar o assunto, serão discutidos alguns conceitos de C2. Posteriormente será apresentado e analisado o Ciclo de C2, que consolida a ideia de funcionamento do C2. A partir daí poderão ser discutidos os seus requisitos, chamados de Princípios de C2. Finalmente, poderá ser analisado o funcionamento das comunicações por satélite, seguido de uma série de conclusões parciais.

3.1 Conceitos de C2

As estruturas de comando são antigas e sua história se confunde com a das operações militares. O seu conceito é tão básico e disseminado que até mesmo a Bíblia o demonstra com clareza.

> Porque eu também tenho superiores, e tenho soldados sob meu comando. Quando digo a um 'vá!', ele vai. Quando digo a outro 'venha!', ele vem. E quando digo ao meu criado 'faça isso', ele o faz. (MATEUS 8,9)

O primeiro tratado de estratégia militar identificado (COUTAU-BÉGARIE, 2010, p. 124) é do século V a.C. e também já trata a questão. Nele, Sun Tzu[2] (2002, p. 17) dividiu o problema do comando em dois dos seus cinco fatores constantes: o Chefe; e o método e a disciplina.

Outros teóricos da guerra também o estudaram, como Clausewitz[3] (2007, p. 32-42, 45, 59). Ele ampliou os conceitos, tratando não apenas das características básicas inerentes ao comandante e suas forças, mas também da importância da informação por ele recebida. Foi

[2] General chinês e o primeiro estrategista conhecido, tendo vivido provavelmente no século V a.C. (COUTAU-BÉGARIE, 2010, p. 124).

[3] General e estrategista prussiano (1780-1831) considerado “o mais conhecido de todos os pensadores militares” (COUTAU-BÉGARIE, 2010, p. 167).

percebida a relevância da análise das informações que podem estar incompletas, eivadas de conhecimentos falsos ou equivocados, criando o conceito da névoa da guerra.

O problema também tem sido analisado por teóricos navais. Corbett[4] (1911, p. 2) amplia o conceito, indicando que não basta o líder decidir de maneira correta. É necessário também que seus subordinados compreendam claramente as decisões e sejam capazes de convertê-las em ação.

Conforme demonstrado, apesar de estas abordagens não serem novas, a preocupação a respeito do comando e do controle das forças tem crescido exponencialmente desde 1939 (CREVELD, 1985, p. 1-4). Tal fato tem se beneficiado e tem sido o impulsor de vários desenvolvimentos tecnológicos que resultaram na chamada Era do Conhecimento. Essa evolução tem influenciado diretamente o combate, ocasionando efeitos como o desvanecimento das frentes de combate, a ampliação dos fatores de destruição, a maior distribuição espacial dos meios e a aceleração do combate (TOFLER; TOFLER, 1995, p. 73-93).

Os Estados Unidos da América (EUA) são um dos países fortemente influenciados por essa nova era. Como resultado disso e dos grandes investimentos em Defesa e da capacitação tecnológica das Forças Armadas daquele país, é ideal verificar como é encarada a questão. No seu arcabouço doutrinário, o termo C2 se refere ao exercício da autoridade e direção de um comandante durante uma operação (EUA, 2010, p. 40).

Já no Brasil, além da definição acima são incorporados dois outros significados. O primeiro é o que se refere à ciência e à arte que regem o desempenho de uma estrutura de comando. O último é o de sistemas de comando e controle propriamente ditos (BRASIL, 2007, p. 58). Pode-se assim observar que a definição brasileira é mais abrangente, uma vez que incorpora toda uma questão conceitual, além da estrutura física representada pelos sistemas de C2.

---

[4] Um dos maiores estrategistas navais britânico (1854-1922) (COUTAU-BÉGARIE, 2010, p. 437).

Como se depreende da definição acima, o C2 envolve três componentes indissociáveis e que se inter-relacionam (BRASIL, 2014c, p. 15):

a) a autoridade – elemento do qual emanam as ordens e para o qual se destinam as informações para a execução do controle;

b) o processo decisório – apoiado na doutrina, norteia as decisões e estabelece os fluxos informacionais, permitindo a disseminação das ordens e o exercício do controle; e

c) estrutura – incorpora a estrutura física, incluindo instalações, equipamentos e suas tecnologias, bem como o pessoal para a consecução do C2.

Conforme visto nos conceitos apresentados, é importante considerar que o C2 é uma conjunção de ciência e arte. Ele não pode ser negligenciado, e por isso tem sido cientificamente estudado, seja por estrategistas ou por outras ciências sociais, seja por ciências exatas, como a engenharia. A arte é advinda das experiências pessoais, enquanto a ciência de um estudo criterioso, não devendo nenhum deles ser negligenciado.

Além disso, ao serem analisados os componentes de C2 podemos observar a figura do comandante e a estrutura hierárquica de seu comando, que, como já visto, foi prescrito por Sun Tzu. Encontramos o processo de gerenciamento da informação, com duas vertentes, uma cujo foco é a disponibilidade de conhecimentos (vertente informacional) e outro a compreensão daquilo que se observa (vertente cognitiva), que, conforme mencionado, foi previsto por Clausewitz e Corbett. E, finalmente, temos a estrutura (vertente física) que habilita que o comando seja executado empregando as suas vertentes informacional e cognitiva.

A seguir será apresentado o conceito de Ciclo de C2, que demonstrará como a doutrina militar brasileira e muitos teóricos consideram o desenvolvimento das vertentes informacional e cognitiva do processo decisório de C2. Depois serão apresentados quais

requisitos devem ser atendidos por todo esse processo, no que é doutrinariamente chamado de Princípios de C2. E finalmente será discutida a vertente física de interesse desta pesquisa, representada pelas comunicações por satélite.

3.2 Ciclo de C2

O Ciclo de C2 também pode ser chamado de Ciclo de Decisão, Ciclo OODA, ou Ciclo de Boyd[5]. Ele prevê que o processo decisório ocorre de forma cíclica seguindo a sequência Observação, Orientação, Decisão, Ação (completando o acrônimo OODA) (BRASIL, 2014b, p. A-5).

Durante a primeira etapa é Observada uma alteração na situação vigente (vertente informacional). A partir daí, durante a Orientação, a nova situação é compreendida por meio da elaboração de um modelo mental (vertente cognitiva). Já na terceira etapa é elaborado um plano de ação e a Decisão do comandante é disseminada (também vertente cognitiva). Finalmente, a Ação é implementada na última etapa, devendo os resultados serem observados, o que reinicia o ciclo (FIG. 1 - ANEXO A) (BRASIL, 2014b, p. A-5).

A ideia é que se realize o ciclo completo, mais rapidamente do que o oponente (BRASIL, 2014b, p. A-5). Dessa forma, o inimigo teria que se tornar reativo, garantindo a inciativa das ações às nossas forças. Apesar deste conceito estar previsto na doutrina de vários países, inclusive do Brasil, deve ser ressaltado que o ciclo originalmente imaginado por Boyd possui uma complexidade muito superior e permite uma análise mais refinada do problema (CORAM, 2002, p. 335-339).

Como pode ser visto na versão completa do Ciclo de C2 (FIG. 2 - ANEXO B), ele possui inúmeras setas que encerram em si múltiplos ciclos (CORAM, 2002, p. 335-339). No

[5] Coronel da Força Aérea estadunidense (1927-1997), piloto de caça e autor de diversas teorias como a de energia e movimento que tem orientado a construção de aeronaves de combate, além do Ciclo de C2 que leva seu nome e outros conceitos que redundaram no que é chamado a Guerra de Manobra (CORAM, 2002).

entanto, o importante é observar a relevância nesse novo diagrama que a etapa da orientação recebe. Um indício desse fato é que ela se conecta com maior número de elementos, o que indica a sua centralidade e consequentemente sua importância (OPSAHL *et al.*, 2010, p. 245).

Além disso, fica claro em todo o desenvolvimento conceitual das teorias de John Boyd a importância alocada para esse processo de compreensão da realidade (SPINNEY, 2014, p. 4-36). Apesar de não ser o foco desta pesquisa aprofundar os conhecimentos nessa área, é relevante apontar que também são originados nessa etapa instruções para os sensores realizarem a coleta e diretrizes implícitas que influirão diretamente na ação dos subordinados. Além disso, essa possibilidade de interferir nas percepções do inimigo serve de base para grande parte da teoria de Boyd (SPINNEY, 2014, p. 44-52).

Podemos analisar o que foi apresentado, observando que as setas propostas no Ciclo de C2 correspondem em grande parte a estruturas de comunicação que constituem o componente físico mencionado anteriormente, das quais uma parcela é composta por sistemas por satélite. Além disso, podemos correlacionar o componente informacional visto na subseção anterior com a coleta realizada durante a etapa da observação. Podemos, ainda, fazer a correspondência entre o componente cognitivo e a etapa da orientação.

A teoria completa de Boyd nos demonstra não só a importância da rápida execução do Ciclo de C2, mas também nos alerta sobre a relevância da cognição das informações disponíveis no processo de tomada de decisão. Esse poder também o torna uma grande vulnerabilidade. Uma vantagem decisiva pode ser obtida ao se intencionalmente ampliar a névoa da guerra, dificultando ou induzindo o processo decisório do oponente ao erro empregando estratagemas[6].

Tendo sido analisado o modelo conceitual de C2 na forma do Ciclo de Boyd, agora é possível identificar quais os requisitos para assegurar o bom funcionamento da

[6] Conjunção de medidas para o despistamento e para a obtenção da surpresa nos níveis estratégico e operacional de condução da guerra (WHALEY, 2007, p.1).

estrutura. A doutrina brasileira os chama de Princípios de C2 e eles serão apresentados a seguir.

3.3 Princípios de C2

Os princípios de C2 estão previstos na doutrina de defesa brasileira e são "pressupostos básicos que deverão ser observados no planejamento ou na execução das atividades de C2" (BRASIL, 2014c, p. 16). São eles: Unidade de Comando, Simplicidade, Segurança, Flexibilidade, Confiabilidade, Continuidade, Rapidez, Amplitude e Integração. Com base no Ciclo de C2, é possível identificar como sendo de interesse para esta pesquisa os princípios da Segurança, da Confiabilidade, da Continuidade e da Rapidez.

A Segurança consiste em dificultar ou negar o acesso não autorizado às informações das próprias forças, minimizando os riscos de ataques. Já a Confiabilidade está associada com a resiliência[7] de um sistema de C2. A Continuidade prevê que a estrutura de C2 possa ser operada ininterruptamente. E, finalmente, a Rapidez prevê que se deve proporcionar agilidade ao processo decisório (BRASIL, 2014c, p. 17-18).

Se analisarmos esses princípios poderemos tentar identificar as possíveis ameaças aos sistemas de C2. Inicialmente, pode ser identificada a ameaça de monitoramento das comunicações que impactaria diretamente com o princípio da segurança. Outra ameaça vislumbrada é a interrupção ao serviço que afetaria a agilidade do Ciclo de C2, prejudicando os princípios da confiabilidade, da continuidade e da rapidez. A terceira e última ameaça está relacionada com a possibilidade de que comunicações do sistema de C2 próprio sejam simuladas pelo oponente. Esta última ameaça também impactaria o princípio da segurança.

A lógica de ameaças apresentada fica bem clara quando comparada com os

---

[7] Característica de um sistema que é capaz de sobreviver e se recuperar de interrupções originadas por eventos ocorridos no ambiente operacional (PFLANZ; LEVIS, 2012, p. 141).

princípios da segurança da informação digital[8], gerando quase um mapeamento unívoco, excluindo a integridade e a legalidade. A primeira está relacionada com dados arquivados ou demanda a interrupção e substituição daqueles em trânsito, ato avaliado como não sendo exequível no espectro eletromagnético. Já a legalidade não faz sentido no contexto de comunicações militares de inimigos em conflito. A TAB. 1 sumariza essa correlação.

TABELA 1
Correlação entre ameaças, princípios de C2 e de segurança da informação digital

Ameaça	Princípios de C2	Princípios de Segurança da Informação Digital
Monitoragem	Segurança	Confidencialidade
Interrupção	Confiabilidade, continuidade e rapidez	Disponibilidade
Simulação de Comunicações Falsas	Segurança	Autenticidade

Já tendo sido possível identificar os princípios de C2 e mapear as possíveis ameaças que os sistemas de comunicação possam vir a sofrer, é possível descrever, na próxima subseção, como funciona a componente física da rede de comunicações por satélite.

3.4 Comunicações por Satélite

As comunicações por satélite têm grande utilidade para a transmissão de voz e dados a longas distâncias. A alternativa comum ao uso dos satélites para essa finalidade é o emprego de ondas rádio de alta frequência (HF) ou o emprego de cabos ou fibras óticas. A propagação em HF é altamente dependente de condições ionosféricas e de terreno, causando desvanecimentos, o que a torna pouco confiável (DOMÍNGUEZ, 1990, p.137). O custo de cabos e fibras aumenta à medida que crescem as distâncias pela necessidade de estabelecimento de uma maior infraestrutura (GORDON; MORGAN, 1993, p. 2).

Além disso, as comunicações por satélite possuem as vantagens de poderem

[8] Os princípios de segurança da informação digital são a confidencialidade, integridade, disponibilidade, autenticidade e legalidade (SILVA NETTO; SILVEIRA, 2007, p. 377).

operar com transmissões em *broadcast*[9], empregando banda larga[10], com ampla área de cobertura[11] e com relativa independência de barreiras naturais. Porém, o mais importante é que elas possibilitam comunicações em áreas sem infraestrutura implementada e em regiões marítimas. O seu uso é ainda essencial em áreas devastadas por catástrofes ou conflitos que destruíram a estrutura de telecomunicações (GORDON; MORGAN, 1993, p. 3-4).

Para garantir essas vantagens, um sistema de comunicações por satélite funciona como um retransmissor. Uma estação, por exemplo um navio, que deseja se comunicar, codifica[12] e modula[13] a sua mensagem, transmitindo para o satélite por um enlace ascendente (*uplink*). Este pode, então, realizar um processamento e amplificação do sinal, alterando sua frequência para realizar a transmissão para uma outra estação de terra por meio de um enlace descendente (*downlink*) (GORDON; MORGAN, 1993, p. 3-4).

Tradicionalmente, as transmissões dos usuários de um sistema de comunicações por satélite passarão por uma estação terrena de controle, uma vez que ela possui maior capacidade de processamento e roteamento[14] de informações. Dessa forma, se um navio desejar falar com outro, ele se comunicará com a estação terrena de controle via um satélite (FIG.3 – ANEXO C). Esse subsistema terrestre de controle retransmitirá a mensagem para o equipamento em órbita que fará o enlace descendente para o destinatário final (FIG. 4 - ANEXO C).

Apesar disso, existem exceções a essa estrutura habitual. Um exemplo é o Sistema

---

9 Transmissão de uma unidade para vários receptores, como no caso das emissoras de rádio comerciais (GORDON; MORGAN, 1993, p. 3).

10 O emprego de maior banda permite a transmissão de maior quantidade de dados e a maiores velocidades (GORDON; MORGAN, 1993, p. 3).

11 Área na qual é possível que um equipamento na superfície da Terra consiga se comunicar com o satélite. Considerações adicionais sobre a área de cobertura serão feitas posteriormente nesta pesquisa.

12 Transformação dos bits de informação em uma sequência que proveja segurança por meio da detecção e correção de erros. Basicamente, é como uma mensagem será estruturada em bits para que possa ser transmitida (SKLAR, 2008, p. 305).

13 Transformação de uma onda eletromagnética para que possa transportar a informação desejada (STALLINGS, 2004, p.131).

14 Definição de qual caminho deve ser usado por uma mensagem em uma rede para que ela chegue ao seu destinatário (STALLINGS, 2004, p.11).

Iridium[15], no qual o roteamento das mensagens pode ser feito pelos satélites. Um outro diferencial desse sistema é a possibilidade de a troca de mensagens ser feita entre os satélites. Essa tecnologia foi desenvolvida em face da impossibilidade de criar uma rede de estações terrenas para apoiar este sistema de alcance global (KELLER; SALZWEDEL, 1996, 1220).

No que tange à área de cobertura (*footprint*), ou seja, a área na qual é possível a um equipamento estabelecer um enlace, é importante entender que ela é resultado de uma série de características técnicas do sistema. Ela depende da órbita utilizada, da potência dos transmissores, da sensibilidade dos receptores e das dimensões[16] das antenas do satélite e do equipamento em terra. O ANEXO D ilustra a área de cobertura em determinado instante das constelações dos Sistemas Iridium (FIG. 5) e INMARSAT (FIG. 6).

Finalmente, é possível descrever simplificadamente as principais órbitas empregadas por esses sistemas. Apesar de existirem outros tipos de órbitas, serão apresentados os dois grupos avaliados como mais relevantes para a análise futura:

a) Órbita Geoestacionária (GEO);

b) Órbitas Baixas (*Low Earth Orbit* – LEO).

Na órbita GEO, o satélite fica posicionado a 35.786 km de altura em um plano próximo ao do Equador. Sua grande vantagem é que, nessa situação, sua velocidade de rotação é igual à da Terra, o que faz com que, relativamente à superfície do globo, o satélite pareça parado. Uma desvantagem é que em função das grandes distâncias envolvidas há um pequeno atraso no sinal (cerca de 0,5 s). Em face de ser única, uma posição geoestacionária é muito disputada entre os países para a colocação de satélites (GORDON; MORGAN, 1993, p. 56-57). A constelação INMARSAT (FIG. 6 – ANEXO D) é composta por 3 satélites GEO que

[15] Sistema comercial de comunicações por satélite operado pela Iridium Communications Inc., considerado o único sistema do gênero a possuir cobertura global. (IRIDIUM, 2015).

[16] As dimensões de uma antena são o principal parâmetro que definem o ganho de uma antena, ou seja, o quanto ela é capaz de concentrar energia em uma determinada direção em detrimento de outras (STUTZMAN; THIELE, 1998, p.37). Via de regra, mantidos os demais parâmetros constantes, quanto maior forem as antenas em terra, maior será o seu ganho, ou seja maior será a sua direcionalidade, implicando em maiores áreas de cobertura. Por outro lado, maiores antenas nos satélites implicam em menores áreas de cobertura (GORDON; MORGAN, 1993, p. 35-36).

cobrem cerca de 70% da superfície da Terra (não há cobertura nas regiões polares).

Já as órbitas LEO, em geral, são circulares situadas em altitudes entre 500 e 2000 km. Têm como principais vantagens a necessidade de lançadores menores, empregar satélites menores e mais simples e os atrasos poderem ser reduzidos (para cerca de 0,02 s), além de não ser necessário disputar um dos espaços orbitais geoestacionários. As suas desvantagens são a menor área de cobertura e o permanente movimento do satélite em relação à superfície da Terra, o que demanda um grande número de sistemas em órbita para assegurar a continuidade das comunicações (um dos princípios de C2) (GORDON; MORGAN, 1993, p. 60). A constelação Iridium (FIG. 5 – ANEXO D) é composta por 66 satélites LEO que cobrem toda a superfície da Terra. Como os satélites estão em movimento, a representação das áreas de cobertura da FIG. 5 são válidas apenas para um determinado instante.

A análise dos conceitos apresentados sobre as comunicações satélite permite tecer algumas observações. Inicialmente, devem ser sempre consideradas as características técnicas de cada sistema satélite para que as suas vulnerabilidades possam ser identificadas. Sistemas diferentes poderão ser mais vulneráveis a um determinado tipo de ameaça do que a outros.

De qualquer forma, alguns conceitos gerais são úteis. A mensagem é transmitida no ambiente por meio de uma codificação e modulação que deve ser entendida pelo receptor para o sucesso da comunicação. Além disso, é necessário que o receptor esteja dentro da área de cobertura do sinal, o que é uma função de várias características técnicas dos sistemas, inclusive as dimensões da antena do receptor.

É possível, agora, sumarizar as conclusões parciais que podem ser depreendidas do que foi discutido nesta seção.

3.5 Conclusões Parciais

Com essas ideias podemos concluir o referencial teórico sobre o C2, ressaltando a

sua importância para o desenvolvimento das operações militares. Ele, por sua vez, é uma composição de ciência e arte, não devendo ser negligenciado o seu estudo em bases científicas. O Ciclo de Boyd é uma parcela desses estudos científicos, já tendo inclusive sido doutrinariamente incorporado à MB.

O Ciclo de C2 prega a importância da rapidez da sua execução e do processo cognitivo de orientação, redundando na grande oportunidade que resultaria em entender e afetar negativamente o processo similar do oponente. Isso indica um grande potencial da obtenção de conhecimentos sobre o processo do oponente e como a interferência nessa etapa por meio de estratagemas pode prejudicar o inimigo. Tal ciclo se desenvolve sobre sistemas de comunicação que, em grande parte, empregam o espectro eletromagnético.

Essas ideias, entre outras, foram sumarizadas nos princípios de C2, que podem ser entendidos como requisitos. A junção desses princípios com os demais conceitos mencionados, permitiu a identificação das principais ameaças a sistemas de comunicações. Elas podem ser consolidadas como a possibilidade das comunicações serem monitoradas, interrompidas, ou que o oponente simule nossas próprias comunicações para afetar nosso processo cognitivo.

Além disso, foi apresentado que cada sistema satélite deve ter suas características técnicas analisadas individualmente para identificar suas capacidades. Porém, como visto em linhas gerais, um receptor será capaz de receber o sinal se estiver dentro da área de cobertura do satélite, que é uma função de várias características técnicas dos sistemas, inclusive as dimensões da antena do receptor. Por analogia, o conceito nos permite considerar que para cada sistema é necessário avaliar suas vulnerabilidades de acordo com as suas características.

Para tal, é necessário expandir os conceitos sobre a ameaça representada pela GE, o que será feito na próxima seção.

4 GUERRA ELETRÔNICA

Conforme mencionado anteriormente, nesta seção serão descritos, explicados e analisados os conceitos básicos referentes à GE. Tal passo é essencial para a compreensão da potencial ameaça às redes de comunicações por satélite que será abordada nesta pesquisa.

Para tal, inicialmente será descrito o conceito da GE. Posteriormente serão apresentadas, explicadas e analisadas as suas vertentes compostas pelas Medidas de Apoio à Guerra Eletrônica (MAGE)/ Inteligência de Sinal (INTSAL), Medidas de Ataque Eletrônico (MAE) e Medidas de Proteção Eletrônica (MPE).

4.1 Conceitos de Guerra Eletrônica

A GE é um conjunto de ações que envolvem o uso da energia eletromagnética com basicamente três finalidades distintas (BRASIL, 2014b, p. 3-23; BRASIL, 2007, p. 125):

a) determinar e explorar o uso do espectro eletromagnético pelo oponente para obter conhecimentos que podem incluir sua ordem de batalha, intenções e capacidades;

b) impedir, reduzir ou prevenir o uso pelo oponente de sistemas que empreguem ondas eletromagnéticas; e

c) proteger e assegurar o uso dos nossos sistemas que empreguem ondas eletromagnéticas.

Na primeira vertente de determinação e exploração do uso do espectro eletromagnético, encontram-se as MAGE e a INTSAL. Quando a finalidade é impedir, reduzir ou prevenir o uso de sistemas pelo oponente temos as MAE. Por fim, quando se deseja garantir o uso dos nossos sistemas, temos as MPE.

A seguir, serão discutidas esses elementos componentes da GE, iniciando-se pelas MAGE e INTSAL.

4.2 Medidas de Apoio à Guerra Eletrônica e Inteligência de Sinal

Conforme já comentado, as MAGE e a INTSAL visam determinar e explorar o uso que o oponente faz do espectro eletromagnético. A grande diferença é que nas MAGE o interesse é o emprego imediato em apoio a uma operação em execução, enquanto a INTSAL visa coletar conhecimentos de cunho estratégico para permitir o desenvolvimento de uma capacidade de GE, ou ainda para o planejamento de uma operação (tanto no nível operacional quanto tático) que ainda está por vir (BRASIL, 2007, p. 138, 156).

Os Fuzileiros Navais estadunidenses realizam essa diferenciação pelo cliente do conhecimento. Se o usuário daquele conhecimento for um comandante engajado em uma operação (tanto no nível operacional quanto tático), então está sendo realizada MAGE. Se por outro lado, aquele conhecimento se destina a um órgão que não o seu comandante operacional e/ou tático e é para uso futuro, então trata-se de INTSAL (EUA, 1999, p. 1-2).

Tanto as MAGE, quanto a INTSAL, podem estar voltadas para a área de comunicações ou para os demais sistemas que empreguem o espectro eletromagnético, tais como sensores e sistemas de navegação entre outros. Como o interesse desta pesquisa são as comunicações e os sistemas de C2, serão tratadas as questões das MAGE de comunicações (MAGE-COM) e da parcela da INTSAL chamada Inteligência de Comunicações (INTCOM) (BRASIL, 2007, p. 138).

As MAGE-COM e a INTCOM se iniciam com uma busca no espectro eletromagnético. Uma vez identificado um sinal que possa ser de interesse, ele começa a ser monitorado e posteriormente será analisado e o conhecimento obtido será registrado (BRASIL, 2007, p. 156). A análise do sinal é conduzida em cinco vertentes de análise: da mensagem, do tráfego, de localização eletrônica, técnica e final (VIEIRA, 2008, p.1).

A análise da mensagem visa produzir conhecimento a partir do conteúdo das mensagens. Para tal, faz-se necessário ser capaz de demodular e decodificar os sinais

interceptados. É necessário, também, a compreensão do idioma, para que a mensagem, ainda que obtida em texto claro possa ser plenamente entendida (VIEIRA, 2008, p.2).

Pela análise do tráfego podem ser obtidas informações a partir do fluxo de mensagens em determinada rede. Assim, é possível determinar se uma rede é para atender demandas logísticas ou táticas. Ou ainda, é possível determinar o indicativo de um comandante, uma vez que ele se comunica com todos os seus subordinados. Outros dados que podem ser levantados, por exemplo, são preparativos para o suspender de uma força naval, ou ainda o início de uma marcha para o combate por fuzileiros navais. Enquanto a INTCOM identifica previamente esses padrões, as MAGE-COM caso observem a existência daquele padrão previamente conhecido, poderão estimar o seu significado (VIEIRA, 2008, p.2).

A análise de localização eletrônica visa produzir conhecimentos sobre o posicionamento das forças inimigas. Naturalmente a distribuição espacial dos emissores dá indícios dos escalões envolvidos (pelotão, companhia, etc.) e do seu dispositivo empregado, conhecimentos essenciais seja para a defensiva quanto para a ofensiva (VIEIRA, 2008, p.2).

Por sua vez, a análise técnica utiliza os parâmetros do sinal interceptado (frequência, modulação, codificação, etc.). Esses dados permitem gerar conhecimentos sobre que tipo de oponente se encontra no campo de batalha com base nos equipamentos empregados. Possibilita, ainda, a estimativa da capacidade de GE do oponente, permitindo que redimensionemos as capacidades de nossa força ou exploremos as vulnerabilidades do adversário (VIEIRA, 2008, p.3).

Por último, a análise final é aquela que integra o conhecimento produzido pelas demais análises (VIEIRA, 2008, p.3). É importante ressaltar que a impossibilidade de realizar uma das análises não inviabiliza a geração de conhecimento que não possa ser extremamente útil tanto como MAGE-COM quanto para a INTCOM.

Uma análise conceitual das MAGE e da INTSAL quando comparadas com o

Ciclo de C2 permite realizar as seguintes observações. Inicialmente, deve ser considerado que, como um sensor, ela se baseia na fase de observação do ciclo. Ao permitir monitorar as comunicações que compõem as setas no interior do ciclo do oponente, é possível iniciar o nosso ciclo antes que o do oponente acabe. Não é mais necessário aguardar a decisão, seguida da ação para que os nossos sensores detectem, por exemplo o deslocamento de tropas. É possível interceptar a ordem, ou até mesmo a consulta de um comandante questionando em quanto tempo uma tropa estará pronta para se deslocar.

Esses dados não devem limiar a análise das possibilidades do inimigo em um processo de planejamento, que devem ser exaustivamente analisadas, mas podem apoiar o processo decisório do comandante. Esta é uma das formas observadas para efetivamente se conseguir "entrar" no processo decisório do oponente e antecipar suas ações. Naturalmente o risco de estratagemas deve ser sempre cuidadosamente analisado.

Feita essa análise, serão discutidos os conceitos inerentes à segunda vertente da GE, as MAE, que visam impedir, reduzir ou prevenir o uso pelo oponente de sistemas que empreguem ondas eletromagnéticas.

4.3 Medidas de Ataque Eletrônico

Quando a finalidade é impedir, reduzir ou prevenir a utilização do espectro eletromagnético pelos sistemas do inimigo, temos as MAE. Elas podem ser divididas em destrutivas e não-destrutivas (BRASIL, 2014b, 3-24). As MAE destrutivas incluem os mísseis antirradiação e as armas de energia direcionada (ADAMY, 2001, p. 4). Elas não serão abordadas nesta pesquisa, uma vez que, pela especificidade que demandam para seu emprego contra satélites, compõem uma subclasse de um tipo especial de armamento chamado de antissatélite (ASAT), ficando, entretanto, o registro de sua existência.

Já as MAE não-destrutivas podem ser divididas em supressão eletromagnética

(genericamente chamada de bloqueio), despistamento eletromagnético (referido nesta pesquisa como despistamento, uma vez que manteremos o emprego do termo estratagema para os demais casos) e armas de energia direcionada (POISEL, 2004, p. 2). Para este trabalho, serão considerados apenas o bloqueio e o despistamento pela sua relevância.

O bloqueio visa interromper as comunicações em determinado momento o que poderá inviabilizar o uso daquele sistema, ou causar retardos sensíveis para que as comunicações aconteçam (POISEL, 2004, p. 2). Já o despistamento visa induzir o oponente a erro pela geração de informações falsas (BRASIL, 2007, p. 82). A forma de realização desse despistamento de interesse a esta pesquisa é a geração de mensagens que simulem as comunicações do próprio inimigo de forma que ele entenda terem sido geradas por suas próprias forças, sendo por isso chamado de despistamento imitativo (BRASIL, 2014a, p.2-2).

A partir do descrito, fica patente que as MAE objetivam atingir as comunicações de duas formas distintas. Na primeira, é esperada a interrupção, ainda que temporária, das comunicações. Conforme apresentado nos conceitos sobre C2, essa medida causa atrasos na condução do Ciclo de Boyd e afetam os princípios da confiabilidade, da continuidade e da rapidez. Já 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. Ele atua amplificando a névoa da guerra, e 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.

Tendo sido discutidas as MAE de interesse, é agora possível apresentar os tópicos de interesse sobre Medidas de Proteção Eletrônicas.

4.4 Medidas de Proteção Eletrônica

As MPE são aquelas que visam proteger e assegurar o uso pelos nossos sistemas

das ondas eletromagnéticas. Como naturalmente as ameaças da GE são as MAGE e as MAE, as MPE podem ser classificadas em anti-MAGE e anti-MAE.

São alguns exemplos de MPE anti-MAGE, o emprego de criptografia, de códigos ou cifras que visam negar o conteúdo da mensagem. Alterações frequentes de indicativos prejudicando a análise de tráfego. Emprego de antenas direcionais que restringem a área na qual é possível a interceptação das comunicações. Uso de técnicas de transmissão de espalhamento espectral por sequência direta[17] que visam reduzir a potência do sinal transmitido, prejudicando a busca de interceptação MAGE (BRASIL, 2014a, p.2-2 – 2-8).

Dentre as MPE anti-MAE temos o espalhamento espectral por salto em frequência[18], diminuindo a eficiência do ataque eletrônico. A já citada criptografia, também é assim considerada, uma vez que dificulta o emprego do despistamento imitativo. Outro exemplo é o uso de autenticação e outros procedimentos de segurança que visem confirmar a origem de uma mensagem. Sendo um outro exemplo, o uso de antenas direcionais também dificulta o ataque eletrônico, exigindo maiores potências de ataque para torná-lo eficaz.

Ao analisarmos o exposto sobre as MPE, podemos observar que a sua existência pressupõe a existência das ameaças. Só existem MPE por que existem MAGE/INTSAL e MAE. Essa relação causal, apesar de parecer óbvia, é importante de ser formalmente observada. Como um exemplo, o propósito da criptografia é prioritariamente proteger as comunicações de interceptação e secundariamente dificultar o despistamento imitativo. Não existe sentido em instalar criptografia em um sistema se essas ameaças não forem percebidas.

É possível, agora, sumarizar as conclusões parciais que podem ser depreendidas do que foi discutido nesta seção.

---

[17] Técnica de sistema que visa gerar múltiplas cópias do sinal que são espalhadas no espectro eletromagnético, reduzindo a potência de pico do sinal transmitido (POISEL, 2004, p. 7).

[18] Técnica de sistema na qual o equipamento altera a sua frequência de transmissão rápida (às vezes em milésimos de segundo), sistematicamente e seguindo uma sequência pseudoaleatória, fazendo com que um bloqueador tenha um tempo de atraso para identificar a nova frequência a ser atacada ou tenha que dividir sua potência de bloqueio em uma grande faixa do espectro (POISEL, 2004, p. 8-9).

4.5 Conclusões Parciais

Quando essas ameaças são comparadas com a GE vemos uma semelhança muito grande. As MAGE e a INTSAL permitem o monitoramento das comunicações. Isto agiliza o nosso Ciclo de C2, uma vez que não é necessário o início da ação do oponente. 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.

Já as MAE, como apresentado, permitem a interrupção das comunicações e o despistamento. A primeira, ainda que ocorra apenas temporariamente, ocasiona atrasos no ciclo de C2. Já o despistamento, especialmente o do tipo imitativo, é capaz de prejudicar a cognição do oponente, prejudicando o seu processo decisório e ampliando a névoa da guerra. Secundariamente ele retarda a condução do Ciclo de Boyd, ao tirar a credibilidade do sistema de C2 demandando uma reavaliação dos conhecimentos existentes.

Finalmente, como visto, as MPE podem ser usadas como um indício muito claro da ameaça percebida, tanto da MAGE e da INTSAL, quanto das MAE. A sua existência se justifica pela presença da ameaça.

Nas duas seções posteriores, será analisado como essas correlações e interações entre o apresentado entre C2 e GE ocorrem no que tange às comunicações satélite. Os princípios básicos de funcionamento das comunicações por satélite foram apresentados. Foi possível identificar que existem diferentes tipos de sistemas por satélite e que deverão ser analisados individualmente de maneira mais profunda. Entretanto foi possível identificar princípios gerais que poderão apoiar esta análise posterior.

O próximo capítulo apresentará a análise das vulnerabilidades e as tentativas de falseamento da hipótese da pesquisa de que as comunicações por satélite são vulneráveis à GE.

5 ANÁLISE DAS VULNERABILIDADES

A seção 2 demonstrou que se assumiu a hipótese dedutiva que as comunicações por satélite, por empregarem o espectro eletromagnético, são vulneráveis à GE. Agora, podemos expandir este conceito, indicando que, mais especificamente, elas são vulneráveis às MAGE/ INTSAL e MAE e deverão empregar MPE para garantir seu funcionamento. Essa conjectura será falseada nesta seção, ou seja, será tentado desmenti-la. Isso será feito em duas etapas. A primeira, conceitual, estudará a viabilidade da consecução das ameaças às comunicações por satélite a partir dos conceitos teóricos estabelecidos até o momento. A segunda, será feita por meio da apresentação de casos conhecidos e disponíveis nas fontes abertas em que os requisitos de C2 foram afetados, bem como, da existência de MPE em satélites, o que contribuirá para comprovar as análises realizadas.

A TAB. 2 correlaciona os dados levantados na subseção de C2 com os componentes da GE, a partir dos quais realizaremos a presente análise.

TABELA 2
Correlação entre ameaças, princípios de C2 e a GE

Ameaça	Princípios de C2	GE
Monitoragem	Segurança	MAGE/INTSAL
Interrupção	Confiabilidade, continuidade e rapidez	MAE
Simulação de Comunicações Falsas	Segurança	MAE

Dessa forma, esta seção analisará, inicialmente, o efeito das MAGE/INTSAL e posteriormente das MAE contra as comunicações por satélite.

5.1 MAGE/INTSAL contra as Comunicações Satélite

Conforme já mencionado, a comunicação com o satélite ocorre por meio de um *uplink* e originada dele por meio de um *downlink*. Teoricamente seria possível interceptar as comunicações do *uplink* ou do *downlink*, bastando que para isso o receptor estivesse dentro da área de cobertura da conexão.

Monitorar um *uplink* é uma atividade mais complexa, que demandaria a presença de uma aeronave ou outro satélite para facilitar a interceptação dessa comunicação ascendente. Já para monitorar o *downlink* seria necessária uma outra estação de terra dentro da área de cobertura do satélite. Deve-se ainda levar em consideração que essa área de cobertura pode ser ampliada pelo uso de grandes antenas em solo.

É possível que o *downlink* para as estações de controle em terra tenham uma área de cobertura diferente da conexão descendente para os usuários finais. Essa peculiaridade pode fazer com que apenas um dos dois *downlinks* possa ser monitorado. Essa lógica é a mesma aplicada na teoria da GE para a interceptação de qualquer tipo de comunicação, cujos conceitos encontram-se na obra de vários autores como Adamy (2009, p. 235-250).

O efeito prático desse fenômeno é que, nesses casos, pode ser ouvido apenas um lado das comunicações. Por exemplo, suponhamos que só seja possível monitorar o *downlink* para a estação de controle. Nesse caso, se temos uma comunicação originada em terra, por exemplo, que chega por fibra ótica à estação de controle e é transmitida para o satélite e depois para um navio, como esse enlace descendente não será interceptado, será impossível ouvir essa parte da comunicação. Entretanto, a resposta, que sai do navio para o satélite e depois é realizado o link descendente para a estação de controle, poderá ser interceptada.

Nesse mesmo sistema hipotético, se for imaginada uma viatura no terreno que deseje se comunicar com esse mesmo navio por meio de um satélite, a transmissão, nesse caso, seria feita diretamente com o satélite e deste seria realizado um *downlink* para a estação de controle (poderá ser monitorada) (FIG.7 – ANEXO E), subindo novamente e chegando ao navio. A resposta seguiria um caminho análogo e também poderia ser monitorada (FIG.8 – ANEXO E).

O exemplo demonstra que existe a possibilidade de monitoração, mas que como se trata de um evento técnico, deve ser analisado cuidadosamente dependendo do sistema

utilizado. Por outro lado, não se deve considerar isso uma desvantagem. Essa lógica, nas quais muitas vezes só um dos lados da comunicação pode ser ouvido, é a mesma que ocorre em outras situações nas atividades de GE. A atividade de inteligência, consiste exatamente em tentar juntar esses retalhos de dados para que se possa formar uma colcha de conhecimento (KEEGAN, 2002, p. 5-6).

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.

Se considerarmos que o sistema de comunicações por satélite é extremamente importante e confiável, isso o torna canal prioritário para o tráfego das comunicações mais sensíveis de uma Força Armada. Essa importância relativa também o coloca como um tráfego prioritário para as atividades de criptoanálise. Uma vez que esse processo é altamente dispendioso de pessoal e recursos computacionais, é de se supor que sua priorização se dá em relação à importância das comunicações que devam trafegar naquele canal e que, portanto, justifiquem o esforço criptoanalítico (SHULSKY; SCHMITT, 2002, p. 42-48).

Finalmente a localização eletrônica é uma análise um pouco mais complexa. O método mais facilmente visualizado seria por meio da triangulação das emissões de uma conexão ascendente, empregando, por exemplo, uma aeronave. Um segundo método, poderia ser por meio da medição das reflexões secundárias da transmissão em outros satélites geoestacionários. Uma vez que esses satélites na órbita GEO têm posições relativamente conhecidas, pelas diferenças de tempo de chegada, seria possível estimar uma área de incerteza do transmissor, em uma lógica matemática muito similar à empregada pelo Sistema

de Posicionamento Global por satélite (GPS).

Um terceiro método, mais engenhoso, considera que muitas estações de usuários transmitem seus dados de posição no seu protocolo de funcionamento, para permitir a seleção das frequências de link descendente e consequentemente o roteamento das mensagens. Logo, a capacidade de interceptar o sinal do satélite já proveria também a análise de localização. Um dos sistemas que opera dessa forma é o sistema INMARSAT que informa a posição do usuário a intervalos frequentes (CURTIS, 2014).

Conforme mencionado anteriormente, a presença de MPE anti-MAGE é um claro indício de que o próprio fabricante dos satélites identificam a ameaça de interceptação. Um exemplo é o emprego de criptografia em satélites comerciais (INMARSAT, 2012). Um outro exemplo é a possibilidade de emprego de pequenas áreas de cobertura conteiráveis que podem acompanhar as estações de interesse (ARAKAKI, 2009, p. 30), dificultando a interceptação do enlace descendente.

Um outro indício da possibilidade de interceptação são as inúmeras referências ao sistema *Echelon*[19]. Além disso, a presença de novas estações de monitoragem de comunicações em países como a Nova Zelândia e as suas relações com a Agência de Segurança Nacional (*National Security Agency – NSA*) dos EUA tornadas conhecidas por documentos vazados por Edward Snowden[20], confirmam esse conhecimento (GALLAGHER; HAGER, 2015). O exemplo mais recente é um extrato de um banco de dados da NSA vazado no Wikileaks[21] e que indica, entre os telefones prioritários para monitoragem do Brasil, o número do equipamento INMARSAT do avião presidencial (CHADE, 2015; WIKILEAKS, 2015).

Com isso ficou patente que não só a monitoragem de comunicações satélite,

[19] Programa usado por algumas estações de interceptação de comunicações por satélite dos EUA e do Reino Unido para coleta, análise e disseminação de comunicações interceptadas (KEEFE, 2005, p. 294).

[20] Ex-analista da NSA que vazou documentos sobre os programas de monitoragem daquela agência (FRANCE PRESSE, 2015).

[21] Organização Não Governamental de mídia que divulga documentação sigilosa de várias organizações. (WIKILEAKS, 2011).

incluindo todas as suas análises, não só é tecnicamente possível, como há vários indícios de seu emprego em fontes ostensivas. Esses indícios estão associados à presença de MPE anti-MAGE, documentos vazados e à própria existência de estações de monitoragem de satélites espalhadas pelo mundo. Várias fontes poderiam corroborar esse trecho da pesquisa, mas a citação deles foi restrita, pois essas fontes iriam apenas confirmar os indícios já mencionados.

Na próxima subseção será abordada a análise da ameaça representada pelas MAE contra as comunicações por satélite.

5.2 MAE contra as Comunicações Satélite

Conforme mencionado anteriormente, as MAE podem funcionar, para efeito desta análise, como bloqueio ou como despistamento imitativo. O conceito de operação de ambos é muito similar, por isso estão sendo agrupados.

O ataque pode realizar-se tanto no enlace ascendente, quanto no descendente. No primeiro caso, o ataque é realizado contra o satélite, enquanto no segundo, o ataque é realizado contra a estação terrena. Basicamente, é necessário que o atacante possua um sistema transmissor e que suas características técnicas sejam capazes de sensibilizar o receptor, seja do satélite ou da estação terrena.

O despistamento imitativo demanda 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. Embora mais difícil, seu potencial de exploração é muito superior por afetar o processo cognitivo do oponente. Já o bloqueio trabalha com uma premissa de que, se for empregada potência suficiente, o ataque será satisfatório. Apesar de ser um método de mais fácil execução, o seu menor refinamento redunda em resultados diferentes do despistamento, uma vez que ele busca interromper a comunicação, gerando atrasos no Ciclo C2.

Quando analisamos pelo aspecto das MPE, podemos identificar que um dos três

segmentos de comunicações militares estadunidenses é de sistemas protegidos ou seguros. O grande diferencial desse segmento é a forte presença de MPE anti-MAE e o seu foco de emprego será na gerência de comunicações e para centros de C2 móveis, entre outros (ARAKAKI, 2009, p. 28). Pode ser observado que o sistema com maior capacidade de MPE, e portanto, maior custo, é aquele responsável pela estrutura de C2. Esse fato, por si só, indica a execução de um gerenciamento de risco pelas Forças Armadas estadunidenses.

Em um estudo dos casos disponíveis na literatura ostensiva, pode ser encontrada a previsão de ataque à constelação de satélites estadounidense MILSATCOM, em moldes similares ao proposto neste trabalho (SCHLEHER, 1999, p. 53). Essa possibilidade foi confirmada pelo General John Hyten[22] que informou que as redes de comunicações por satélite são constantemente atacadas por elementos externos (MATISHAK, 2015).

Em uma situação emblemática, a Polícia Rodoviária Federal prendeu em 5 de maio de 2015 um caminhoneiro que, a partir da adaptação de sistemas comerciais de baixo custo, fazia uso pessoal do sistema estadunidense de comunicações militares por satélite FLEETSATCOM, interferindo nas comunicações da marinha daquele país (COSTA; ARAÚJO, 2015). Caso similar ocorreu em 2009 com inúmeros presos (FOLHA ONLINE, 2009).

Esses casos demonstram, não só a possibilidade de realizar ataques a sistemas de comunicações por satélite, mas também que, dependendo dele, tal ofensiva pode ser realizada por meios rudimentares e pessoal com pouco conhecimento técnico. Tendo sido comprovada a vertente relacionada com a ação das MAE contra os satélites, podemos concluir esta seção.

5.3 Conclusões Parciais

Nesta seção foi possível avaliar conceitualmente se seria possível realizar a

[22] Comandante do Comando Espacial da Força Aérea estadunidense em 2015 (MATISHAK, 2015).

monitoragem, o despistamento e o bloqueio das comunicações por satélite. Não só foi considerada conceitualmente viável, como foram apresentados casos disponíveis na literatura ostensiva e que confirmam a sua ocorrência.

Esses casos envolveram desde a presença de MPE em satélites para fazer frente a essas ameaças, como casos reais de ocorrência dos eventos, consolidados em documentos indicando a sua execução ou em equipamentos para tal. O que é marcante, ainda, é que em alguns dos casos, foi comprovado que elementos não estatais de pequeno conhecimento técnico e com recursos rudimentares conseguiram afetar o funcionamento de sistemas de comunicações militares estadunidenses.

Tal fato confirma a nossa hipótese de que as comunicações por satélite são vulneráveis à GE.

6 CONCLUSÃO

Esta pesquisa se propôs a responder a seguinte questão: será que as comunicações por satélite são completamente seguras como se imagina?

Para tal, uma vez que as redes de comunicações por satélite são parte de um sistema de C2, o seu referencial teórico foi apresentado, explicado e analisado, ressaltando a sua importância para o desenvolvimento das operações militares. O C2 é uma composição de ciência e arte, não devendo ser negligenciado o seu estudo em bases científicas. O Ciclo de C2 é uma parcela desses estudos científicos, já tendo inclusive sido doutrinariamente incorporado à MB.

O Ciclo de Boyd, conforme apresentado, prega a importância da rapidez da sua execução e enfatiza a importância do processo cognitivo de orientação, redundando na grande oportunidade que resultaria em entender e afetar negativamente o processo similar do oponente. Isso indicou um grande potencial da obtenção de conhecimentos sobre esse processo do oponente e como a interferência nessa etapa por meio de estratagemas pode prejudicar o inimigo.

Tais ideias, entre outras, foram sumarizadas nos princípios de C2, que podem ser entendidos como requisitos. A junção desses princípios com os demais conceitos mencionados, permitiu a identificação das principais ameaças a sistemas de comunicações. Elas puderam ser consolidadas como a possibilidade de as comunicações serem monitoradas, interrompidas, ou que o oponente simule nossas próprias comunicações para afetar nosso processo cognitivo.

Essas possíveis ameaças foram então comparadas com a GE, tendo sido observada uma semelhança muito grande. As MAGE e a INTSAL permitem o monitoramento das comunicações. Isso agiliza o nosso Ciclo de C2, uma vez que não é necessário o início da ação do oponente. Permite, ainda, analisar e entender o processo cognitivo do oponente,

permitindo, em conjunto com as possibilidades do inimigo, que o comando esteja melhor preparado para antecipar as ações do adversário.

Já as MAE, como apresentado, permitem a interrupção das comunicações e o despistamento. A primeira, ainda que ocorra apenas temporariamente, ocasiona atrasos no ciclo de C2. Já o despistamento, especialmente o do tipo imitativo, é capaz de prejudicar a cognição do oponente, prejudicando o seu processo decisório e ampliando a névoa da guerra. Secundariamente ele retarda a condução do Ciclo de Boyd, ao tirar a credibilidade do sistema de C2 demandando uma reavaliação dos conhecimentos existentes.

Finalmente, como visto, as MPE puderam ser usadas como um indício muito claro da ameaça percebida, tanto da MAGE e da INTSAL, quanto das MAE. A sua existência se justificaria apenas pela presença da ameaça.

Quando a GE foi confrontada com as comunicações por satélite, foi possível avaliar conceitualmente que seria possível realizar a monitoragem, o despistamento e o bloqueio das comunicações por satélite. Não só foi considerada conceitualmente viável, como foram apresentados casos disponíveis na literatura ostensiva e que confirmam a sua ocorrência.

Esses casos envolveram desde a presença de MPE em satélites para fazer frente a estas ameaças, como casos reais de ocorrência dos eventos, consolidados em documentos indicando a sua execução ou em equipamentos para tal. O que é marcante, ainda, é que em alguns dos casos, foi comprovado que elementos não estatais de pequeno conhecimento técnico e com recursos rudimentares conseguiram afetar o funcionamento de sistemas de comunicações militares estadunidenses. Esta pesquisa, dessa forma, confirmou a hipótese de que as comunicações por satélite são vulneráveis à GE.

Esta análise foi toda baseada em documentação ostensiva, assegurando que o conhecimento possa ser disseminado sem as restrições dos documentos sigilosos. Além disso,

a identificação da vulnerabilidade das comunicações por satélites empregando apenas documentos disponíveis ao público em geral permite estimar que as vulnerabilidades possam ser muito mais profundas se analisadas a partir de documentação sigilosa.

Conforme apresentado, cada sistema satélite deve ter suas características técnicas analisadas individualmente para identificar suas capacidades e vulnerabilidades. Também como mencionado, a possibilidade de monitoragem, bloqueio e despistamento das nossas comunicações por satélite devem ser consideradas nas possibilidades do inimigo e no gerenciamento de risco. Deve ser considerado que essa atividade é repleta de sigilo o que prejudicaria a confirmação dessa capacidade e que, dependendo do caso, elementos de pequeno conhecimento técnico e com recursos rudimentares tiveram meios para executar essa tarefa. Naturalmente, dentro do conceito de gerenciamento do risco, dependendo das características do sistema e das suas MPE, as suas probabilidades de ocorrência e impactos serão analisados diferentemente.

Como sugestões para trabalhos futuros, poderia ser avaliada a vulnerabilidade das comunicações satélite às ações de Guerra Cibernética e às armas anti-satélite. Além disso, poderia ser feita uma análise, também de fonte aberta, da legislação estadunidense, incluindo o Ato de Vigilância de Inteligência Estrangeira (*Foreign Intelligence Surveillance Act – FISA*), permitindo identificar de maneira ostensiva as vulnerabilidades a que a MB está exposta em suas atividades em solo estadunidense.

Este trabalho, por ser ostensivo, abre a oportunidade para divulgação irrestrita e, consequentemente, para aprimorar a compreensão das vulnerabilidades das redes de C2 baseadas em comunicações por satélite. Contribuirá, ainda, com a compreensão das possibilidades de emprego da GE contra esse tipo de redes de comunicação de interesse, incrementando a mentalidade operacional da MB.

REFERÊNCIAS

ADAMY, David. *EW 101*: a first course in electronic warfare. Boston: Artech House, Inc., 2001, 308 p.

ADAMY, David. *EW 103*: tactical battlefield communications electronic warfare. Boston: Artech House, Inc., 2009, 330 p.

ALBERTS, David S. *The unintended consequences of information age technology*. Washington, DC: National Defense University, 1996, 62 p.

ARAKAKI, Fábio Kenji. Comunicações Satelitais Militares – perspectivas para o futuro. *Revista Passadiço*, Niterói, n. 29, p. 28-32, 2009.

BRASIL. Ministério da Defesa. *Gerenciamento do risco operacional nas operações conjuntas*. 1. ed. Brasília, DF, 2015. 15 f.

_____. Comando de Operações Terrestres. *EB70-CI-11.403 Caderno de instrução*: Medidas de Proteção Eletrônica. 1. ed. Brasília, DF, 2014a. 44 p.

_____. Estado-Maior da Armada. *EMA-305 Doutrina Básica da Marinha*. 2. Rev. Brasília, DF, 2014b. 102 p.

_____. Ministério da Defesa. *MD-31-M-03 Doutrina para o Sistema Militar de Comando e Controle*. Brasília, DF, 2014c. 44 p.

_____. _____. *MD30-M-01 Doutrina de operações conjuntas*. v.1. Brasília, DF, 2011. 128 p.

_____. _____. *MD-35-G-01 Glossário das Forças Armadas*. Brasília, DF, 2007. 274 p.

_____. Estado-Maior da Armada. *EMA-331 Manual de planejamento operativo da Marinha*. 1. ed. v. 1. Brasília, DF, 2006. 139 p.

CARDOSO, Caio G. A Guerra Eletrônica e a batalha da informação. *Revista Passadiço*, Niterói, n. 32, p. 44-46, 2012.

CHADE, Jamil. EUA interceptaram até o telefone do avião de Dilma, diz Wikileaks. *Estadão*, São Paulo, 4 jul. 2009. Disponível em: <http://politica.estadao.com.br/noticias/geral,ate-telefone-do-aviao-de-dilma-foi-interceptado-pelos-eua--dizem-wikileaks,1719184>. Acesso em: 18 jul. 2015.

CLAUSEWITZ, Carl Von. *On war.* Tradução de J. J. Graham. [Thousand Oaks, CA]: BN Publishing, 2007. 167 p.

CORAM, Robert. *BOYD: the fighter pilot who changed the art of war.* New York: Back Bay Books, 2002. 484 p.

CORBETT, Julian S. *Principles of maritime strategy.* New York: Longmans, Green and Co.,

1911. 317 p.

COSTA, Catarina; ARAÚJO, Gilcilene. PRF prende caminhoneiro com rádio que intercepta satélite americano. *G1 PI*, Teresina, 05 maio 2015. Disponível em: <http://g1.globo.com/pi/piaui/noticia/2015/05/prf-prende-caminhoneiro-com-radio-que-intercepta-satelite-americano-no-pi.html>. Acesso em: 18 jul. 2015.

COUTAU-BÉGARIE, Hervé. *Tratado de estratégia*. Tradução de Brigitte Bentolila de Assis Manso et. al. Rio de Janeiro: Escola de Guerra Naaval, 2010.776 p.

CREVELD, Martin Van. *Command in war*. Cambridge: Harvard University Press, 1985. 339 p.

CURTIS, Sophie. Malaysia Airlines MH370 search: latest. *The Telegraph*, London, 24 mar. 2014. Disponível em: <http://www.telegraph.co.uk/technology/news/10719304/How-British-satellite-company-Inmarsat-tracked-down-MH370.html>. Acesso em: 25 jul. 2015.

DOMÍNGUEZ, Néstor Antonio. *Satélites*: Vª etapa tecnologica naval y su incidencia en la guerra de Malvinas. Buenos Aires: Instituto de Publicaciones Navales, 1990. 845 p.

EUA. Department of Defense. *JP 1-02 Department of Defense dictionary of military and associated terms*. Washington, DC, 2010. 466 p. Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>. Acesso em: 18 jul. 2015.

_____. U.S. Marine Corps. *MCWP 2-15.2 Signals Intelligence*. Washington, DC, 1999. 123 p.

EX4U TELECOM. *All new Iridium 9555*. Escazu, 2015. Disponível em: <http://www.ex4u.org/Iridium_9555.php>. Acesso em: 18 jul. 2015.

FOLHA ONLINE. PF prende um em operação contra uso ilícito de satélites militares americanos. *Folha Online*, São Paulo, 18 mar. 2009. Disponível em: <http://www1.folha.uol.com.br/poder/2009/03/536889-pf-prende-um-em-operacao-contra-uso-ilicito-de-satelites-militares-americanos.shtml>. Acesso em: 18 jul. 2015.

FRANCE PRESSE. Casa Branca se nega a dar perdão presidencial a Edward Snowden. *G1 Mundo*, [Rio de Janeiro], 28 jul. 2015. Disponível em: <http://g1.globo.com/mundo/noticia/2015/07/casa-branca-se-nega-a-dar-perdao-presidencial-a-edward-snowden.html>. Acesso em: 28 jul. 2015

GALLAGHER, Ryan; HAGER, Nicky. Documents shine light on shadowy new zealand surveillance base. *The Intercept*, [S.l.], 7 mar. 2015. Disponível em: <https://firstlook.org/theintercept/2015/03/07/new-zealand-ironsand-waihopai-nsa-gcsb/>. Acesso em: 28 jul. 2015

GORDON, Gary D.; MORGAN, Walter L. *Principles of communications satellite*. New York: John Wiley & Sons, Inc., 1993. 533 p.

INMARSAT. *Using the Crypto AG voice encription system over BGAN*. London, 2012. Disponível em: <http://www.inmarsat.com/wp-

content/uploads/2013/10/Inmarsat_Using_Crypto_AG_Voice_Encryption_System_over_BGAN%20.pdf>. Acesso em: 18 jul. 2015.

INMARSAT. *Our Coverage*. London, 2015a. Disponível em: <http://www.inmarsat.com/about-us/our-satellites/our-coverage/>. Acesso em: 18 jul. 2015.

Iridium. *Company profile*. McLean (VA), 2015. Disponível em: <https://www.iridium.com/About/CompanyProfile.aspx>. Acesso em: 26 jul. 2015.

KEEFE, Patrick Radden. *Chatter*: uncovering the echelon surveillance network and the secret world of global eavesdropping. New York: Random House Trade Paperbacks, 2005. 312 p.

KEEGAN, John. *Intelligence in war*: the value-and limitations-of what the military can learn about the enemy. New York: Vintage Books, 2002. 387 p.

KELLER, Harald; SALZWEDEL, Horst. Link Strategy for the mobile satellite system Iridium. In: VEHICULAR TECHNOLOGY CONFERENCE, 1996, Atlanta. *Mobile Technology for the Human Race,* IEEE 46th, vol. 2. Atlanta: IEEE, 1996. p. 1220-1224. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.44.9979&rep=rep1&type=pdf>. Acesso em: 19 jul. 2015.

MATISHAK, Martin. Cyber general: US satellite networks hit by 'millions' of hacks. *The Hill*, [S.l.], 28 abr. 2015. Disponível em: <http://thehill.com/policy/defense/240286-general-us-space-networks-probed-millions-of-times-annually>. Acesso em: 23 jul. 2015

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Fundamentos de metodologia científica*. 7. ed. São Paulo: Atlas, 2010. 297 p.

MATEUS. In: NOVA BÍBLIA PASTORAL. N.T. *Evangelho segundo Mateus*. São Paulo: Paulus, 2014. 1543 p.

OPSAHL, T.; AGNEESSENS, F.; SKVORETZ, J. Node centrality in weighted networks: Generalizing degree and shortest paths. *Social Networks*, v. 32, n. 3, 245-251, Abr. 2010. Disponível em: <http://toreopsahl.com/2010/04/21/article-node-centrality-in-weighted-networks-generalizing-degree-and-shortest-paths/>. Acesso em: 19 jul. 2015.

PFLANZ, Mark; LEVIS, Alexander. An approach to evaluating resilience in command and control architectures. In: NEW CHALLENGES IN SYSTEMS ENGINEERING AND ARCHITECTING CONFERENCE ON SYSTEM ENGINEERING RESEARCH, 2012, St. Louis, MO. *Procedia Computer Science*. St. Louis: Elsevier, 2012. p. 141-146. Disponível em: <http://ac.els-cdn.com/S1877050912000312/1-s2.0-S1877050912000312-main.pdf?_tid=746d1a3c-3326-11e5-8a3f-00000aacb35e&acdnat=1437867776_9da01ab47e47d9cf7ec3ede96b2ed7a0>. Acesso em: 25 jul. 2015.

POISEL, Richard A. *Modern communicatios jamming principles and techniques*. Boston: Artech House, 2004. 479 p.

POPPER, Karl S. *A lógica da pesquisa científica*. 2. ed. São Paulo: Cultrix, 1975 *apud* MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Fundamentos de metodologia*

científica. 7. ed. São Paulo: Atlas, 2010. 297 p.

SCHLEHER, D. Curtis. *Electronic Warfare in the information age*. Boston: Artech House, 1999. 605 p.

SELLERS, Jerry Jon. *Understanding space*: an introduction to astronautics. 3rd ed. Com contribuições de William J. Astore, Robert B Giffen, Wiley J Larson. New York: McGraw-Hill Higher Education, 2005. 774 p.

SHULSKY, Abram N.; SCHMITT, Gary J. *Silent Warfare*: understanding the world of intelligence. 3. ed. Washington, DC: Potomac Books, Inc., 2002. 246 p.

SILVA NETTO, Abner da; SILVEIRA, Marco Antonio Pinheiro da. Gestão de segurança da informação: fatores que influenciam a sua adoção em pequenas e médias empresas. *Journal of information systems and technology management*, São Paulo, v. 4, n. 3, p. 375-197, 2007. Disponível em: <http://www.scielo.br/pdf/jistm/v4n3/07.pdf>. Acesso em: 26 jul. 2015.
SKLAR, Bernard. *Digital communication*: fundamentals and applications.2nd ed. London: Prentice Hall, 2008. 1079 p.

SPINNEY, Franklin C. *Evolutionary epistemology*: a personal view of John Boyd's "Destruction and Creation" … and its centrality to the … OODA loop. Versão 2.4, 2014. [S.l.]. Disponível em: <https://dl.dropboxusercontent.com/u/52781209/Evolutionary%20Epistemology%20copy.pdf>. Acesso em: 19 jul. 2015.

STALLINGS, William. *Data and computer communications*. 7th ed. London: Pearson Prentice Hall, 2004. 847 p.

STUTZMAN, Warren L.;THIELE, Gary A. *Anthena theory and design*. 2nd ed. Hoboken, NJ: John Wiley & Sons, 1998. 648 p.

TOFLER, Alvin; TOFLER, Heidi. *War and anti-war*: making sense of today's global chaos. 1. ed. New York: Warner Books, Inc., 1995. 370 p.

TREMBLAY JR, *Shaping and adapting*: unlocking the power of Colonel John Boyd's OODA Loop. 2015. 33 f. Dissertação (Master of Military Studies) – Command and Staff College, Marine Corps University, Quantico, 2015.

TZU, Sun. *A arte da guerra.* Tradução de José Sanz. Rio de Janeiro: Record, 2002. 112 p. Adaptação em inglês do original japonês: James Clavell.

VIEIRA, Alexandre Mindas. O avanço tecnológico e as novas habilidades do analista de GE. *Sentinela da Colina*, n. 6, Abr. 2008. Brasília, DF: Centro Integrado de Guerra Eletrônica. Disponível em: <http://www.ccomgex.eb.mil.br/cige/sent_colina/6_%20edicao_abril_08/index.htm>. Acesso em: 19 jul. 2015.

WHALEY, Barton. *Stratagem*: deception and surprise in war. Boston: Artech House, 2007. 560 p.

WIKILEAKS. NSA high priority targets for Brazil. *Wikileaks*, [S.l.], 4 jul. 2015. Disponível em: <https://wikileaks.org/nsa-brazil/selectors.html>. Acesso em 18 jul. 2015

WIKILEAKS. About – What is wikileaks. *Wikileaks*, [S.l.], 7 maio 2011. Disponível em: <https://wikileaks.org/About.html>. Acesso em 18 jul. 2015.

FOLHA ONLINE. PF prende um em operação contra uso ilícito de satélites militares americanos. *Folha Online*, São Paulo, 18 mar. 2009. Disponível em: <http://www1.folha.uol.com.br/poder/2009/03/536889-pf-prende-um-em-operacao-contra-uso-ilicito-de-satelites-militares-americanos.shtml>. Acesso em: 18 jul. 2015.

ANEXO A – CICLO OODA

FIGURA 1 – Ciclo OODA.

Fonte: CARDOSO, 2012, p. 45.

ANEXO B – CICLO OODA COMPLETO

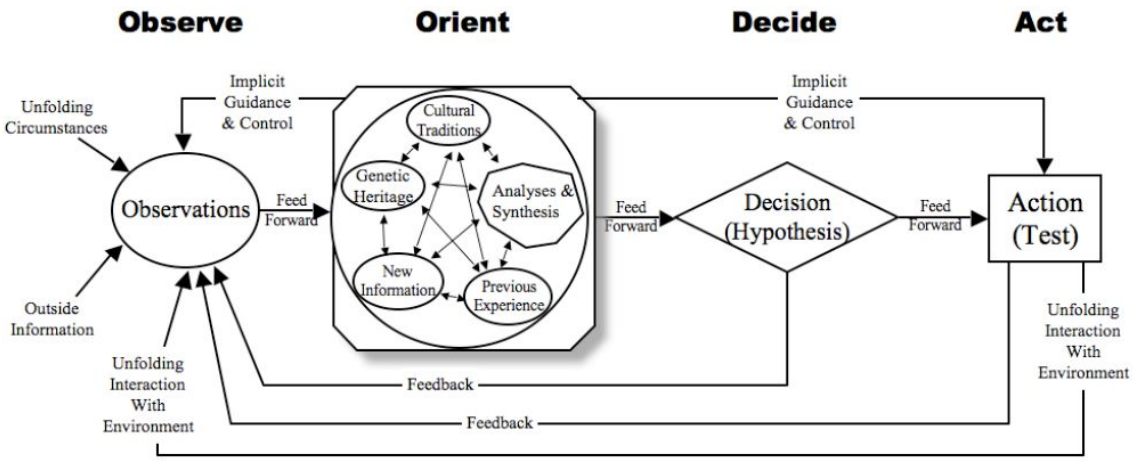

FIGURA 2 – Ciclo OODA Completo.

Fonte: TREMBLAY JR, 2015, p. 7.

ANEXO C – PRINCÍPIO DE FUNCIONAMENTO DE UM SISTEMA SATÉLITE

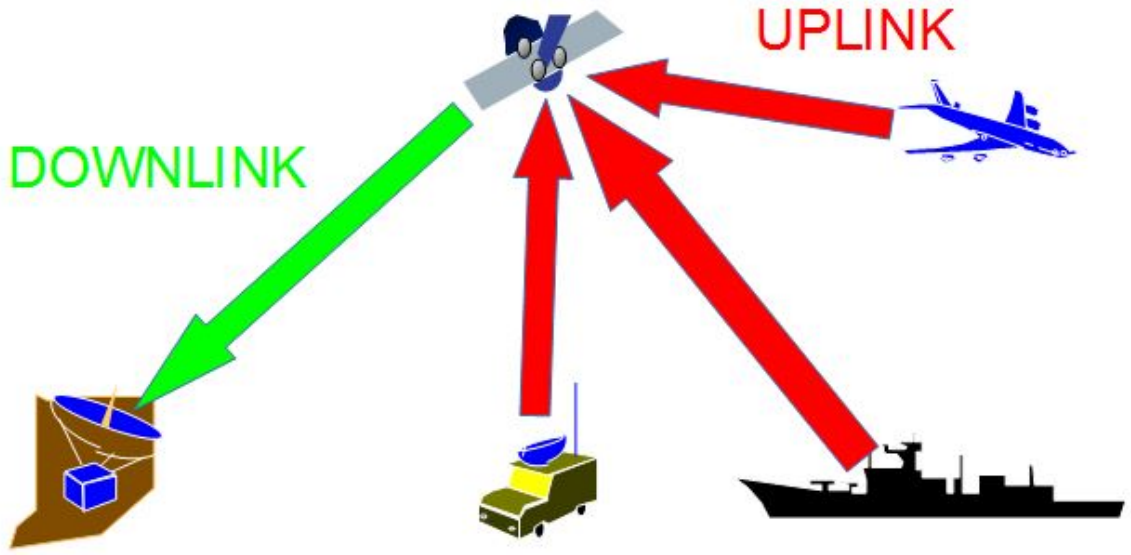

FIGURA 3 - Enlace do usuário para estação terrena.

Navio que deseja se comunicar, fará o enlace com o satélite que retransmitirá para uma estação terrena de controle.

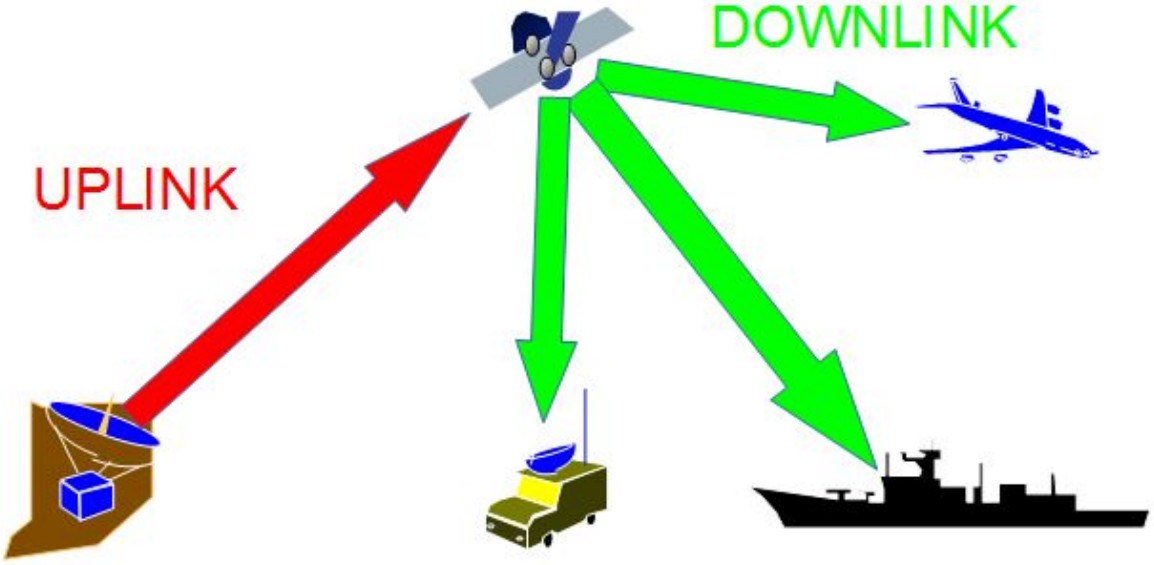

FIGURA 4 - Enlace da estação terrena para o usuário.

A estação terrena de controle retransmitirá a mensagem ao satélite para seu usuário final.

ANEXO D – ÁREA DE COBERTURA DE ALGUNS SISTEMAS DE COMUNICAÇÃO POR SATÉLITE

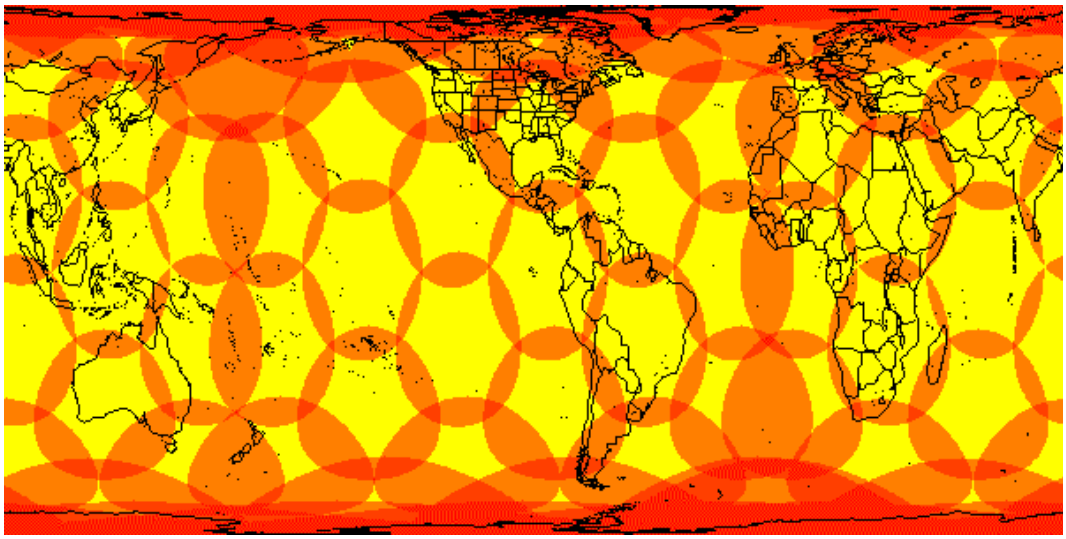

FIGURA 5 – Área de cobertura dos satélites IRIDIUM em determinado momento.

Fonte: EX4U TELECOM, 2015.

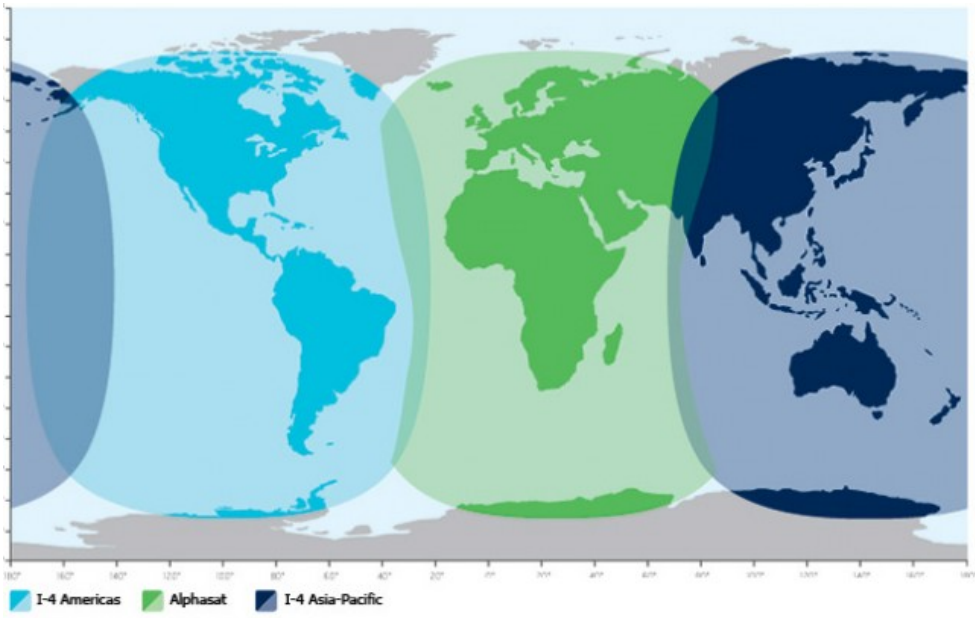

FIGURA 6 – Área de cobertura dos satélites INMARSAT.

Fonte: INMARSAT, 2015.

ANEXO E – PRINCÍPIO DE INTERCEPTAÇÃO DE UM SISTEMA SATÉLITE

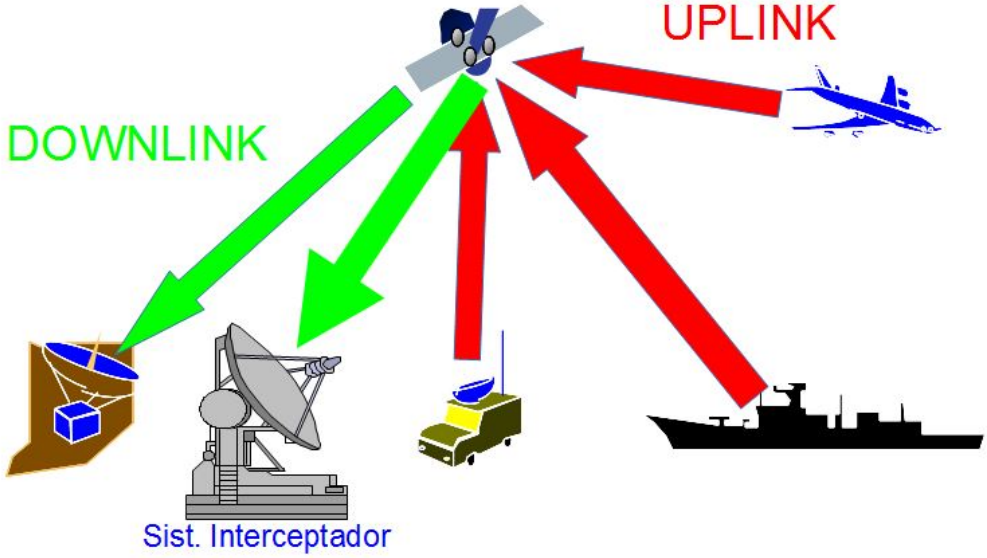

FIGURA 7 – Interceptação do enlace do usuário para estação terrena.

Navio que deseja se comunicar, fará o enlace com o satélite que retransmitirá para uma estação terrena de controle, cujo enlace descendente poderá ser interceptado.

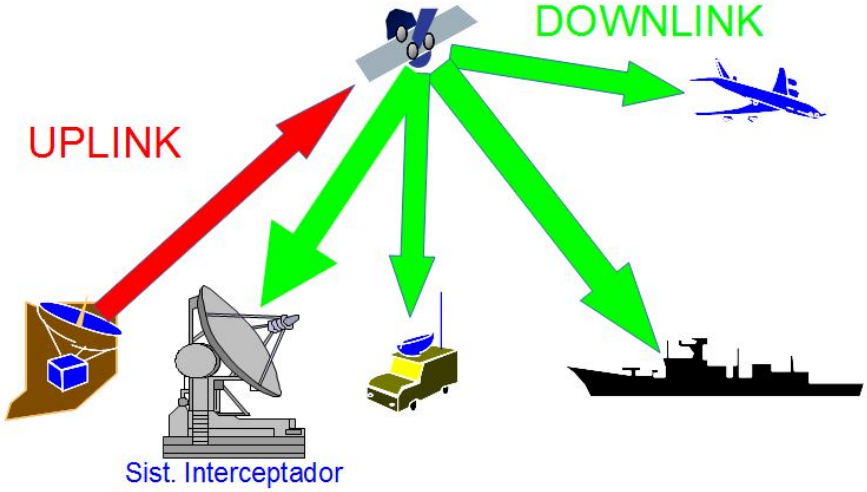

FIGURA 8 – Interceptação do enlace da estação terrena para o usuário.

A estação terrena de controle retransmitirá a mensagem ao satélite para seu usuário final, cujo enlace descendente poderá ser interceptado.