ESCOLA DE APERFEIÇOAMENTO DE OFIÇIAS

CAP COM MOUSSA SENE

A IMPORTÂNCIA DAS MEDIDAS DE PROTEÇÃO ELETRÔNICA NAS OPERAÇÕES OFENSIVAS

Rio de Janeiro

2022

ESCOLA DE APERFEIÇOAMENTO DE OFIÇIAS

Cap COM MOUSSA SENE

A IMPORTÂNCIA DAS MEDIDAS DE PROTEÇÃO ELETRÔNICA NAS OPERAÇÕES OFENSIVAS

Rio de Janeiro

2022

Ficha catalográfica elaborada pelo Bibliotecário Francisco José de Paula Junior CRB7/6686

S475

Sene, Moussa.

A importância das medidas de proteção eletrônica nas operações ofensivas / Moussa Sene – 2022.

36 f. : il.

Trabalho de Conclusão de Curso – Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2022.

Orientação: Cap. Glauco Gonçalves da Silva

1. Medidas de proteção eletrônica. 2. Comunicações. 3. Guerra eletrônica. I Escola de Aperfeiçoamento de Oficiais. II Título.

CDD: 355

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS
(EsAO/1919)

DIVISÃO DE ENSINO E PESQUISA / CURSO DE COMUNICAÇÕES

Ao Cap Com MOUSSA SENE (ONA - SENEGAL)

O Presidente da Comissão de Avaliação do TCC, cujo título é A IMPORTÂNCIA DAS MEDIDAS DE PROTEÇÃO ELETRÔNICA NAS OPERAÇÕES OFENSIVAS, informa à Vossa Senhoria o seguinte resultado da deliberação: **APROVADO** com o conceito **REGULAR**.

Rio de Janeiro, 20 de setembro de 2022

CARLOS ANDRE DOS SANTOS MEIRELLES DE ANDRADE - Maj
Presidente

GLAUCO GONÇALVES DA SILVA - Cap
1º Membro

WAGNER DE FARIAS FIGUEIREDO - Cap
2º Membro

CIENTE:
MOUSSA SENE - Cap
Postulante

AGRADECIMENTOS

Graças ao major, que com muita paciência compreendeu nosso estado de oficial das nações amigas e fez de tudo para nos orientar pouco a pouco na compreensão dos cursos e da doutrina brasileira. Gostaría também de expressar nossos mais calorosos agradecimentos a todos os instrutores pela riqueza de conhecimento que nos deram durante os diferentes módulos. Saímos desses cursos com um valor agregado ao nosso conhecimento das táticas militares; agradecer ao meu padrinho que sempre foi um pilar para minha integração no Brasil e também a todos os camaradas da turma 2022 da curso da comunicação.

RESUMO

A articulação das condições que permitem assegurar a convergência de esforços com vista à execução de um plano de manobra essencial ao exercício do comando. Em cada nível, o líder é responsável por estabelecer a ligação com seus subordinados diretos, com as unidades que apoia, com as unidades vizinhas, no âmbito das ordens da autoridade superior. Os meios necessários para o comandante exercer o seu comando são articulados em um ou mais PCs. Essa articulação resulta de considerações funcionais e de segurança. Esses Posto do comando devem estar localizados no campo em locais que permitam estabelecer as ligações nas melhores condições e, em particular, que o funcionamento das relações técnicas seja assegurado de forma satisfatória ao longo da missão. No que nos diz respeito, as missões ofensivas, o envolvimento de várias forças e o seu domínio móvel tornam-se mais um constrangimento para a permanência dos ligações, na medida em que o desenvolvimento de técnicas de guerra electrónica reduz consideravelmente a nossa capacidade de proteção dos ligações. Conhecer as medidas de proteção também pode garantir o sucesso no planejamento da manobra do escalão superior. Especialmente no contexto de uma missão ofensiva, todas as forças de manobra devem estar permanentemente em contato desde o início da operação até o fim.

ABSTRACT

A segurança das comunicações está se tornando cada vez mais sensível devido às inúmeras ameaças. Eles são difusos e muito multifacetados e podem atuar sobre o material e em diferentes níveis. No campo, a Guerra Eletrônica pode ser uma contribuição muito decisiva para a batalha, especialmente para missões ofensivas, onde, graças à descoberta da direção, pode-se descobrir todo o sistema de armas do inimigo, sua organização tática e seu sistema de comunicação. Entretanto, todo um processo de proteção está disponível para que os amigazes possam garantir uma segurança mais ou menos confiável. Diz respeito ao pessoal e ao material. Para o pessoal, um treinamento prévio para prepará-los é muito importante a fim de minimizar os riscos de ataques e a proteção do material. Finalmente, uma adaptação material é muito importante, na medida em que a mutação das novas tecnologias é cada vez mais fulgurante e muito acentuada.

Palavras chaves : Segurança, Proteção, Adaptação

ABSTRACT

Communications security is becoming increasingly sensitive due to the numerous threats. They are diffuse and very multifaceted and can act on material and on different levels. In the field, Electronic Warfare can be a very decisive contribution to the battle, especially for offensive missions, where, thanks to direction finding, one can discover the enemy's entire weapon system, its tactical organisation and its communication system. Meanwhile, a whole process of protection is available so that the friendlies can guarantee a more or less reliable security. It concerns personnel and material. For the personnel, a previous training to prepare them is very important in order to minimize the risks of attacks and the protection of the material. Finally, a material adaptation is very important, insofar as the mutation of new technologies is more and more striking and very accentuated**.**

Keys words : Security, Protection, Adaptation

SUMÁRIO

1. INTRODUÇÃO

A primeira revolução no domínio da comunicação nos campos de batalha passou pelos meios de transmissão que se tornaram com a descoberta das ondas eletromagnéticas um meio essencial até hoje. Assim, em geral, os enlaces radioelétricos têm atendido a diversas necessidades de coordenação tanto no domínio civil quanto no militar. Sua maestria e controle são muito cruciais no resultado da luta.

Em 8 de junho de 1967, durante a terceira guerra entre árabes e israelenses, Israel atacou o USS Liberty, porque pensava que era um navio inimigo. De fato, poucos dias antes do início da guerra, o USS Liberty recebeu a ordem de realizar uma coleta de inteligência eletrônica no Mar Mediterrâneo, próximo à costa norte da Península do Sinai, localizada entre o Egito e Israel. Devido a uma falha nas ligações de rádio, o navio americano não recebeu ordens de Israel pedindo-lhes que se afastassem da costa egípcia onde os combates estavam ocorrendo. As ordens são recebidas várias horas após o ataque. (Pierre Hazan, *1967, la guerre des six jours : la victoire empoisonnée*, Éditions Complexe, 2001)

Além disso, no campo civil, um dos maiores desastres no campo da aviação civil é resultado da má transmissão de autorizações e informações importantes para a segurança do tráfego aéreo. Em 27 de março de 1977, dois Boeing 747 colidiram em Tenerife, no aeroporto de Los Rodes, por causa de uma camada de neblina que impedia a propagação das ondas e causava centenas de mortes. (Le secret des boîtes noires, enregistrements avant le crash, Jean Pierre Otelli, Editions Altipresse, 2005.)

No campo militar que nos interessa, a sua utilidade no campo de batalha permanece inegavelmente uma condição sine qua non para o processo decisório do comandante conjunto. Assim como durante as manobras ofensivas e defensivas, a coordenação entre fogo e manobra na zona de ação exige um sistema de comunicação rústico e flexível, garantindo a segurança das comunicações.

Certamente, ela continua sendo a dobradiça dos sistemas de comunicaçães em todos os exércitos, na medida em que sua ausência é sinônimo de uma batalha

perdida. No entanto, eles apresentam alguns inconvenientes cada vez mais degradantes para as unidades com o avanço da Guerra Eletrônica.

A manobra ofensiva que envolve a aquisição de um ponto ou de uma determinada área é ainda mais complicada como manobra porque envolve um

equilíbrio de poder amplamente favorável para as unidades amigas com o objetivo de trazer o inimigo em suas últimas trincheiras. Requer uma coordenação conjunta muito alta, boa gestão de inteligência e domínio do equipamento de rádio.

1.1. PROBLEMA

Os meios de comunicação implantados com vistas a satisfazer as necessidades de ligação de um escalão de comando constituem o sistema de comunicação desse escalão para uma missão bem definida. A organização destes últimos no terreno assenta na implementação de um conjunto de meios de extremidades cuja coordenação é assegurada, a nível técnico, pelo comandante de sinais ao mais alto nível. Além disso, um estudo cuidadoso os desvantagens dos meios deve ser realizado para garantir maior segurança das transmissões.

Assim, levar em conta a situação tática no desenvolvimento do sistema das comunicações é uma pedra angular na otimização dos links de rádio.

1.1.1 Antecedentes do Problema

O problema é principalmente técnico porque várias operações resultaram em muitas perdas devido à falta de comunicação. Ou não cumprimento das medidas de proteção eletrônica.

1.1.2 Formulação do Problema

A delicadeza dos meios de comunicação é tanto mais complexa quanto não pode ser completamente definida. Porque ele usa principalmente ondas eletromagnéticas. No entanto, há uma parte da responsabilidade humana que merece ser abordada neste tema de análise.

1.2. OBJETIVOS

1.2.1 Objetivo geral

O objetivo geral é mostrar a importância dos ligações de rádio nas manobras ofensivas de um exército. Ao destacar indiretamente suas desvantagens e suas vantagens para as forças amigas. Isso pode permitir que o comandante do sinal tenha uma melhor compreensão dessa ferramenta, que é útil e indiscreta para uma manobra ofensiva. Requer uma boa proteção das comunicações táticas e técnicas Obviamente, sem qualquer pretensão de escrever um manual de comunicação, esta pesquisa visa fazer um estudo analítico do uso tático das medidas de proteção radioelétricos durante uma manobra ofensiva.

1.2.2 Objetivos específicos

a) Apresentar as manobras como um todo
b) Apresentar a particularidade da manobra ofensiva.
c) Destacar os requisitos de ligação do comandante para uma manobra ofensiva.
d) Apresentar o meio de transmissão.
e) apresentar a possibilidade de ataque eletrônico pelo inimigo.
f) apresentar finalmente os meios de proteção eletrônica

1.3 QUESTOES DE ESTUDO

Quais são as particularidades de uma manobra ofensiva?

Quais são os meios de comunicação em uma manobra ofensiva?

Quais são os métodos do inimigo que podem afetar nossas comunicações?

Quais são as medidas de proteção eletrônica?

1.4 JUSTIFICATIVAS

A flexibilidade das relações radioelétricas constitui um ponto de ancoragem para o comando. Eles têm a facilidade de estabelecer a interoperabilidade entre as diferentes unidades e muitas vezes podem ser mantidos durante o movimento.

No entanto, o uso de enlaces radioelétricos em uma manobra ofensiva é muito delicado, na maioria das vezes requer a implementação de vários meios em um terreno de manobra relativamente contíguo.

Além disso, a evolução da manobra com as diferentes fases de execução exige flexibilidade para reagir com facilidade e com profissionalismo para garantir o sucesso das ações do comando.

2. REVISAO DE LITERATURA

2.1 CARACTERISTICAS DAS OPERAÇÕES OFENSIVAS

As operações ofensivas são muito complexas tanto em sua conduta quanto em seu planejamento devido às numerosas medidas de coordenação que devem ser tomadas a montante e a jusante. O objetivo deles é :

a) destruir forças inimigas;

b) conquistar áreas ou pontos importantes do terreno que permitam a obtenção de vantagens para futuras operações;

c) obter informações sobre o inimigo, particularmente sobre a situação e o poder de combate;

d) adquirir ou comprovar dados referentes ao terreno e às condições meteorológicas;

e) confundir e distrair a atenção do inimigo sobre o esforço principal, desviando-o para outras áreas;

f) antecipar-se ao inimigo para obter a iniciativa, aproveitando qualquer oportunidade que se apresente, negando-lhe qualquer tipo de vantagem;

g) fixar o inimigo, restringindo-lhe a liberdade de movimento e manobra, mediante diferentes esforços e apoio de fogo, com o objetivo de permitir concentrar o máximo poder de combate sobre ele no ponto selecionado

h) privar o inimigo de recursos essenciais com os quais sustente suas ações, realizando atividades e operações em profundidade; e

i) desorganizar o inimigo mediante ataques sobre meios e/ou instalações essenciais para geração e emprego do seu poder de combate.

O sucesso desta missão deve atender a uma série de fundamentos que sejam capazes de garantir o máximo sucesso.

2.1.1 Fundamentos das operações ofensivas:

a) manutenção do contato;

b) esclarecimento da situação;

c) exploração das vulnerabilidades do inimigo;

d) controle dos acidentes capitais do terreno

e) iniciativa e segurança;

f)neutralização da capacidade de reação do inimigo;

g)fogo e movimento;

h) impulsão

i) concentração do poder de combate

j)aproveitamento do êxito;

O planejamento de uma missão ofensiva deve, antes de tudo, cuidar desses fundamentos para o sucesso da missão. Esta é a razão pela qual as medidas de coordenação devem estar nas condições ideais para permitir a tomada de decisões atempadamente e assegurar a sua execução (*Ministere de exercito brasilleiro , commando de operações terrestres, manual de campanha operações ofensivas e defensivas, EB70-MC-10.202, 1ère Edition 2017 p. 3-2 – 3-1)*.

2.2 O APOIO DE COMUNICAÇÕES ÀS OPERAÇÕES OFENSIVAS

Na doctrina do Senegal, o uso das comunicações está exclusivamente sob a reserva do comandante conjunto, que determina suas necessidades de ligação. Assim o oficial de comunicações que, a partir da manobra ofensiva, planeja sua missão. No entanto, o cumprimento desta missão de comunicação pressupõe:

1) a existência prévia de condições essenciais como sentimentos e objetivos comuns, conhecimento aprofundado das possibilidades e modo de ação das diversas forças envolvidas e unidade da doutrina;

2) estabelecer relacionamentos adequados para o encaminhamento de pedidos, solicitações, relatórios e informações;

É responsabilidade da comunicação garantir essas relações essenciais e é sua missão essencial satisfazer as necessidades de ligação do líder.

A ligação deve ser assegurada em todas as circunstâncias entre as várias autoridades designadas pelo comando e deve ser feita de forma inteiramente satisfatória.

Qualquer falha no ligação, qualquer falha na operação ou erro nas comunicações podem ter consequências desastrosas. O uso de comunicações é muitas vezes feito usando certos números de meios disponibilizados a nós pelo escalão superior, que vão desde os suportes até os meios finais.

Os meios de comunicações são os meios materiais utilizados para o estabelecimento de diversos ligações remotos necessários ao exercício do comando, relatórios e solicitações. Eles fornecem esses ligações remotos na forma de “conversas e trocas rápidas” de mensagens ou sinais. Incluem também os meios que, para além dos correios, permitem o transporte de baterias. Os meios de transmissão são de tipo muito variado e constituem aplicações de várias técnicas. Alguns são comumente usados e são chamados de MEIOS PRINCIPAIS são eles:

- Transmissões com fio
- ligações de microondas
- transmissões de rádio
- mensageiros.

Outros meios chamados COMPLEMENTARES podem ser utilizados dependendo das circunstâncias, são eles:

- Processos sonoros
- Processos visuais
- Animais vestidos

Não existe um meio único que atenda imediatamente a todas as circunstâncias e necessidades. É por isso que é necessário estudar os diferentes meios de acordo com seu papel na conexão, que é o que faremos neste capítulo.
Os meios de acordo com seu papel na conexão podem ser classificados como suportes o meios finais.

O meio é qualquer meio que permita o transporte remoto, sob qualquer forma, de voz, sinais ou textos (linha telefônica, por exemplo). E os meios finais são aqueles que permitem carregar a fala dos sinais ou textos em suportes.
Entre estes meios distinguimos os meios de exploração, (rádio, fh, etc.)

2.2.1 Suportes

Existem cinco (5) categorias de mídia:

- Suportes com fio
- Despachar cavaleiros e animais treinados
- Feixes Hertzianos
- Aparelhos de rádio

2.2.1.1 Medidas Com Fio

Os circuitos cabeados são feitos com equipamentos de campanha militar ou aproveitando as instalações de infraestrutura de telecomunicações; normalmente infra-estrutura civil possivelmente infra-estrutura militar.

a- os circuitos militares de campanha:

Estes são os cabos frequentemente isolados. Circuitos de fio desencapado em isoladores são às vezes, mas raramente, em conflitos modernos, construídos em escalões de comando significativos.

Os cabos isolantes são de vários tipos: A escolha do tipo de cabo para uma determinada relação depende da distância entre os correspondentes e do volume de tráfego a ser roteado. A colocação de um cabo requer atrasos que variam de acordo com o tipo de cabo, geralmente é realizada apenas durante o dia.

b- circuitos de infraestrutura com fio:

Em circuitos de infraestrutura cabeada, existem:

- circuitos de telecomunicações
- os circuitos das redes particulares
- circuitos militares

Circuitos de fio desencapado em isoladores cujo alcance varia de 100 a 200 Km de amplificação.

Circuitos subterrâneos: em cabo de longa distância que agrupa várias centenas de circuitos e permite estabelecer alcances praticamente ilimitados graças a estações de amplificação estabelecidas permanentemente.

Nos cabos regionais que agrupam algumas dezenas de circuitos e que, não estando geralmente associados a estações de amplificação, não permitem estabelecer comunicações ao longo de algumas dezenas de quilómetros.

Os circuitos de redes particulares são os das redes ferroviárias, eletricidade etc.…

Os circuitos militares são em geral circuitos em cabos subterrâneos e às vezes aéreos para os campos. A utilização de circuitos de infraestrutura é interessante porque facilita o estabelecimento de ligações nas operações, mas os traçados não

são adaptados às necessidades da situação tática. Então; sujeito à segurança, é possível apropriar-se deles

c- condições de uso dos suportes cablados:

Os circuitos subterrâneos são geralmente usados apenas em níveis muito altos. Seus reparos exigem longos prazos e equipes especializadas.

Os circuitos aéreos são muito sensíveis a bombardeios, metralhadoras aéreas, ações de sabotagem.

A construção e manutenção de circuitos cabeados em áreas inseguras são tarefas difíceis para as equipes de proteção para que as equipes técnicas tenham seu melhor desempenho.

2.2.1.2 Comunicações De Rádio Elétrica

Uma relação radioelétrica pode ser estabelecida sem aviso prévio entre dois correspondentes equipados com meios apropriados. Permite alcançar simultaneamente vários correspondentes, agrupados na mesma rede. O relacionamento muitas vezes pode ser mantido enquanto estiver em movimento.

2.2.1.3 Feixes De Rádio

Um feixe de rádio permite criar, em ondas direccionadas muito curtas, um circuito radioeléctrico de excelente qualidade no qual é possível, graças à utilização de dispositivos multicanal (meios de adaptação), encaminhar simultaneamente várias comunicações telefónicas e telegráficas.

O uso de ondas muito curtas requer na maioria das vezes a instalação entre os terminais de uma ou mais estações retransmissoras em pontos geralmente altos, cada relé tendo apenas um papel de repetidor. As vigas hertzianas funcionam em duplex. Uma cadeia terrestre é geralmente composta por duas estações terminais e possivelmente um ou mais relés.

Em cada seção a relação radioelétrica bilateral é assegurada com duas frequências diferentes não interferindo entre si as ondas são concentradas em um feixe mais ou menos largo por meio de antenas de radiação direcional. É feita uma

distinção entre: - ligações de microondas na frente com baixa capacidade (4 canais) em ondas métricas

- cortar franqueadores
- ligação de rádio de média capacidade (4 a 48 canais) em ondas decimétricas ou centimétricas
- ligação de rádio de alta capacidade para o exército. Em ondas decimétricas ou centimétricas.

Os cabos Hertzianos têm a vantagem de sua velocidade de instalação que depende do número de repedidor e da facilidade de acesso aos pontos altos do solo e sua invulnerabilidade.

Por outro lado, estão expostos a incidentes técnicos operacionais e muitas vezes exigem a instalação de unidades de proteção para seus relés e são difíceis de camuflar. ligaçoes diretos são geralmente usados para ligação de unidades pequenas, ligações diretos e links laterais.

As pontes de corte permitem substituir uma seção de zona relativamente curta ocupada pelo Inimigo. Os enlaces de microondas de média capacidade são usados para enlaces de escalão intermediário: brigada e escalão superior as estações são móveis: os enlaces de média e/ou longa distância são alcançados através deles; O uso de relés é comum. Os links de rádio de alta capacidade do exército são usados para os ligações dos altos escalões, braço, grupo do exército, geralmente são instalados em estações fixas.

2.2.1.4 Mensageiros

O mensageiros continua sendo um meio essencial de transmissão, apesar do andamento dos processos e radioelétricos. É capaz de veicular dobras e documentos volumosos - seu uso muitas vezes é necessário para o encaminhamento da mensagem; Este é particularmente o caso.

2.2.1.5 Animais Treinados

O pombo-correio, um agente de transmissão relativamente fácil de usar, permite a transmissão de texto de todos os tipos. Constitui um meio normalmente

unilateral, utilizável apenas durante o dia, requer retransmissão desde o pombal e não oferece qualquer garantia de segurança, podendo ser entregue aos utilizadores por pára-quedas.

As oportunidades de trabalho são limitadas porque você precisa:

-reabastecer a cada dois ou três dias as unidades detentoras de pombos, pois estes devem ser soltos e regressar ao pombal de origem no final deste período.

-Permitir um período de uma semana antes de qualquer reutilização de pombos de um pombal cada vez que ele se mover.

-Pombos raramente são usados fora de situações estáticas

-O cão pode ser útil em certas circunstâncias, nos níveis mais baixos, desde que você tenha animais muito bem treinados.

2.2.2 Os Meios De Extremidade - Meios De Exploração

Os meios de transmissão final são utilizados na forma de conversas, ou para o encaminhamento de mensagens ou documentos.

A mensagem permite manter um registro escrito das comunicações. Pode ser organizado de forma a tornar-se incompreensível para os serviços de interceptação por um período de tempo que não permite o contato direto entre os correspondentes e os prazos de entrega podem ser variáveis.

-As mensagens podem ser transmitidas:

-Na telefonia

-Telegrafia em código Morse

-Por tipo de dispositivo de telégrafo, teleimpressora

-Por mensageiros (para suporte de memória).

2.2.2.1 Utilização de meios de extremidade para transmissão de documentos

A aparência de transmissores de imagem ou FAC SIMILE permite a transmissão fiel de documentos de mensagens atuais, os chefes podem adicionar esboços e mapas. Este meio de entrega que atualmente está reservado para níveis bastante elevados; de comandos provavelmente será estendido para unidades avançadas. O documento também é transmitido por despachantes.

2.2.2.2 Meios de transmissão de fala

O microfone de rádio: existem duas categorias principais de microfone. O microfone de carbono e o microfone eletrodinâmico. O microfone de carbono mais simples, menos frágil e o mais usado no exército, embora menos fiel ao microfone eletrodinâmico. Geralmente é conectado diretamente ao meio de rádio, mas pode ser conectado através do microcontrole remoto.

O alto-falante: fazendo parte integrante do aparelho ou conectado a ele por meio de um cabo, permite acompanhar as conversas.

O alto-falante pode ser duplicado ou substituído por fones de ouvido (HS30) que isolam o correspondente do ruído externo.

O Telefone: datado do final do século XIX, o telefone permite conversas e respostas imediatas, em uma palavra, cria um contato direto entre os assinantes.

Distingue-se entre: telefones electromagnéticos, telefones com baterias locais e telefones com baterias centrais.

O telefone eletromagnético, sua fonte de alimentação de microfone, é geralmente usado em estações de baixo nível (TS de CE11) e para distâncias muito curtas. Alguns têm sistemas de chamada e atendimento (TA)

Os telefones de bateria, fornecem sua corrente de microfone (baterias) e tem um sistema de chamada (o magneto) Os telefones de campo E.E.8 são frequentemente usados para controle remoto.

Os telefones com bateria local recebem a corrente do microfone através do meio com fio e transmitem as chamadas de uma discagem para a discagem desejada. O controle remoto: o controle remoto é um sistema técnico que permite usar um meio com fio para transmitir e receber longe do meio radioelétrico. O controle remoto pode ser simples (J.B.60 de S.C.R.399 ou R.M.29) ou tornando mais complexa a ação de ligar e desligar o aparelho (c.433 e C434 de AN/GRC-3 a 8) pode ser realizada para a voz de um monofone e a parada do microfone e um fone de ouvido ou telefone.

2.2.2.3 Meios de transmissão de sinal

O Manipulador: utilizado para telegrafia em código Morse, e composto por dois contatos abertos que estão no ritmo da manipulação, são conectados

diretamente à estação radioelétrica ou através de um sistema de controle remoto. Certos manipuladores mais sofisticados chamados vibradores permitem uma manipulação rápida.

O Telégrafo: pode ser usado e composto por um manipulador e um sistema de criação de som utilizável (TG5). É mais frequentemente conectado ao seu suporte com fio por apropriação.

Teleimpressoras: existem duas categorias principais de teleimpressoras, teleimpressoras start-stop que podem ser conectadas diretamente a suportes com fio, teleimpressoras de frequência de voz (ou teleimpressoras de rádio) podem ser conectadas a suportes com fio ou radioelétricos.

- os teleimpressores start-stop ainda são os mais difundidos, usam um código de cinco momentos e permitem velocidades de telégrafo de 60 a 100 palavras por minuto. Os mais usados são o TG- (teclado americano) o Olivetti (teclado europeu).

- Teleimpressoras de frequência de voz permitem conexão direta a um canal telefônico ou diretamente a um canal de rádio.

Alguns desordenam todo o caminho do telefone e podem ser comutados por uma central telefônica normal, outros podem ser transpostos diretamente acima do caminho do telefone.Eles geralmente permitem alcances de rádio maiores do que os de voz

Sinais ópticos ou visuais: Os sinais ópticos são obtidos de objetos ou materiais visíveis de um observatório ou aeronave. São eles: sinais elétricos: lâmpadas marinhas- holofotes- INFRA-VERMELHOS etc.…Foguetes e bombas de fumaça sinais de trânsito e estacas. Cada vez menos utilizados, ainda são utilizados pela marinha e para ligações ar-terra.

Os sinais sonoros: apitos – buzinas, são utilizados apenas pelos escalões inferiores e permitem apenas a transmissão próxima de sinais convencionais planejados com antecedência. Permanecem no excelente meio de disparo de alertas. Especialmente durante uma missão de junção entre duas unidades amigas.

2.2.2.4 Meios de transmissão de documentos

Além dos correios, os documentos podem ser transmitidos por transmissores de imagem ou FAC-SIMILE que retransmitem com fidelidade, qualquer que seja o texto ou os esboços escritos em uma folha.

A telegrafia por fac-símile pode ser realizada usando dois procedimentos principais que são: a telefonografia e a impressão direta, a telefotografia permite uma reprodução mais fiel por uma grande sutileza de exploração, uma melhor reprodução de cores mas em trabalho de materiais. A impressão direta mais fácil e simples de implementar, por outro lado, oferece uma qualidade de imagem inferior. Os materiais de fac-símile, cuja técnica melhora a cada dia, agora podem ser usados corretamente com suportes com fio ou radioelétricos.

2.2.2.5 Meios de extremidade - meios de adaptação

Os meios terminais de adaptação são aqueles que permitem ligar ou transpor meios operacionais em suportes que tecnicamente nã o têm a possibilidade de os receber directamente. Possibilitam a troca de conversações também podem ser usados teletipos de voz com frequência.

2.3 OS EFEITOS DA GUERRA ELETRONICA INIMIGA SOBRE AS OPERAÇÕES OFENSIVAS

Em tempo de paz ou não, a guerra de computadores permite sabotar os sistemas informatizados de infraestruturas estratégicas (civis e militares), realizar ações de espionagem (para fins militares e econômicos) por intrusão nos sistemas.

Suas principais armas são: vírus (pequenos programas que contaminam o funcionamento das redes); worms (vírus que se reproduzem e circulam na rede para contaminar gradualmente outros computadores e programas, até ocupar todo o espaço da memória e paralisá-la); escotilhas (sistema instalado secretamente pelo projetista que permite a entrada contornando as proteções); “Cavalos de Tróia” (programas escondidos dentro de outro programa capaz de destruir o conteúdo de um computador); “bombas lógicas” (programas que injetam vírus e worms em um sistema, que podem ser ativados remotamente ou que são acionados quando

determinados programas ou determinados comandos são implementados, agindo assim como detonadores); canhões de microondas (o pulso de rádio que interrompe componentes eletrônicos); ondas eletromagnéticas - são armas de "microondas" transportadas em uma máquina (ou logo transportadas no campo de batalha por um soldado de infantaria) que geram um pulso de duração muito curta e potência muito alta capaz de paralisar tudo ou parte de um sistema eletrônico, seja ele os controles de um avião, um tanque, um navio ou o "disparo" de mísseis e outros sistemas de armas.

Durante as operações ofensivas, o elemento surpresa, que é essencial, pode ser comprometido pelas ações da guerra eletrônica do inimigo sobre nossas armas e nossos meios de comunicação.

A guerra eletrônica é o conjunto de medidas tomadas pelos beligerantes para tentar garantir a superioridade no uso da radiação eletrônica. Estende-se a todos os aspectos de seu uso, comunicações propriamente ditas, navegação, radar, sistema de orientação e controle, etc.

2.3.1 ATAQUE ÀS COMUNICAÇÕES DO INIMIGO.

Atacar alvos de sinais inimigos: perturbar nossas relações radioelétricas nos campos de batalha interceptar nossos meios de comunicação para obter informações técnicas e táticas, interrupção de comunicações amigáveis
abordado :

O ataque às instalações, uma missão incumbida em todos os níveis em todas as circunstâncias para aniquilar nossa missão.

A intrusão que consiste em o inimigo introduzir uma estação em nossa rede elétrica e tanto tentar obter informações, podendo comprometer o andamento de nossa missão enviando-nos informações errôneas. Pode ser executado em qualquer nível de comando.

Interceptação de comunicações
consiste em:

• Capture nosso tráfego tocando.
• localizar nossos aparelhos de rádio por localização de direção.

2.3.2 O INTRUSO

Classificação definida como "a introdução de sinais ou mensagens nas vias de transmissão dos elementos de manobra, com a intenção de enganar". A intrusão permite ainda:

- Obter informações
- Para interromper ou proibir o funcionamento normal dos sistemas.

No entanto, a proteção contra esses aspectos de intrusão é da conta de todos, porque você deve saber que:

- Cada vez mais armas, transmissões ou sistemas de comando dependem de eletrônicos e computadores, sua neutralização pode ser obtida acionando uma operação errática de automação e/ou computadores
- A intrusão em sistemas informatizados é particularmente perigosa; ele envolve não apenas o presente, mas também o passado, permitindo o acesso às memórias e ao futuro, alterando o software.

2.3.3 INTERFERÊNCIA

Bloquear os receptores dos nossos sistemas consiste em sobrepor um sinal parasita indesejável às radiações que normalmente lhe são destinadas.

Essa interferência pode ser:

- Pontual quando se aplica a uma frequência sem perturbar as frequências vizinhas.

Amortecimento quando se aplica simultaneamente a todas as frequências de uma dada banda relativamente ampla. Sequencial quando se aplica seletiva e simultaneamente a várias frequências de uma dada banda. Além de seus efeitos clássicos de neutralização temporária das redes de transmissão, esse bloqueio pode possibilitar a obtenção de : O funcionamento errático de sistemas de transmissão informatizados, em particular quando as ordens de reconfiguração do sistema são roteadas neste mesmo sistema.

2.3.4 L’IMPULSION ELECTROMAGNETIQUE

Recém-chegado à panóplia de meios de neutralização ou destruição de sistemas eletrônicos, o Pulso Eletromagnético (EMP) tem um efeito brutal e massivo. Uma explosão nuclear em altitude muito elevada provoca o aparecimento de uma onda muito curta (400 ns) e muito energética (5 megawatts/m2) ao longo de milhares de km2

Induzida nos circuitos e componentes, a EMI que resulta desta onda pode causar:

- A destruição do nosso equipamento
- Funcionamento errático dos nossos sistemas.

Os ataques eletrônicos do inimigo atrapalham na maioria dos casos o andamento da manobra amiga e nos obrigam a ser resilientes alterando boa parte do planejamento ou simplesmente entendendo toda a manobra. No entanto, existem formas e medidas que podem proteger as ligações amigáveis. Essas medidas são tomadas em todos os níveis de comando.

2.4 MEDIDAS DE PROTEÇÃO ELETRÔNICA

Sem comunicações torna-se impossível realizar uma operação bem sucedida, mas também sem segurança mínima, o comprometimento da missão é registrado automaticamente antes do início da missão. Manobras ofensivas envolvendo várias tropas requerem perfeita coordenação e proteção dos meios de comunicação amigos. Nesse capítulo veremos as diferentes medidas a tomar e os meios utilizáveis susceptíveis de garantir a proteção e também conduzir uma guerra eléctrica ao nosso nível.

2.4.1 Segurança de comunicação

Na doutrina do Senegal, a proteção das comunicações é muitas vezes conseguida através de medidas preventivas

- Proteger o tráfego contra interceptação e análise
- Garantir os meios contra itrusão, obstrução e destruição.

Essas medidas tendem a garantir a segurança operacional.

A segurança da transmissão diz respeito não apenas às redes de rádio que erroneamente se acredita serem as únicas partes responsáveis por ações de guerra eletrônica, mas também a todas as outras emissões: HF, radar, sistema de orientação, transmissões de dados, etc.

A segurança das comunicações deve ser assegurada de forma contínua, tanto em tempos de paz como em tempos de guerra, porque a ameaça é permanente. Apenas as formas de ataque diferem.

Em tempo de paz: sendo improvável a destruição e o congestionamento, a proteção do tráfego continua a ser a grande preocupação, sem esquecer ou subestimar os riscos sempre reais de intrusão.

Em tempos de guerra: aos riscos acima, devemos acrescentar os de neutralização eletrônica ou física que, ao desorganizar o comando; impossibilitar seu exercício.

Se a segurança da encriptação ou a proteção das instalações técnicas continua a ser, em grande parte, da responsabilidade dos especialistas, a segurança das transmissões é da responsabilidade de todos os utilizadores dos meios de transmissão.

2.4.2 Proteção contra tráfego, interceptação e análise

Os correspondentes de uma rede de transmissão estão ligados em um determinado momento por um relacionamento. Essa relação pode ser:

- Radioelétrica
- Estruturas de arame
- Ligações de rádio
- Composto

Em caso de heterogeneidade, é o elo mais fraco que deve ser levado em consideração para avaliar a segurança do relacionamento.

O nível de aprovação e o grau de segurança têm a mesma finalidade, mas:

- Em um relacionamento aprovado, a informação circula de forma clara
- Numa ligação com encriptação de canal ou junção, portanto caracterizada por um grau de segurança, a informação circula encriptada.

2.4.3 Aprovação de relacionamentos

Um relacionamento é aprovado quando as informações classificadas podem circular lá de forma clara. Dada a vulnerabilidade dos meios, apenas os relacionamentos com fio podem, sob certas condições, ser aprovados discretamente.

2.4.3.1 Condições de aprovação

Qualquer proposta de aprovação de relações deve ser precedida de visita técnica do responsável pela segurança das comunicações.
Durante esta visita, este oficial avalia:

- Proteção contra interceptação: um circuito cabeado aprovado deve funcionar em uma área supervisionada com acesso controlado.
- O nível de autorização do pessoal operacional ou técnico que deve ser pelo menos igual à aprovação.
- A qualidade das instalações.
- Condições de funcionamento. Qualquer envio inadvertido de informações classificadas por circuitos não aprovados deve ser evitado.

No entanto, em caso de ocorrência de eventos graves ou em operações em que a urgência prevaleça sobre a segurança ou quando se estima que a vida útil da informação seja inferior aos tempos de funcionamento dos serviços de escuta adversa, a informação classificada pode ser encaminhada de forma clara nas referidas relações . Esta decisão é da exclusiva responsabilidade do comandante do escalão em questão.

2.4.3.2 Transmissão de informações classificadas sobre relacionamentos não aprovados

Quando for tomada a decisão de encaminhar informações sigilosas da Defesa (C.D) confidenciais sobre um relacionamento não aprovado, as seguintes medidas devem ser aplicadas:

A classificação da informação nunca deve ser transmitida, é substituída pela palavra "claro". Qualquer referência a informações previamente criptografadas é proibida.

Após o recebimento, a mensagem é marcada com as palavras “clear recibo”. tal mensagem é tratada como um C.D. A remarcação editorial é obrigatória ao usar o procedimento “claro” O encaminhamento sob tais condições de informações Secretas – Defesa (S.D) somente é autorizado em caso de engajamento de operações
reais quando se tratar de informações táticas consideradas obsoletas no decorrer do engajamento.

2.4.3.3 Transmissão de Informações Não Protegidas sobre Relacionamentos Não Aprovados

O roteamento de informações desprotegidas sobre relacionamentos não confiáveis é a solução normal. No entanto, os redatores de mensagens e os usuários dos meios de transmissão devem procurar minimizar esse tráfego por todos os meios, pois:

- Os tempos de transmissão são tanto maiores quanto o tráfego é alto
- É provável que o tráfego claro seja analisado muito rapidamente pelos centros de escuta opostos.
- Como corolário, a soma de informações desprotegidas pode constituir informação sensível: efeito de acumulação.

2.4.4 Medidas a serem aplicadas pelos operadores e usuários

Os usuários e operadores dos meios de transmissão são os responsáveis finais pela aplicação das medidas de segurança operacional; como tal devem:

-Respeite os procedimentos e regras de operação das transmissões:

-Use meios regulatórios de camuflagem

-Use procedimentos de autenticação com frequência e sabedoria

-Reduzir o tempo de transmissão

-Preparar comunicações

-Use formatos de mensagem

-Excluir conversa

-Reduzir lixo nocivo

-Escolha o local de emissão

-Use a antena mais adequada

-Limite a potência dos transmissores

-Responder a interferências

-Não use o rádio se existirem outros meios de comunicação.

2.4.5 Proteção contra intrusão, obstrução e destruição

2.4.5.1 Meios de proteção contra intrusão

- Os meios de proteção contra intrusão são:

cumprimento rigoroso dos procedimentos de rede e disciplina por parte dos operadores e utilizadores, pelo que devem ser instruídos e motivados.

A limitação das trocas é clara: o uso de cifras e camuflagem obriga o correspondente a responder usando o mesmo sistema. o intruso ignorante das chaves não pode fazê-lo, a menos que capture um material ou um documento de serviço.

- O uso de autenticação
- A autenticação pode ter três aspectos:
- A autenticação de autoridades permite autenticar um programa ou uma mensagem.
- A autenticação de estações permite que os operadores de rede eliminem possíveis intrusos
- A autenticação da função permite assegurar, num sistema automatizado, que o requerente tem o direito de aceder a determinadas aplicações ou informações do sistema (autorização de acesso)

2.4.5.1 Proteção contra interferência

Em primeiro lugar, não devemos depender inteiramente de meios radiantes, mesmo e especialmente nos níveis inferiores.

- Mensageiros
- Agentes de ligação
- Flags, por exemplo, são meios cuja importância não deve ser minimizada.

Se você for objeto de interferência, você deve:

Corrigir, ou seja, localizar o jammer: operação ininterrupta na frequência congestionada mantendo-a ocupada.

Ao mesmo tempo modifique a posição da antena se possível para tentar mascarar o jammer e manter o ligações.

Destruir, ou seja, reportar ao oficial de segurança de comunicações que possivelmente poderá chamar recursos de combate a incêndio após localizar o jammer.

A mudança de frequência deve ser combinada com uma mudança de indicativos e, se possível, de operadores.

2.4.5.2 Proteção de Impulso Eletromagnético

Dois processos que podem ser complementares garantem a sobrevivência dos relacionamentos: O "endurecimento" das instalações que consiste em impedir que a EMI atinja os componentes. o resultado é obtido por faradização e filtragem

Substituição de hardware não endurecido danificado por EMI. o equipamento sobressalente deve então ser armazenado em condições que impeçam a penetração de EMI.

2.4.6 Responsabilidades do controle e Comando

Garantir a segurança das comunicações é uma necessidade absoluta para o chefe em todos os níveis. É a este preço que a informação operacional pode ser garantida.

O líder em todos os níveis deve:

♣ Motivar e treinar suas unidades para manobrar em ambiente de guerra eletrônica.

♣ Definir o regime e os termos de utilização e implementação das suas redes de transporte no quadro das diretivas e regulamentos em vigor.

♣ Controlar a instrução de pessoal e a aplicação de medidas de segurança para comunicações.

2.4.6.1 Função do responsável pela segurança das comunicações (secom)

Em termos de segurança de transmissão, o oficial “SECOM” é responsável por:

• Propor medidas de segurança operacional ao comando

- Circuitos a aprovar ou a aprovar
- Esquemas para o uso de meios radiantes
- Autorização de transmissões excepcionais

• Controlar a instrução do pessoal e a aplicação das regras de segurança

- Comunicar aos usuários ou operadores qualquer violação de segurança das comunicações
- Efectuar escutas telefónicas das redes pelas quais é responsável
- Realizar controle de tráfego diário
- Garantir que as autoridades que enviam mensagens estejam autorizadas a fazê-lo
- Assegurar o cumprimento das medidas de circulação de mensagens classificadas
- Controlar a instrução de operadores e usuários
- Assegurar a aplicação das regras de funcionamento (procedimentos, frequências, códigos, potência, etc.)

• Realizar visitas técnicas.

Isso deve ser feito em relação ao comando e às necessidades táticas que nos impõem uma alta consideração.

As operações ofensivas e suas características intrínsecas exigem coordenação das comunicações e um bom domínio das medidas de proteção eletrônica. Aproveitar ao máximo a ação das unidades de manobra no solo.

2.4.7 Proteção de transmissões amigáveis.

A proteção das transmissões amigas deve ser organizada de modo a tornar tão ineficazes quanto possível os vários métodos de ataque que o inimigo, por seu lado, pode implementar. Esta proteção visa:

• Defesa de instalações.
• proteção contra interferências.
• proteção contra intrusão.
• proteção contra interceptação de tráfego.
• Defesa de instalações.

2.4.7.1 Defesa das instalações

Deve estar previsto nas providências gerais feitas pelo comando para garantir a segurança dentro de sua área de atuação. É facilitado pela camuflagem, que deve ser uma preocupação constante, principalmente em torno dos centros de transmissão.

O pessoal de comunicação, em número estritamente necessário para a implementação técnica dos meios, pode participar desta defesa apenas em caso de crise.

Proteção contra interferência. Esta proteção consiste em procurar limitar os seus efeitos através das seguintes medidas:

• Roteamento de tráfego contínuo apesar do congestionamento, o que exige dos operadores uma formação muito avançada nesta área. Em caso de congestionamento o tráfego passará melhor por radiotelegrafia (radiofonia)
• Alteração da frequência de trabalho, o que requer a alocação de frequências alternativas. Desabilite o jammer, uma ação dentro do comando.
• Proteção contra intrusão.

Essa proteção consiste em assegurar a identidade do correspondente por meio de um procedimento especial denominado “procedimento de autenticação”, que resulta na troca de sinais convencionais estabelecidos segundo um código disponível a todos os operadores de meios de comunicação. Essa autenticação é solicitada sempre que houver dúvida sobre a identidade do correspondente. No entanto, este procedimento, que aumenta os tempos de entrega do tráfego, deve ser utilizado com critério.

Proteção contra interceptação. Nenhum método de comunicação é imune à interceptação. Os grandes serviços de escuta de um exército moderno podem captar praticamente todo o tráfego radioelétrico de um teatro de operações, inclusive transmissões de ondas curtas cujos fenômenos de propagação anômala à distância são frequentes. Estas transmissões podem, em qualquer caso, ser captadas pelos adeptos locais. Cabos de rádio e transmissões com fio também não são imunes à espionagem do inimigo.

No que diz respeito às comunicações telefónicas, os utilizadores não devem perder de vista que qualquer conversa telefónica pode ser captada em vários pontos da relação, mesmo que o circuito utilizado seja constituído por cabos subterrâneos.Essas interceptações podem ser feitas, por exemplo, de centrais telefônicas, despachantes e estações de amplificação.

3. METODOLOGIA

Nosso método de pesquisa é analítico, enfoque como estratégias de utilização de meios de comunicação. Durante uma missão de pesquisa. Será dada ênfase especial aos parâmetros e influências positivas e negativas na continuidade do seu cumprimento das lações técnicas.

3.1 OBJETO FORMAL DO ETUDO

O objetivo deste estudo é mostrar a sensibilidade das medidas de proteção eletrônica durante uma manobra ofensiva. Ela tem a particularidade de ser dinâmica e de solicitar muitos meios radioelétricos. Trata-se de uma manobra ofensiva e o da iniciativa segundo as forças em primeiro lugar e doutrina técnica das comunicações. Em seguida, retorne extensivamente às desavantagens dos meios radioelétricos durante uma manobra ofensiva. Isso requer uma participação de várias forças terrestres e aéreas. Essa concentração de esforço tem como corolário o aumento da necessidade de encaixe e consequentemente dos meios a serem engajados.

3.2 AMOSTRA

Nosso objeto de estudo estuda o envolvimento dos comunicações em uma manobra ofensiva. A ênfase não será colocada em considerações operacionais, mas sim nas características técnicas que podem ser utilizadas para proteger as comunicações de nossa grande unidade contra ataques inimigos. O desenvolvimento dos recursos humanos será um trunfo importante. Na medida em que os meios não são unânimes, é necessário assegurar que o pessoal, o único recurso disponível em todos os níveis de comando, receba o máximo de instrução e preparação técnica para uma determinada operação.

3.3 DELINEAMENTO DE PESQUISA

Iremos prosseguir com um método analítico através de uma síntese tendo em várias especialidades dentro das comunicações em particular e os exércitos em

geral. A sobreposição multidisciplinar nos permitirá ter uma visão sóbria dos fatores que
contribuem para o sucesso da missão, sobre problemas sérios do comunicações no campo de batalha e suas soluções possíveis.

3.3.1 Procedimentos para revisão da literatura

Para uma melhor objetividade e uma análise mais exaustiva do material, exploremos várias vias de informação, combinando webografia e bibliografia sobre manobras ofensivas e
dos comunicações em geral. Assim como nossos manuais do exército que tratam de temas brasileiros próximos ou relacionados em grande assunto.

3.3.2 PROCEDIMENTOS METODOLÓGICOS

Quanto à nossa metodologia de coleta de informações mas na doctrina do Senegal, fé feita em livros que são de combate e transmissores ofensivos e com base principalmente em nosso conhecimento pessoal dos comunicações; bem como um reforço instrutivo graças ao filme ofensivo da Primeira Guerra Mundial e Segunda Guerras, a Normandia.

3.3.3 INSTRUMENTOS

Um certo complexo do tema de reflexão impõe um conhecimento histórico das batalhas para determinar os fatores decisivos dos meios radioelétricos. E também um domínio da manobra qualquer que seja uma doutrina pré-conizada.

3.3.3 ANÁLISE DOS DADOS

Os dados que temos nos dão uma riqueza de informações sobre a complexidade dos meios de comunicações, ainda mais durante uma missão ofensiva. A operação ofensiva é muito particular com seus fundamentos e sua mobilidade o que dificulta um pouco a coordenação da manobra.

Além disso, o regime livre das redes também é outro parâmetro que se soma à panóplia de vulnerabilidades dos meios de comunicação. No entanto, existem medidas aplicáveis a todos os níveis de comando que podem ser um meio muito útil para combater mais ou menos os ataques inimigos.

Começam pelos meios disponibilizados às comunicações e meios imateriais, que nada mais são do que o compromisso do pessoal em respeitar o procedimento e as instruções de segurança da comunicações.

CONCLUSÃO

A sensibilidade das comunicações no campo de batalha é hoje um fato que merece ser levado a sério nos mais altos níveis de comando. É primordial no resultado da batalha; especialmente porque todas as armas e meios de aquisição se tornaram alvos eletrônicos.

Numa missão ofensiva o regime de liberdade favorece a localização do sistema de armamento; além disso, a mobilidade constitui uma vulnerabilidade para as comunicações porque é muito difícil delimitar a propagação das ondas, daí a necessidade de usar Medidas de Proteção Eletrônica para aniquilar todos os ataques inimigos e preservar a discrição da missão.

Os meios do inimigo serão obviamente postos em serviço para aproveitar ao máximo as falhas do nosso sistema de comunicação. Este estudo permitiu-nos exercer a máxima importância das Medidas de Proteção Eletrónica, em geral, durante as missões ofensivas em particular. Com uma instância de investimento humano através de treinamento e discrição, porque mesmo que seja mais ou menos difícil interceptar uma comunicação, deve ser muito complicado invadir a rede ou decifrar o conteúdo das comunicações.

As comunicações são muito essenciais durante uma manobra ofensiva, desde o início até o fim a intervenção dos meios de comunicação é solicitada para permitir que as tropas vizinhas mantenham contato com as unidades de manobra, bem como as unidades de apoio e o escalão superior com seus subordinados.

No entanto, a evolução dos meios resultou em uma digitalização do campo de batalha e causa e efeito, a Guerra Eletrônica tornou-se uma missão. Daí a necessidade de garantir o desenvolvimento e domínio das medidas de proteção eletrônica. A segurança raramente é totalmente garantida durante uma operação, mas a aplicação de medidas em todos os níveis de comando pode reduzir consideravelmente os riscos decorrentes da exploração do espectro eletromagnético pelo inimigo.

Armas e munições são agora apenas parte de um complexa systema, com elementos constantemente ligados entre si, comunicando-se automaticamente e pré-

programados. Cada combatente, cada sistema de armas, cada sistema de informação está suscetível a ser vítima de um ataque eletrônico que pode levar a um longo processo de indisponibilidade.

Nesta pesquisa, a ênfase foi principalmente nas medidas de proteção eletrônica, durante uma missão ofensiva, as implicações táticas não foram muito aprofundadas para não alterar as características técnicas do documento.

As comunicações são técnicas, mas o uso eficiente dos meios de comunicação não poderia ser feito sem levar em conta a manobra das unidades no solo. Essa sutileza implica uma ampla consideração do oficial de comunicações sobre a situação tática e domínio do campo de manobras, a fim de escolher os meios adequados, além das medidas adequadas para proteger as comunicações amistosas.

REFERENCIAS

Bernard marcel, Les étapes de la radiotélégraphie dans l'aviation, Revue radioélectrique t1, n°11, 12, et 13, 1921.

Carlier claude l'emergence des armes nouvelles, Paris, Economica, 1997.

Flichy Patrice, une histoire de la communication moderne espace public et vie privée, Paris, La decouverte, 1991.

Robert Galann, si l'aviation nous etait contee" (encyclopédie de poche de l'aviation) auteur : Editions : privat - isbn : 978-2-7089-9239-9.

Patrick paillot, "Metz, la sentinelle, histoire de la ba 128 - lcl jean dagnaux " auteur : editions : privat - isbn : 978-2-7089-9241-2.

Le secret des boîtes noires, enregistrements avant le crash, Jean Pierre Otelli, Editions Altipresse, 2005.

Ministere de exercito brasilleiro , commando de opéra nnnnnnnnnn terrestre, manual de campanha operações ofensivas e defensivas, EB70-MC-10.202, 1ère Edition 2017.

Ministère de la Défense, Etat-major de l'Armée de Terre, TTA 150, titre 8ème Edition provisoire 2001