EXÉRCITO PORTUGAL
Ao serviço dos Portugueses

PDE 6-00

COMUNICAÇÕES E INFORMAÇÃO

AGOSTO DE 2023

Página intencionalmente em branco

S. R.

MINISTÉRIO DA DEFESA NACIONAL
EXÉRCITO PORTUGUÊS

DESPACHO

1. Aprovo, para utilização no Exército, a PDE 6-00 Comunicações e Informação.
2. A PDE 6-00 Comunicações e Informação é uma publicação classificada como NÃO CLASSIFICADO e não registada.
3. Podem ser feitos extratos desta publicação sem autorização da entidade promulgadora.
4. A PDE 6-00 Comunicações e Informação, entra em vigor a partir da data da sua aprovação.

Lisboa, 21 de agosto de 2023

O CHEFE DO ESTADO-MAIOR DO EXÉRCITO

EDUARDO MANUEL BRAGA DA CRUZ MENDES FERRÃO
GENERAL

Página intencionalmente em branco

REGISTO DE ALTERAÇÕES

IDENTIFICAÇÃO DA ALTERAÇÃO (N.º e Data)	DATA DA INTRODUÇÃO	ENTRADA EM VIGOR (Data)	IDENTIFICAÇÃO DE QUEM INTRODUZIU (Assinatura, Posto e Unidade)

Página intencionalmente em branco

ÍNDICE

ÍNDICE DE FIGURAS E TABELAS

FIGURAS

TABELAS

Página intencionalmente em branco

NOTA PRÉVIA

A implementação de um Exército flexível e moderno, sustentado, com capacidade expedicionária e pronto a atuar em todo o Espectro de Operações, baseado em padrões de excelência e com uma presença cada vez mais efetiva junto da sociedade, trabalhando em prol de Portugal e dos portugueses, requer uma melhoria contínua ao nível dos procedimentos e interoperabilidade e na busca permanente pela eficiência.

A PDE 6-00 Comunicações e Informação (CI) tem como finalidade estabelecer os conceitos gerais, os princípios e as definições que regulam a doutrina CI, quer no nível operacional quer no nível tático.

Esta publicação aplica-se à Capacidade de Comando e Controlo, em vigor no Exército Português, tendo sido adaptada a partir do modelo de abordagem aos Sistemas de Informação e Comunicações da Organização do Tratado do Atlântico Norte (OTAN). Utiliza, tanto quanto possível, abreviaturas, acrónimos e glossário de termos da OTAN para assegurar a interoperabilidade no âmbito CI e em simultâneo facilitar a integração de militares e Forças do Exército nos Quartéis-Generais e Teatros de Operações da Aliança.

A PDE 6-00 Comunicações e Informação encontra-se estruturada em cinco Capítulos, onde são tratadas as matérias relacionadas com as Comunicações, os Sistemas de Informação, a Gestão da Informação e do Conhecimento e a Guerra de Informação, que são consideradas essenciais para a formação e para o treino, e procura ainda consolidar o conhecimento e normalizar os procedimentos a adotar por todos os que participam na edificação da Capacidade de Comando e Controlo Terrestre.

A atual publicação tem como base publicações doutrinárias da OTAN e do Exército dos Estados Unidos da América, nomeadamente o *AJP-6 Allied Joint Doctrine* for *Communications and Information Systems*, de 2017, o *AJP-3.10 Allied Joint Doctrine for Information Operations*, de 2015, o *FM 3-12 Cyberspace Operations and Electronic Warfare*, de 2021. A PDE 3-0 Operações, de 2012, e as Instruções de Segurança Militar, de 2020, foram igualmente fontes bibliográficas para a elaboração da presente publicação.

Da aprovação da presente publicação, decorrerá, em coerência, a produção futura de todo um conjunto de documentos doutrinários que versarão e detalharão os conceitos, funções e procedimentos no âmbito CI, na perspetiva do emprego de Forças.

O CHEFE DA DIVISÃO DE INOVAÇÃO E DOUTRINA

RAUL JOSÉ FELISBERTO MATIAS
COR TIR INF

Página intencionalmente em branco

CAPÍTULO 1 – INTRODUÇÃO

SECÇÃO I – GENERALIDADES

101. Finalidade

A finalidade da presente publicação é proporcionar um conjunto de referências e orientações doutrinárias essenciais ao planeamento e execução do apoio em Comunicações, Sistemas de Informação (SI), Gestão da Informação e do Conhecimento e de Guerra de Informação (GI), quer no nível operacional quer no nível tático.

102. Âmbito

Esta publicação enquadra as Comunicações e a Informação (CI) no ambiente operacional contemporâneo, onde a tecnologia tem um papel determinante na utilização do Ciberespaço e da informação, exigindo Sistemas de Informação e Comunicações (SIC) robustos, seguros e adequados às necessidades das Forças militares, desde os altos escalões até ao Soldado. As CI contribuem ativamente para que o Comando-Missão enquanto Função de Combate, integre e potencie as outras funções de combate ao passo que promove o desenvolvimento da ciência do controlo.

A "era da informação / conhecimento" que molda o mundo contemporâneo, insere-se na visão da transformação e de modernização que o Exército está a empreender, materializando-se na edificação das capacidades operacionais essenciais tendo em mente a obtenção da superioridade de informação, integrando na doutrina e na condução das Operações e conceitos tais como, as operações centradas em Rede (NCO / NCW[1]) e o OTAN *Network Enabled Capability* (NNEC[2]).

SECÇÃO II – O AMBIENTE OPERACIONAL CONTEMPORÂNEO

103. Generalidades

O ambiente operacional contemporâneo é um conjunto cada vez maior de condições, circunstâncias e influências que afetam o emprego da Força Militar e a decisão do

[1] Numa visão holística o *Network Centric Operations* (NCO) é o conceito relativo a uma Operação apoiada/valorizada pela Rede (infraestrutura tecnológica e pessoas colaborativas numa estrutura organizacional), enquanto o *Network Centric Warfare* (NCW) materializa o NCO numa Operação militar. O NCW envolve uma nova forma de pensar a execução das missões, a organização e do nosso inter-relacionamento para operacionalizamos os sistemas de armas de apoio.

[2] NNEC é o conceito da OTAN para as operações centradas em Rede: "*The Alliance's technical ability to federate the various components of the operational environment, from the strategic level* (*including* OTAN HQ) *down to the tactical levels*, *through a networking and information infrastructure* [MCM-0038-2005, *Development of an NATO Network-Enabled Capability* (NNEC)]".

Comandante (Cmdt). Hoje em dia esse ambiente muda rapidamente com o desenvolvimento acelerado das tecnologias e com as mudanças sempre imprevisíveis das perceções e atitudes dos seus intervenientes. Se é um facto que as tecnologias, as perceções e atitudes mudam, também as dos adversários ou potenciais adversários se alteram, sendo por isso que hoje o Exército opera num ambiente operacional mais perigoso e imprevisível. É neste enquadramento que as CI são importantes, porque facultam ao Exército a informação, as redes de comunicações e outras capacidades essenciais para que os seus Cmdt observem, compreendam a situação e ajam primeiro, decisivamente e com sucesso neste novo ambiente operacional.

104. Enquadramento Nacional

a. O Exército, Componente Terrestre do Sistema de Forças Nacional, é uma instituição estruturante do Estado Português. É fundamental a existência de um Exército moderno, adaptado e adaptável às alterações do ambiente político, estratégico e operacional contemporâneo, atento à evolução científica e tecnológica e adequado à realidade da profissionalização. Um Exército em consonância com os recursos humanos e económicos do País, versátil e disponível. Um Exército apto a satisfazer, no seu âmbito, os compromissos externos do Estado, num quadro de segurança internacional cada vez mais coletiva e cooperativa, e de operações militares predominantemente Conjuntas e Combinadas.

b. Por conseguinte, devemos olhar para o Exército como uma estrutura dinâmica, capaz de projetar Forças ao nível tático e operacional, decorrente da muito baixa probabilidade de um ataque militar contra o Território Nacional e das implicações do alargamento das fronteiras de segurança e defesa.

c. O Exército tem por missão principal participar, de forma integrada, na defesa militar da República, através da realização de operações terrestres, participar na cooperação das Forças Armadas com as Forças e Serviços de Segurança e colaborar em missões de proteção civil e em tarefas relacionadas com a satisfação das necessidades básicas e a melhoria da qualidade de vida das populações. Para garantir este desiderato implanta-se no Território Nacional em Unidades, Estabelecimentos ou Órgãos (U/E/O) dispersos pelo território, a partir das quais se projeta a Componente Operacional do Sistema de Forças Nacional.

105. Enquadramento Internacional

a. No âmbito dos compromissos internacionais pretende-se, de acordo com as Missões das Forças Armadas, contribuir para Operações desenvolvidas pelas Organizações de

Segurança e Defesa Coletiva que venham a ser decididas pelos competentes Órgãos de Soberania, com o objetivo de preservar a paz e a segurança internacionais.

b. Assume ainda particular importância, empregar Forças e meios militares na satisfação dos compromissos internacionais assumidos por Portugal, assegurando um contributo equilibrado e credível para a defesa coletiva no âmbito da Organização do Tratado do Atlântico Norte (OTAN) e para as estruturas de defesa da União Europeia (UE). A OTAN continua, no entanto, a constituir um objetivo prioritário no âmbito das organizações de defesa coletiva que Portugal integra, pelo que se torna importante contribuir para a progressiva consolidação de uma identidade de defesa europeia desde que articulada com os compromissos assumidos perante a Aliança Atlântica. Num contexto de partilha de informação em ambiente federado, a interoperabilidade na OTAN assume-se como uma fundamental base para a tomada de decisão a par de princípios de eficiência e reutilização de normas e capacidades existentes preconizados pelo conceito *Federated Mission Networking* (FMN).

106. O Papel dos sistemas C4I no moderno campo de batalha

a. A digitalização do moderno campo de batalha potenciou os sistemas de Comando, Controlo, Comunicações, Computadores e Informação (C4I) que exigem o tratamento e a rápida disseminação da informação aos vários escalões para apoio à tomada de decisão. Consequentemente, a disponibilização de uma maior quantidade de informação e de melhor qualidade de serviços (voz, dados e imagem), exigem comunicações mais robustas, eficientes e com maior largura de banda para disponibilizar a informação necessária às exigências dos utilizadores.

b. Atualmente o ambiente operacional é caracterizado pela mudança rápida não só porque o desenvolvimento tecnológico é acelerado, mas também porque se assiste constantemente a mudanças imprevisíveis dos seus atores, operando o Exército Português num ambiente potencialmente mais perigoso e imprevisível, tornando-se decisiva a existência de uma capacidade C4I capaz de apoiar as várias atividades do Processo Operacional (Planear, Preparar, Executar e Avaliar) permitindo ao Cmdt Visualizar, Descrever, Dirigir e Avaliar/Liderar de forma contínua. Neste enquadramento, as Comunicações e Informação e o seu campo de atuação têm progressivamente um papel mais importante nas Operações do Exército, cada vez mais dependentes de um fluxo contínuo de informação precisa, oportuna, completa e fiável.

c. A adequação dos sistemas C4I do Exército às necessidades das suas Forças no atual Campo de Batalha, vai contribuir para melhorar e potenciar o Comando e Controlo

(C2), dinamizando o treino Conjunto e Combinado, potenciando as capacidades dos Elementos da Componente Operacional do Sistema de Forças (ECOSF) para a pluralidade de missões em que poderão ser empregues (incluindo Operações ou missões da Organização das Nações Unidas, da OTAN e da UE) e garantindo o apoio militar de emergência às populações e às autoridades nacionais, em situações de crise ou catástrofe enquadradas nas operações de Apoio Civil.

107. Tendências de Evolução

a. Prevê-se que, no futuro, os conflitos sejam influenciados pela instabilidade causada pela emergência dos estados falhados, pelo extremismo ideológico e terrorismo, pelas ameaças transnacionais e crime organizado, mas também pela disputa de recursos naturais e pelas alterações climáticas, pelos efeitos da globalização e pelas ameaças sistémicas e cibernéticas que poderão causar a disrupção dos Estados.

b. Neste contexto, o futuro ambiente operacional será certamente muito complexo, quer em termos de espaço de batalha (assimétrico) quer de áreas de atuação (urbana, desértica ou ártica). As Operações futuras terão um forte cariz assimétrico, quer em efetivos quer em tecnologia, e poderão desenrolar-se nas mais variadas Áreas de Operações, desde as áreas urbanas, densamente povoadas e onde o fator 'baixas zero' poderá condicionar a liberdade de atuação das Forças militares até às áridas áreas desérticas ou árticas que condicionarão a manobra e o apoio logístico necessário. Nesse ambiente operacional, a tecnologia terá um papel determinante na utilização do Ciberespaço e da informação, exigindo SIC robustos e adequados às necessidades das Forças militares, desde os altos escalões até ao Soldado que contribuam para a superioridade da informação da Força.

SECCÇÃO III – COMUNICAÇÕES E INFORMAÇÃO NA ERA DO CONHECIMENTO

108. Generalidades

a. O sector das Tecnologias de Informação e Comunicações (TIC) tem um conjunto de características específicas que o diferenciam dos sectores de atividade no sentido convencional do termo, não só porque se trata de um sector baseado na ciência, mas também pela sua enorme flexibilidade, o que faz com que seja transversal a um grande leque de atividades organizacionais (por exemplo: social, política, económica e militar) e também domésticas. As TIC, com a sua linguagem esotérica e as suas concretizações em termos de aplicações, bases de dados, sistemas operativos e redes

de comunicações, que suportam e instrumentam as organizações, são constituídas por Entidades Informacionais, por Fluxos Processuais, por Pontos de Decisão e por Meios de Atuação. É neste referencial que os seres humanos se situam em relação às TIC, pois cada um de nós num dado momento e num certo contexto (fluxo), tendo em conta a problemática concreta (informação) toma a decisão de agir de determinada forma (atuação).

b. A emergência de novos modelos de interação global, acompanhada pelos recentes sinais de exploração militar da Internet e do Ciberespaço[3], tem também um impacto profundo no ambiente estratégico internacional, não só ao nível político, económico e social, mas também ao nível militar, daí resultando inevitáveis implicações para a atividade das Forças Armadas. Dentro deste contexto, o Ciberespaço constitui hoje o quinto domínio operacional, reconhecido por vários países da OTAN e UE, materializando um novo Campo de Batalha onde têm lugar operações militares destinadas a moldar o ambiente de informação, de acordo com a salvaguarda dos interesses dos Estados. Assim, constata-se que a forma como os diferentes atores utilizam a informação pode ser simultaneamente geradora de novas oportunidades e de novas ameaças no Ciberespaço, apresentando importantes implicações na condução da política e da estratégia dos Estados. Isto obriga a que os Estados mantenham o empenhamento das suas capacidades de defesa e segurança em diversos Teatros, reais e virtuais.

c. Neste contexto, a componente não cinética dos conflitos tem vindo a assumir uma especial preponderância, colocando importantes desafios às Forças Armadas, num mundo virtual informático que constitui, cada vez mais, o habitat operacional onde as ações dos seus agentes se concretizam, e onde têm que levantar as capacidades necessárias para uma atuação eficaz em novas dimensões do moderno campo de batalha, nomeadamente no domínio da Informação e do Ciberespaço.

[3] De acordo com a PAD 320-02 Glossário de Termos e Definições do Exército Português, o Ciberespaço é o domínio global dentro do Ambiente Informacional que consiste na interdependência de redes e infraestruturas de tecnologia de informação, tais como a internet, redes de computadores, entre outros.

109. Conceito Sistémico

A Superioridade de Informação[4], constitui um objetivo estratégico a levantar pelo Exército, materializando uma nova capacidade. Esta capacidade, estrutura-se com base na gestão de topo do domínio da informação, coordenando e facilitando o alinhamento do apoio SIC com a área da GI. Através da implementação deste conceito, que envolve Pessoas, Informação e Tecnologia, será possível melhorar a eficácia operacional das Forças Terrestres com base em decisões cada vez mais rápidas e acertadas, em resultado da disponibilização da informação necessária, no momento certo e de forma segura, a todos os níveis e escalões hierárquicos.

Neste contexto, a infraestrutura tecnológica existente, constitui um importante "ponto de partida", uma vez que permite, identificar quatro áreas nucleares e dois instrumentos integradores, sobre as quais se edifica esta capacidade:

a. Áreas Nucleares

(1) Comunicações (Com);

O Sistema de Comunicações do Exército, assegura a integração e a coerência dos sistemas, redes e tecnologias de comunicações estruturais de natureza fixa (nível operacional) e dos conjunturais de natureza tática, bem como a sua capacidade de ligação a Sistemas Conjuntos e Combinados.

(2) Sistemas de Informação;

Os SI e as tecnologias de informação da responsabilidade do Exército, asseguram a compatibilidade e a coerência dos sistemas e tecnologias de informação estruturais e de natureza tática, bem como a sua interoperabilidade com Sistemas Conjuntos e Combinados.

(3) Gestão da Informação e do Conhecimento (GIC);

A preservação, partilha e disponibilização controlada da informação e do conhecimento no Exército, promove o desenvolvimento, implementação e exploração de SI de gestão para o apoio à tomada de decisão no nível estratégico e operacional e no apoio aos Estados-Maiores (EM) na aplicação do processo de decisão.

(4) Guerra de Informação.

---

[4] A Superioridade de Informação ("*Information Superiority*"), conforme refere o JP 3-13, traduz uma situação de vantagem no domínio da informação, resultante da capacidade para "reunir, processar e disseminar um fluxo ininterrupto de informação enquanto se explora ou nega a capacidade de um competidor/adversário poder fazer o mesmo". Uma vez garantida a disponibilidade e a integridade dos SI, uma opção futura que se coloca é a expansão da influência do seu ambiente de informação (Info-esfera) em direção a outros ambientes mais alargados, dentro dos quais a Organização ou o Estado pretende intervir.

A capacidade de Ciberdefesa, Guerra Eletrónica (GE) e a implementação de medidas que garantam a segurança da informação, das comunicações e dos sistemas e tecnologias de informação no âmbito das operações em redes de computadores e a pronta resposta e investigação de incidentes, asseguram a garantia da informação.

b. Sistema de Informação e Comunicações do Exército

O SIC do Exército é composto por duas componentes: uma de natureza estrutural ou permanente, que se designa por Sistema de Informação e Comunicações Operacional (SIC-Op), e outra de natureza conjuntural ou tática, designado por Sistema de Informação e Comunicações Tático (SIC-T).

(1) Sistema de Informação e Comunicações Operacional

(a) Sistema integrador, no nível operacional, das componentes de Comunicações, de Informação e de Segurança dos SIC. De natureza estrutural, visa garantir a capacidade de C2 do Exército sobre as suas U/E/O, desenvolvendo-se através dos seguintes vetores:

1. Vetor da transmissão, comutação de dados e redes locais;
2. Vetor da atualização dos serviços de apoio à produtividade, à gestão e ao C2 de nível operacional;
3. Vetor da obtenção, processamento, armazenamento, proteção e distribuição dos dados e informações e partilha do conhecimento.

(b) Articula-se funcionalmente com o SIC-T, com o qual troca informação relevante de forma transparente.

(2) Sistema de Informação e Comunicações Tático

Sistema integrador, no nível tático, das componentes de Comunicações, de Informação e de Segurança SIC. De natureza conjuntural, destinado a apoiar durante um tempo determinado uma Força-Tarefa para uma missão específica, em situação de campanha ou como Força Nacional Destacada (FND), sendo constituído pelos seguintes elementos:

(a) Módulos de Comunicações;

(b) Redes Rádio de Combate, orgânicas das Unidades Táticas;

(c) SI para Operações.

Articula-se funcionalmente com o SIC-Op, com o qual troca informação relevante de forma transparente.

c. Arquitetura

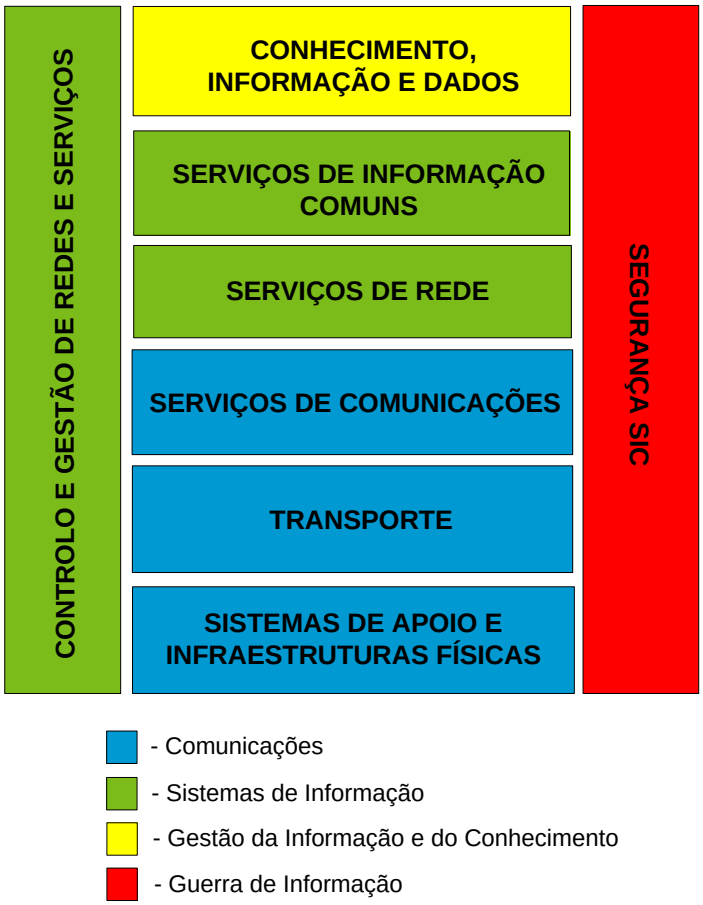

Figura 1-1 - Arquitetura do Sistema de Informação e Comunicações do Exército

110. Desafios da Tecnologia

Tendo em vista preparar o Exército para enfrentar todo o Espectro de Operações e as novas dinâmicas que o moderno Campo de Batalha encerra, o Exército tem promovido a revisão do apoio SIC segundo uma filosofia de Força Centrada em Rede (seguindo os requisitos NNEC), aprovando o enquadramento doutrinário apresentado para a área da GI e definindo princípios de coordenação do domínio da informação. Neste contexto, a capacidade para gerir a mudança e para definir uma gestão de topo, capaz de integrar e coordenar os processos que permitem intervir de forma coerente e eficaz no ambiente de informação, constitui uma condição necessária para empreender um esforço estrutural tão importante como o levantamento de novas capacidades e a transformação de outras já existentes.

A edificação de um sistema de C2, enquanto elemento central para a garantia de superioridade de informação e de apoio ao processo de decisão, materializa a forma como o Exército deverá extrair o valor decorrente de uma utilização cada vez mais coerente, integrada e segura do ambiente de informação. Desenvolve-se a partir de

referências doutrinárias aprovadas, garantindo uma convergência para Objetivos de Força Nacionais, definidos tanto no plano interno como no quadro dos compromissos internacionais assumidos por Portugal (OTAN e UE).

No longo prazo (2030) todos os sistemas tecnológicos utilizados no âmbito da Defesa Nacional terão que operar de acordo com uma arquitetura de informação comum. A interoperabilidade é garantida através da federação de Redes e SI e surge de forma transparente para os utilizadores, facilitando o desenvolvimento de um Portal de acesso aos vários centros de conhecimento do Exército e estimulando a criação de um Sistema Integrado de Gestão do Conhecimento.

Esta transição, quando equacionada em termos estruturais, operacionais e genéticos, consubstancia uma aproximação integrada à mudança, beneficiando e fornecendo orientações para três dimensões-chave: Pessoas (visão estrutural), Informação (visão operacional) e Tecnologia (visão genética).

Além de que permite aproveitar um elevado número de Capacidades que o Exército já possui e permite perspetivar de forma integrada e proactiva a atuação das Forças Terrestres no ambiente de informação, traçando um rumo claro de mudança e materializando uma alteração do paradigma atual, que contraria uma visão segmentada e uma utilização não coordenada das capacidades existentes neste domínio, a ocorrência da transição proposta assenta em três objetivos estratégicos estruturantes (ver figura 1-2):

a. Explorar e potenciar a utilização operacional da informação e a superioridade de decisão

Através da garantia da liberdade de ação no ciberespaço, assegurando a contínua operacionalidade dos SIC, necessária à garantia da disponibilidade e resiliência da informação no Exército, desde o nível estratégico ao nível tático, e explorando as oportunidades da transformação digital para modernizar o processo de decisão.

b. Defender e Proteger o ambiente de Informação

Através do levantamento de uma Capacidade de GI que permita garantir tanto a disponibilidade e integridade da informação (*Information Assurance*) como a possibilidade de intervir no domínio da informação de forma concertada no sentido da obtenção da Superioridade de Informação.

c. Garantir a Gestão de Topo (*Governance*) do ambiente de Informação

Através da coordenação do planeamento e da sincronização de todas as atividades (Comunicações, SI, GIC e de GI) a desenvolver pelo Exército no ambiente de

informação, permitindo explorar sinergias e maximizar a utilização dos recursos disponíveis.

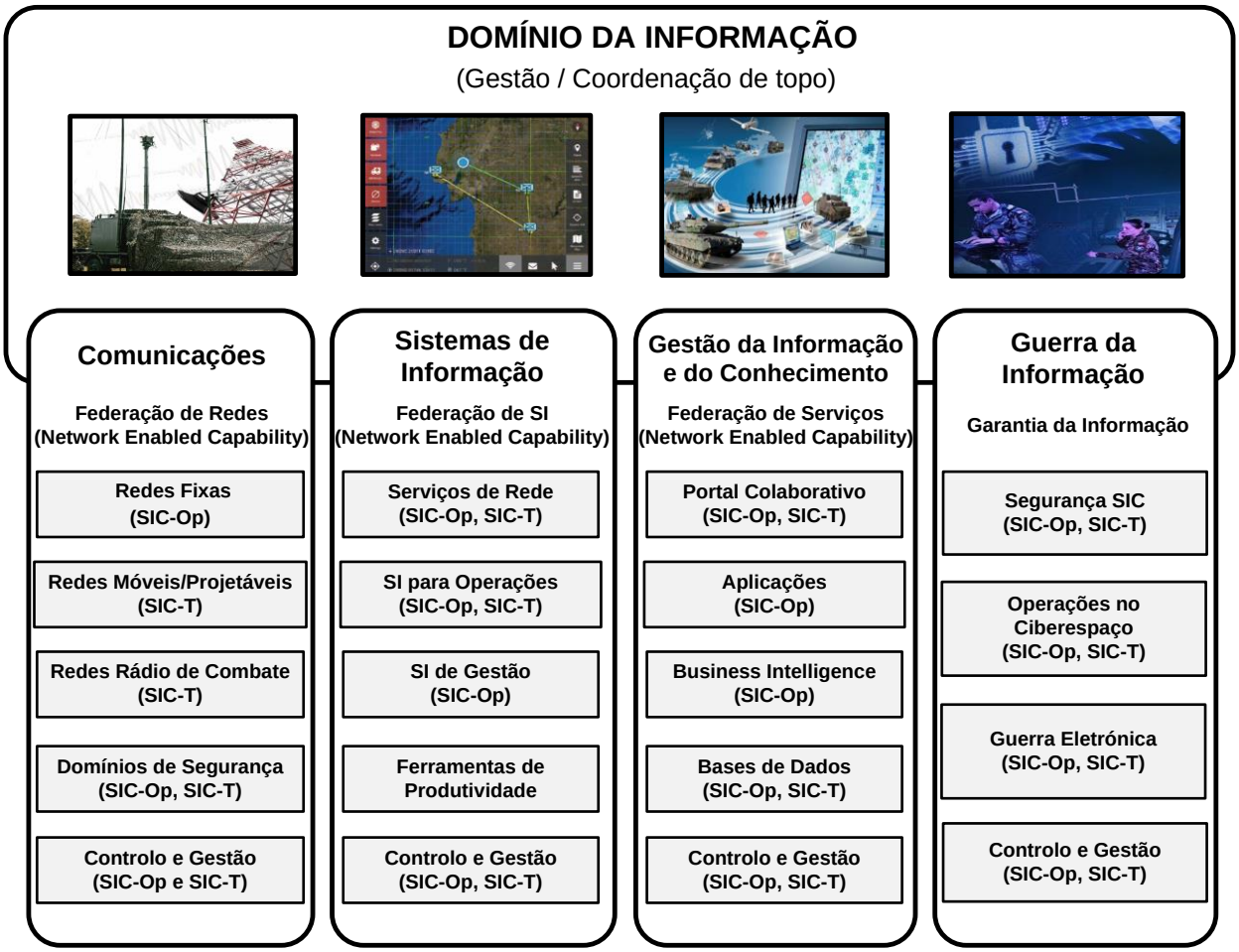

Figura 1-2 – Visão Integrada do Domínio da Informação

A Visão Integrada do Domínio da Informação concretiza assim a forma como o Exército deverá extrair o valor decorrente de uma utilização cada vez mais coerente, integrada e segura do ambiente de informação.

CAPÍTULO 2 – COMUNICAÇÕES

SECÇÃO I – INTRODUÇÃO

201. Generalidades

O atual ambiente operacional reflete o exponencial crescimento e as novas potencialidades das Comunicações e Sistemas de Informação (CSI). Atualmente os cenários operacionais estão centrados em Rede, a qual, se corretamente usada e protegida, garante uma potencial vantagem às nossas Forças.

A disponibilidade permanente de comunicações seguras e a capacidade, sem restrições, de transferência de dados devem ser permanentemente incorporadas nas operações militares, onde quer que elas sejam planeadas ou executadas.

As Operações são normalmente caracterizadas por direção centralizada para alcançar a unidade de esforço, enquanto a autoridade para a execução deve ser descentralizada, ou seja, delegada no menor escalão adequado para garantir o uso mais eficaz das Forças. Para habilitar uma execução descentralizada e direção centralizada, é necessário que a estrutura de C2 seja completamente compreendida em todos os escalões, de forma a facilitar a clara, oportuna e segura transmissão de orientações, ordens, relatórios de situação e informação de coordenação.

Neste capítulo, apresentam-se os princípios e conceitos desta área nuclear, bem como a arquitetura dos sistemas de comunicações quer ao nível estratégico/operacional quer ao nível tático.

202. Princípios das Comunicações

O Cmdt de uma Força Terrestre para atingir os objetivos deve considerar e aplicar, em todas as fases de uma Operação ou Campanha, os princípios das Comunicações. A correta aplicação destes princípios assegura os elementos essenciais para que os sistemas funcionem de forma eficaz numa ampla variedade de situações. Embora este parágrafo aborde estes princípios separadamente, podem estabelecer-se inter-relações entre os mesmos.

a. Ligação

(1) Os meios de Comunicações devem garantir a ligação entre elementos das Forças militares, facilitando a compreensão mútua e a unidade de ação e intenção. A ligação pode ser reforçada através da incorporação da capacidade *reach-back* com o seu escalão superior, quando numa situação de Força projetada. A ligação, uma vez estabelecida, deverá ser efetivamente mantida.

(2) A ligação é estabelecida da seguinte forma:

(a) Do escalão superior para o subordinado;

(b) Da Unidade de apoio para a apoiada;

(c) Da Unidade de reforço para a reforçada;

(d) Entre Unidades localizadas da esquerda para a direita;

(e) De uma Unidade para um destacamento.

b. Economia de Meios

Evitar a duplicação, definir e gerir cuidadosamente os requisitos dos utilizadores e impor uma disciplina rigorosa de transmissão que permita alcançar a economia de meios de Comunicações. Para maximizar a eficiência e satisfazer as expectativas dos utilizadores, os requisitos devem ser desenvolvidos com sugestões dos utilizadores e claramente definidos na fase inicial do planeamento, através de *Information Exchange Requirements* (IER). No entanto, uma ênfase excessiva na economia de emprego dos meios de Comunicações pode reduzir o benefício que alguns desses meios podem fornecer, não podendo em caso algum colocar em causa o apoio de Comunicações a uma Força.

c. Interoperabilidade

Os objetivos gerais subjacentes às operações terrestres exigem que as estruturas de comunicações que habilitam o Comando das Forças Terrestres Nacionais e aliadas sejam normalizadas, tanto quanto possível de forma a atingir a interoperabilidade. A interoperabilidade é garantida através da compatibilidade[5], da normalização[6] e do uso de equipamentos e sistemas comuns[7]. Os planos de comunicações devem assegurar que os requisitos essenciais de normalização de todas Forças Nacionais e aliadas são especificados. A eficácia das operações terrestres multinacionais exige sistemas de

[5] A compatibilidade é uma condição necessária para a obtenção da interoperabilidade. Define-se como a capacidade de dois ou mais componentes de equipamentos ou sistemas funcionarem na mesma estrutura ou ambiente sem que exista interferência mútua. A compatibilidade eletromagnética e informática tem de ser considerada logo nos estágios conceptuais iniciais e durante todo o planeamento, desenho, desenvolvimento, teste e avaliação, e ciclo de vida operacional de todos os sistemas.

[6] Os interfaces e protocolos dos SIC devem seguir *standards* (nacionais e/ou OTAN). Devem ser reduzidos ao mínimo as soluções de recurso para compensar faltas de conformidade com interfaces/protocolos padrão. Esta característica facilita também reabastecimento de recurso/emergência de componentes entre as várias Componentes de uma Força Combinada ou Conjunta. Contribui igualmente para evitar duplicações de esforços na pesquisa e desenvolvimento de novas tecnologias.

[7] Os equipamentos e sistemas são comuns, quando podem ser operados e mantidos por pessoal com formação em qualquer um dos sistemas sem necessidade de treino ou formação adicional, e quando os seus sobresselentes e consumíveis (módulos ou componentes) podem ser trocados entre si.

comunicações interoperáveis que permitam ao Comando da Componente Terrestre e aos seus Cmdt Subordinados o exercício do C2 eficaz entre os elementos da Força. Estabelecem-se os seguintes pré-requisitos para facilitar a interoperabilidade:

(1) Desenvolver um conceito de Comunicações conjunto para a Força;
(2) Harmonizar a informação, a semântica e desenvolver a gestão de dados;
(3) Disponibilizar e implementar acordos operacionais, procedimentos e normas técnicas;
(4) Partilhar informação e serviços com outros elementos da Força.

d. Flexibilidade

A flexibilidade deve garantir que os sistemas de Comunicações projetados possam responder às mudanças dos níveis de empenhamento, ao ritmo operacional e à postura da Força. A flexibilidade é necessária para responder a situações de mudança e à diversidade das Operações com o mínimo de perturbação ou atraso. Por exemplo, uma mudança de postura da Força, de manutenção para imposição da paz, pode resultar em pequenas alterações na estrutura da Força, que poderão resultar em requisitos de Comunicações consideravelmente diferentes. A flexibilidade é conseguida através dos seguintes fatores:

(1) Desenvolvimento e ensaio de planos de contingência;
(2) Uso de infraestruturas e sistemas comerciais;
(3) Utilização de equipamentos e sistemas de comunicações com elevada mobilidade e transportabilidade;
(4) Liberdade de manobra dentro do ambiente eletromagnético;
(5) Existência de meios de reserva;
(6) Serviços e processos normalizados;
(7) Fazer uso de meios alternativos.

A flexibilidade permite que o planeamento e a manobra de Comunicações sejam facilmente integrados nos planos e manobra operacional.

e. Redundância

É um elemento vital para a flexibilidade das Comunicações, pois permite ao pessoal de transmissões os meios necessários para disponibilizar os serviços por caminhos alternativos, o que aumenta significativamente a probabilidade de comunicações ininterruptas.

f. Gestão do Espectro

A utilização dos meios ativos de Comunicações deve ser coordenada aos níveis estratégico, operacional e tático em ambientes nacionais ou internacionais. O uso

destes meios deve ser considerado durante a elaboração do plano de controlo de emissões (EMCON) e durante a sua implementação. O uso do espectro eletromagnético, em apoio aos requisitos da missão, deve ser planeado por pessoal qualificado, quer para assegurar maior eficiência na utilização dos limitados recursos disponíveis, quer para assegurar a coordenação com as Unidades adjacentes, o escalão superior e outras autoridades.

g. Resiliência

Resiliência é a capacidade dos sistemas e equipamentos de comunicações de se recuperarem de falhas/avarias que causam anomalias no seu funcionamento. A robustez[8] dos equipamentos e os princípios da economia de meios, a flexibilidade e a redundância contribuem para a resiliência. A disponibilidade das comunicações, devido ao seu papel crítico nas Operações, apresenta alta prioridade. Todavia, os meios de Comunicações disponíveis e resistentes não são necessariamente resilientes sem pessoal devidamente treinado para os operar e gerir. A capacidade de sobrevivência dos sistemas de comunicações deve ser tal, que os mesmos continuem a apresentar níveis de desempenho pré-definidos, mesmo quando sujeitos a ações hostis, desastres naturais ou quaisquer outras calamidades graves, ou falhas técnicas do pessoal. Sistemas que suportam tarefas militares críticas, podem exigir proteção contra impulsos eletromagnéticos, serem construídos com precauções especiais e estar localizados em instalações protegidas, no entanto, os custos de implementação associados obrigam a que estas facilidades sejam apenas disponibilizadas a comunidades de utilizadores selecionados.

h. Priorização

Os Cmdt e seus EM devem estar cientes que os meios de Comunicações necessários para apoiar uma Operação são aproximadamente proporcionais à escala da Operação. Todavia, devem também ser considerados outros fatores, tal como a necessidade de uma capacidade mínima de meios CSI para suportar o C2 de uma Força Terrestre, independentemente do escalão da Força Operacional empregue. Esta consideração torna-se importante quando existe o envolvimento simultâneo em várias Operações, mesmo de escala moderada. Em todas as Operações, há uma necessidade de estabelecer prioridades rigorosas para a alocação dos limitados recursos CSI, incluindo largura de banda, com base nos IER e na intenção do Cmdt.

[8] Robustez é a capacidade de os equipamentos continuarem a funcionar em condições ambientais adversas (choques, trepidações, etc.).

i. Capacidade

Embora a capacidade de Comunicações seja invariavelmente finita, os avanços tecnológicos aumentaram significativamente o volume e a taxa de entrega de dados. Para evitar atrasos no processo de decisão, devem ser tomados os necessários cuidados para garantir uma capacidade SIC adequada, para apoiar a gestão e os requisitos de exploração da informação. Deve-se disponibilizar uma capacidade ajustada à procura previsível, mas podem sempre surgir situações operacionais em que limitações de comunicações precipitam a adoção de diferentes estratégias de exploração ou da gestão da informação. Sempre que possível, tecnologias e procedimentos tais como a gestão dinâmica da largura de banda, a comutação de protocolo de internet, mensagens instantâneas e eficientes, podem ser utilizadas para maximizar a capacidade. O uso de meios de Comunicações comerciais podem constituir um recurso para aumentar a capacidade.

203. Conceitos

a. Sistema de Informação e Comunicações

Sistema que permita armazenar, processar e transmitir informação e compreende todos os ativos necessários ao seu funcionamento, designadamente infraestrutura, organização, pessoal e recursos.

b. Sistema de Comunicações

Conjunto de equipamentos, métodos, procedimentos e, se necessário, pessoal, organizado para assegurar a transmissão de informação entre entidades.

c. Comando

É o processo pelo qual a vontade do Cmdt, os planos, e as intenções são transmitidas aos subordinados. O Comando engloba a autoridade e a responsabilidade para projetar Forças no cumprimento de uma determinada missão.

d. Controlo

É o processo através do qual o Comandante, Diretor ou Chefe (Cmdt/Dir/Ch), assistido pelo seu EM, organiza, dirige e coordena as atividades das Forças que lhe são atribuídas. Para alcançar este objetivo o Cmdt/Dir/Ch e o seu EM utilizam procedimentos normalizados, em conjugação com o equipamento CSI disponível.

e. Comando e Controlo

Juntos, estes dois processos formam o sistema de C2, que o Cmdt/Dir/Ch, EM e subordinados usam para planear, dirigir, coordenar e controlar as Operações. Os militares que integram o EM CSI (G6) fornecem os pareceres sobre a arquitetura do sistema de C2 mais eficaz, considerando as capacidades CSI disponíveis.

O sistema de C2 deve proporcionar aos Cmdt um cenário no qual possam tomar as suas decisões. Para apoiar esta situação, o sistema de C2 deve habilitar o EM a gerir o tempo e o fluxo de informação. Além disso, a estrutura de C2 da Força e todas as Relações de Comando devem ser robustas, capazes de suportar desenvolvimentos e adaptações durante o curso da Operação. Por último, mas não menos importante, é necessária uma arquitetura de comunicações e informação robusta para apoiar um sistema de C2.

O âmbito e a amplitude do sistema SIC no apoio ao C2 são determinados pela combinação da estrutura de C2, pela sua dispersão geográfica, pelo nível de informação a ser trocada entre cada entidade C2 e pela aplicação do conceito *reach-back*. A estrutura de C2 e sua dispersão geográfica serão determinadas por fatores operacionais, numa base caso-a-caso e moldadas às necessidades de cada missão.

f. Requisitos de Intercâmbio de Informação

Os Requisitos de Intercâmbio de Informação (*Information Exchange Requirements* - IER) definem as necessidades para troca de informação entre duas ou mais entidades envolvidas num determinado processo. Os IER descrevem a origem e destino do fluxo de informação, o conteúdo e, normalmente, outras características do fluxo de informação (formato, classificação de segurança, tamanho, atributos, entre outros). Os IER são essenciais para o planeamento do apoio de Comunicações, assegurando que todas as relevantes necessidades de C2 são identificadas e alcançadas.

g. Serviço

Capacidade fornecida para beneficiar ou apoiar comunidades de utilizadores.

h. Arquitetura

Organização fundamental de um sistema refletido nos seus componentes e nas relações entre eles, na sua relação com os restantes sistemas, bem como os princípios que orientam o seu desenho e evolução.

i. Federação de Redes

Agregação de múltiplas redes independentes que têm diferentes ou iguais características técnicas, procedimentos ou segurança. Essas redes são estabelecidas e operadas independentemente; no entanto, elas seguem os padrões e protocolos acordados para executar a operação adequada da Rede abrangente como um todo.

j. *Federated Mission Networking*

FMN é a abordagem da OTAN para unificar redes de diferentes membros de uma coligação para fornecer serviços de troca de informações, permitir troca de informações entre os membros da coligação e orientar o estabelecimento de relações

da Rede de missão entre a OTAN, nações da OTAN e entidades não OTAN nas quais se podem realizar toda a gama de atividades operacionais dentro das Operações lideradas pela OTAN.

SECÇÃO II – DOMÍNIO CLASSIFICADO E DOMÍNIO NÃO CLASSIFICADO

204. Enquadramento

A superioridade da informação só será alcançável com a implementação de uma cultura de partilha de informação organizacional a quem tem necessidade de a conhecer. Todavia este ambiente requer um conjunto de medidas e políticas de segurança para garantir que apenas os utilizadores autorizados tenham acesso à informação. Para garantir estes mecanismos de partilha e segurança da informação, o sistema é estruturado em domínios de segurança, podendo a informação ser partilhada entre domínios utilizando *gateways* que permitem uma troca controlada de informação e habilitam um único domínio virtual de informação. Os domínios de segurança previstos no SIC do Exército são:

a. Domínio Não Classificado (DNClas)

Este domínio integra a infraestrutura CSI não classificada dos SIC do Exército, SIC-Op e SIC-T, com acesso à internet, destinados a garantir o processamento, armazenamento e transmissão de informação NÃO CLASSIFICADA.

b. Domínio Classificado (DClas)

Este domínio integra a infraestrutura CSI classificada dos SIC do Exército, SIC-Op e SIC-T, sem acesso à internet, destinados a garantir o processamento, armazenamento e transmissão de informação com classificação de segurança até SECRETO, nas diversas marcas de classificação de segurança.

c. Domínio de Missão

Domínios estabelecidos para uma missão específica no tempo e no âmbito de nações da OTAN e entidades não pertencentes à OTAN (governamentais ou não governamentais), que integram as infraestruturas CSI específicas da missão, sendo as políticas de implementação estabelecidas e acordadas por todos os participantes. Dependendo da situação, das tarefas da missão e das entidades participantes, um domínio de missão pode ou não ter um caráter subsidiário em relação aos domínios da OTAN. Um domínio de missão pode ser estabelecido independentemente das medidas e políticas de segurança SIC em uso no Exército ou na OTAN, de forma a permitir que todas as entidades numa Operação operem como pares iguais, incluindo entidades não pertencentes á OTAN. Embora este domínio esteja mais vocacionado

para o SIC-T, também se pode encontrar no SIC-Op, nomeadamente ao nível de Comando de Componente.

205. Serviços Transversais

Existem um conjunto de serviços de apoio ao C2 que estarão disponíveis em cada um dos domínios de segurança. A informação principal, para utilização diária no EM, nos Comandos Funcionais e no Comando da Componente Terrestre, reside no DClas, o qual permite o tratamento da informação com a classificação de segurança com a marca Nacional SECRETO.

Os serviços de apoio C2 estão disponíveis para apoiar os diferentes níveis de Comando, Direção ou Chefia, na execução do C2 e os EM na construção do processo de decisão e na gestão da informação. Os restantes utilizadores contribuem para aqueles dois objetivos principais.

Serviços de comunicações	DNClas	DClas
Telefonia	x	x
Videoconferência	x	x
Mensagens Instantâneas	x	x
Redes *Wireless Welfare*	x	
Serviço de Internet	x	

Tabela 2-1 – Exemplos de Serviços de Comunicações de Apoio ao C2

SECÇÃO III – SISTEMA DE COMUNICAÇÕES OPERACIONAL

206. Enquadramento

O Exército é uma organização habilitada a conduzir operações militares, de forma isolada, Conjunta ou Combinada. Para garantir este desiderato implanta-se no território Nacional em U/E/O dispersos pelo território, a partir das quais se projetam os ECOSF. Estas Forças quando projetadas são apoiadas pela componente de comunicações conjuntural ou tática, de natureza temporária e móvel, adaptada ao emprego em campanha de Forças-Tarefa e que disponibiliza pequenas e médias larguras de banda, paralelamente garante a interligação destas Forças com a sua estrutura territorial, através de uma componente de comunicações estrutural ou operacional, de natureza permanente e fixa, instalada nas U/E/O do Exército e dispõe de uma apreciável largura de banda.

A componente de comunicações operacional apoia as atividades militares diariamente desenvolvidas nas U/E/O e as atividades operacionais, garantindo o exercício e a consistência do C2 e a garantia de utilização, de uma forma simples, eficaz e segura, das

facilidades e dos serviços oferecidos pelas modernas tecnologias e SI, de forma a contribuir para a superioridade da informação.

Utilizando a mesma tecnologia de comunicações, as duas componentes, tática e operacional, são transparentes entre si, permitindo um fluxo ininterrupto de informação relevante entre os utilizadores em estações de trabalho em campanha e na componente fixa das U/E/O, neste sentido, considera-se que o sistema de comunicações do Exército é tendencialmente único, articulando-se nas duas componentes referidas.

207. Arquitetura do Sistema

a. O SIC-Op assenta numa arquitetura de comunicações integradora da arquitetura do SIC-T e compatível com as arquiteturas específicas dos sistemas do Estado-Maior General das Forças Armadas (EMGFA) e dos Ramos, visando a interoperabilidade com base no conceito de federação de sistemas, tal como é preconizado na OTAN, através do conceito NNEC, sendo complementado por sistemas civis contratualizados no domínio da voz e dos dados (telemóveis, telefones fixos, acessos internet).

b. O sistema de comunicações operacional, na sua arquitetura, é constituído pela Rede de Dados do Exército (RDE), pela Rede de Transmissão do Exército (RTE) e pelos Sistemas de Apoio associados (energias AC e DC e climatização) e infraestruturas físicas (edifícios das estações de comunicações, torres de comunicações e condutas de comunicações), que se caracterizam pela instalação fixa e funcionamento permanente.

208. Rede de Transmissão do Exército

A RTE é a estrutura de comunicações de suporte ao transporte de dados, sem restrições, entre os equipamentos da RDE e simultaneamente possibilitar o acesso a essa informação, às U/E/O e ao SIC-T, ao longo de todo o Território Nacional, com o objetivo de potenciar o exercício do C2 do Exército, nos diferentes níveis das Operações (estratégico, operacional e tático).

A RTE é constituída por várias sub-redes, das quais se destacam a Rede de Transmissão por Feixes Hertzianos (FHz), as Redes de Transmissão por Fibra Ótica, a Rede de Comunicações por Satélite (VSAT) para as Forças Nacionais Destacadas (FND)[9], as ligações VPN IPSEC, os circuitos dedicados alocados na infraestrutura partilhada de

[9]A Autoridade Funcional e Técnica para os aspetos militares do programa espacial da Defesa Nacional é o EMGFA, através da Unidade ou órgão que dirige os aspetos militares do programa espacial da Defesa Nacional.

transmissão das Forças Armadas e os circuitos dedicados alugados a operadores de telecomunicações.

A arquitetura da RTE é baseada numa estrutura com topologia em malha, composta por dois segmentos:

a. *Backbone* ou Segmento *Core*: é a estrutura de ligações centrais partilhada, entre Estações Nodais[10] e/ou Estações Repetidoras[11], com a capacidade de transmissão adequada às necessidades de acesso das U/E/O. Nas Estações Nodais é efetuada a "amarração" das ligações de acesso (Segmento de Acesso).

b. Acesso ou Segmento de Acesso: define as ligações entre as Estações Terminais[12] das U/E/O e as Estações Nodais.

209. Rede de Dados do Exército

A RDE tem uma abrangência Nacional e garante a ligação em malha das redes locais das U/E/O do Exército, bem como a ligação às redes exteriores. Assenta no estabelecimento de um ambiente de Rede suportado nos protocolos IP[13], o qual permite suportar toda a gama de serviços de Rede e aplicações, nas componentes de voz, dados e vídeo. A RDE é a estrutura responsável pelo roteamento da informação no SIC-Op, através de um conjunto de equipamentos ativos designados por *routers* e *switches*[14], que formam uma malha Nacional. Os serviços de comutação de voz e de videoconferência são igualmente suportados por esta Rede.

A arquitetura da RDE é assente numa estrutura em árvore em que as ligações aos elos de um dado nível confluem num único Nó do nível superior. Cada nível constitui uma estrutura em estrela, que liga um ou mais *routers* de nível superior (segmento core) a vários *routers* do nível imediatamente inferior (segmento de distribuição), estando todos os *routers core* interligados entre si, em malha ou anel, conforme figura 2-1.

[10] Estações Nodais – Estações do Segmento Core que interligam ligações de acesso.
[11] Estações Repetidoras – Estações que interligam Estações Nodais.
[12] Estações Terminais – Estações das U/E/O, que pertencem ao Segmento de Acesso.
[13] Protocolo de comunicação da camada de Rede no conjunto de protocolos da Internet para retransmissão de pacotes através dos limites da Rede. O seu roteamento permite ligar redes e, essencialmente, estabelece a Internet.
[14] *Router* é um equipamento de Rede que faz o encaminhamento de pacotes de dados entre redes de computadores. *Switch* é um equipamento de Rede que liga dispositivos numa Rede de computadores, recebendo pacotes de dados e encaminhando-os para o dispositivo de destino.

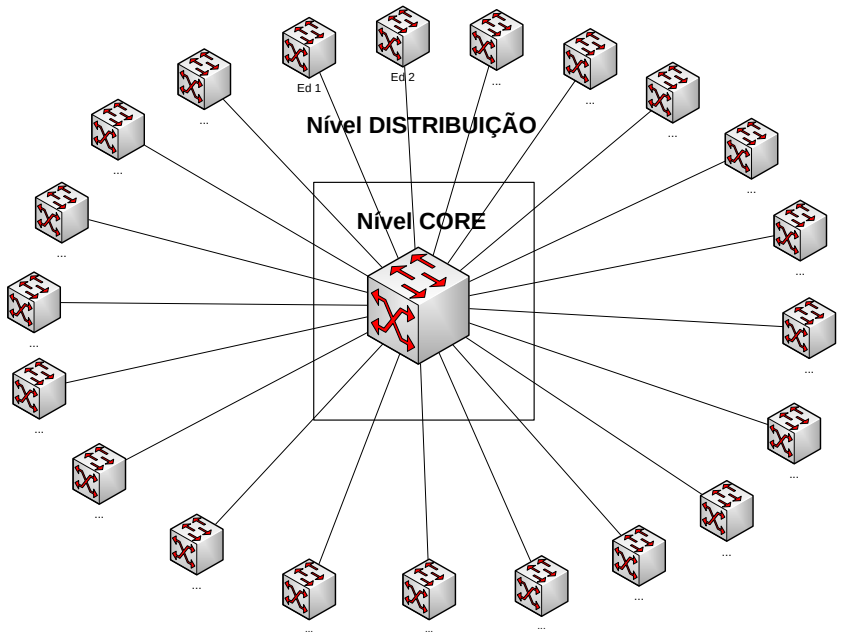

Figura 2-1 - Estrutura *Core* e de Distribuição da Rede de Dados

As Redes Locais (LAN) das U/E/O são fundamentalmente constituídas pelas componentes ativa e passiva. A componente passiva é genericamente constituída pelas infraestruturas de subsolo para encaminhamento de cablagem, bastidores, cablagem de cobre e fibra ótica e respetivos acessórios. A componente ativa é constituída pelo conjunto de equipamentos ativos de Rede passíveis de gestão remota (*switches*, UPS, etc.) que garantem aos utilizadores as condições para acesso aos dois domínios de Rede implementados nas redes locais, permitindo as melhores condições para a realização do trabalho aplicacional diário.

Também nas redes locais se implementa uma estrutura baseada em níveis hierárquicos, onde cada nível apresenta uma estrutura em estrela, que liga um ou mais bastidores de distribuição de cablagens a vários bastidores de distribuição e/ou acesso no nível hierárquico imediatamente abaixo.

As redes locais, para cada um dos domínios, assentarão em três segmentos de Rede:

a. Segmento *Core*

Neste segmento da Rede garante-se a conectividade entre edifícios, a ligação à WAN do Exército, o acesso à Internet (DNClas), a outras redes exteriores e aos *Datacenters* ou *Server Farms*. O seu principal objetivo é a comutação de tráfego a velocidades muito elevadas entre os diferentes módulos da Rede. A configuração de equipamentos *core* é mínima, basicamente *routing* e *switching*.

b. Segmento de Distribuição

Este segmento agrega os equipamentos de acesso, minimizando o número de ligações diretas ao segmento *core*. Adicionalmente cria uma fronteira para falhas na Rede, constituindo-se como um ponto de isolamento lógico no caso de ocorrência de avarias em equipamentos no segmento de acesso. Neste nível são configurados parâmetros de Qualidade de Serviço (QoS) e de balanceamento de carga, bem como de facilidade de provisionamento.

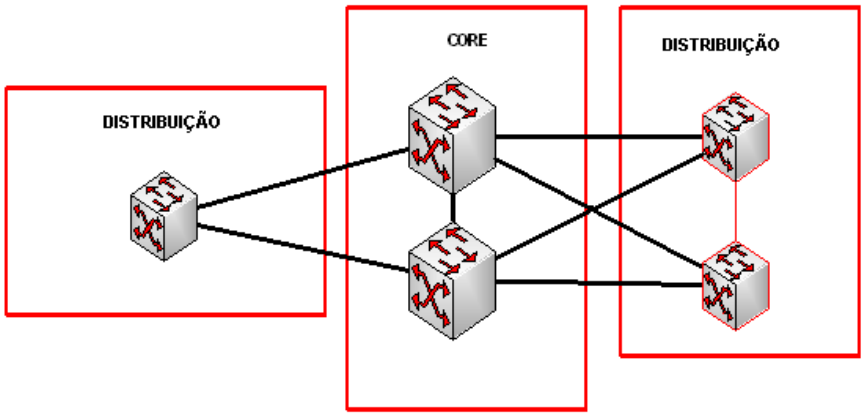

Figura 2-2 - Implantação de equipamentos de *Core* e Distribuição na Rede de Dados

c. Segmento de Acesso

O Segmento de Acesso constitui o ponto de entrada, em cada domínio da Rede, para equipamentos terminais como computadores, telefones IP, impressoras de Rede, terminais de videoconferência, sistemas de videovigilância e de controlo de acessos, etc. A marcação do tráfego deverá ocorrer neste nível.

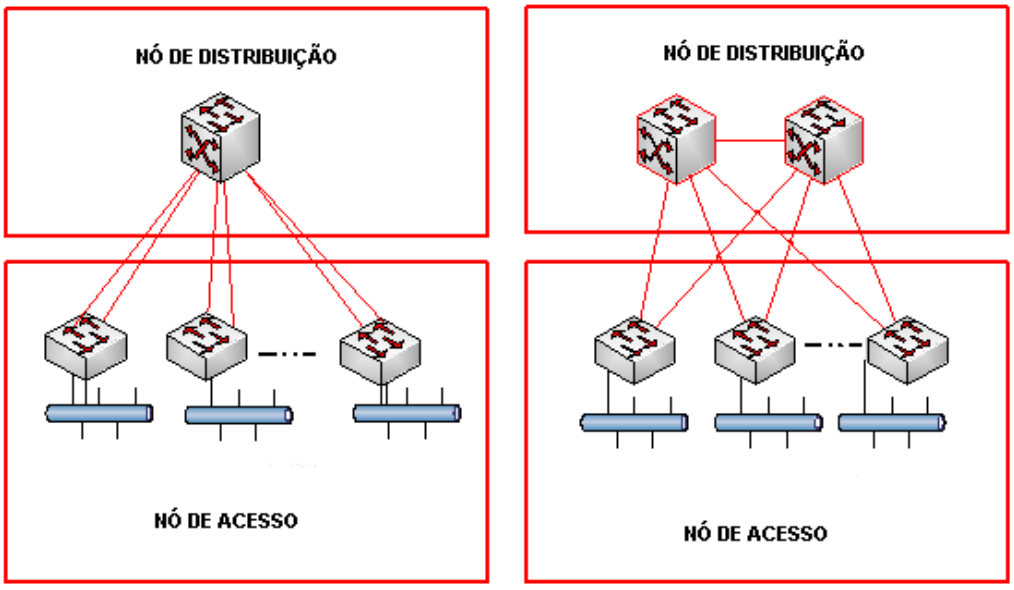

Figura 2-3 - Implantação de equipamentos de *Core* e Distribuição e Acesso na RDE

SECÇÃO IV – SISTEMA DE COMUNICAÇÕES TÁTICO

210. Enquadramento

O SIC-T foi desenhado para dar resposta à evolução do ambiente operacional e aos atuais e futuros cenários de empenhamento das Forças Operacionais do Exército. Neste novo ambiente operacional, torna-se fundamental a existência de redes robustas de comunicações que facilitem a ligação e a partilha de informação entre todas as entidades relevantes do espaço de batalha, constituindo a base para melhorar a colaboração entre todos os níveis organizacionais e melhorar a sincronização das ações militares. No âmbito estritamente militar, esta híper-conectividade entre todos os elementos do espaço de batalha, permite a partilha da perceção comum da situação operacional, conduz a um aumento da qualidade e rapidez na tomada de decisão, potenciando assim a capacidade de C2 que um Cmdt tem sobre as Forças à sua disposição.

O sistema de comunicações tático garante a ligação entre os Soldados no seu ambiente tático e entre as estruturas de Comando de uma Força. Permite também que esta estrutura de Comando tenha acesso, sem restrições, à informação necessária ao exercício do C2, dispondo de uma visão comum da situação operacional permanentemente atualizada, constituindo a base essencial para a criação e avaliação da compreensão da situação operacional.

211. Arquitetura do Sistema

O SIC-T tem por base uma infraestrutura de comunicações de natureza conjuntural e projetável, de geometria variável, adaptada ao emprego em campanha de Forças-Tarefa e que disponibiliza uma arquitetura modular e funcional, capaz de suportar um conjunto de serviços que percorrem de forma transparente os diversos módulos, subsistemas ou meios de transmissão, com o mínimo envolvimento do utilizador. Na ótica do utilizador, o sistema está orientado para uma federação de serviços, a disponibilizar em cada um dos escalões das Forças Operacionais. Cada escalão de Forças é apoiado por um ou mais módulos CSI projetáveis, com as valências que garantem o conjunto de capacidades consideradas necessárias ao exercício da capacidade de C2 nesse escalão de Força. Estas valências traduzem-se na disponibilização de serviços aos utilizadores, normalmente localizados num Posto de Comando (PC), mas também na garantia dos *links* de comunicações entre os diferentes níveis operacionais, ou pela constituição de uma estrutura malhada de Rede, baseada no conceito de apoio de comunicações de área para utilização em Operações convencionais. Na sua componente de comunicações, o

SIC-T subdivide-se em três subsistemas, cada um constituído por diferentes módulos sistémicos:

a. Subsistema de Área Estendida (SAE);

b. Subsistema de Área Local (SAL);

c. Subsistema de Utilizadores Móveis (SUM).

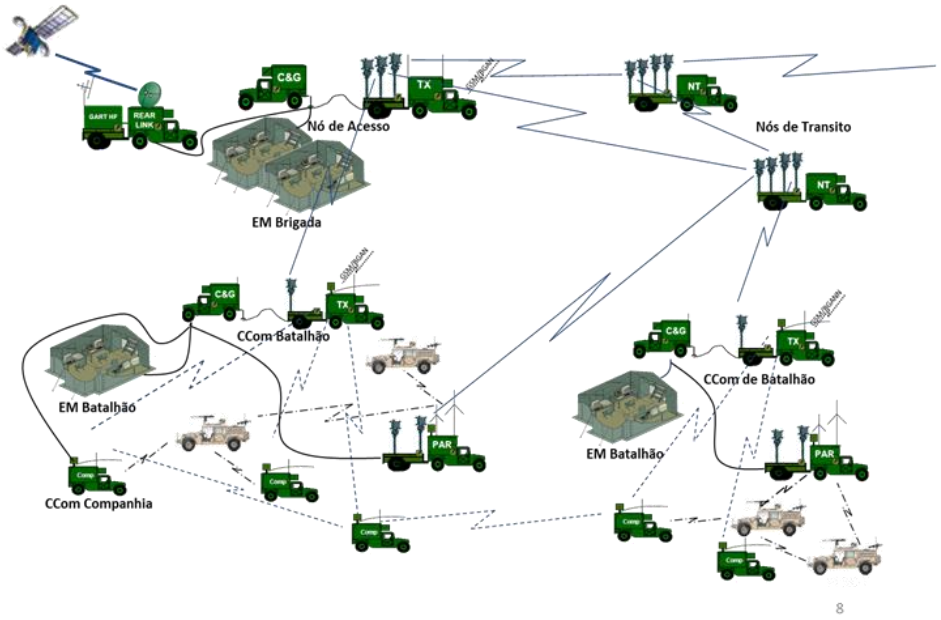

Figura 2-4 - Módulos de Comunicações no apoio a uma Brigada

Os módulos constituintes de cada subsistema disponibilizam serviços e possuem meios de transmissão específicos que concorrem para o propósito do subsistema respetivo. Contudo, de acordo com o conceito modular do SIC-T, todos os módulos possuem serviços e interfaces de Rede comuns como fibra e cobre, conferindo flexibilidade à topologia da Rede.

212. Subsistema de Área Estendida

O SAE constitui a espinha dorsal (*backbone*) da Rede, composto por um conjunto de nós de comutação interligados, fundamentalmente por ligações (*links*) rádio multicanal (FHz) ou, em casos específicos, com terminais de satélite de banda larga. O SAE integra os módulos:

a. Nó de Trânsito

O Nó de Trânsito (NT) destina-se a implementar um Nó da estrutura de Rede em malha que constitui a infraestrutura principal de comunicações do SIC-T. O NT baseia-se numa infraestrutura de FHz que garante o encaminhamento automático do fluxo de informação, através de um conjunto de ligações redundantes, capazes de assegurar a sobrevivência do sistema.

b. *Rear Link*

O *Rear-Link* (RL) destina-se a apoiar uma Força Operacional quando projetada, garantindo a integração da Força com a componente estrutural, quando tal não é possível com outros meios. Instalado junto ao PC da Força apoiada, garante a ligação à retaguarda (território nacional) através de ligação satélite de banda larga ou por ligação de dados em HF, utilizando protocolos de comunicação OTAN. Contudo, pode ser utilizado, embora com algumas limitações, para interligar via satélite dois nós de trânsito em Operações convencionais.

213. Subsistema de Área Local

O SAL destina-se a proporcionar a um determinado grupo de utilizadores, normalmente localizados num PC de um determinado escalão de Forças, as diversas categorias de serviços (voz, dados, C2, mensagens ou vídeo) disponíveis em cada domínio de informação e, adicionalmente, garante o acesso do PC apoiado à estrutura superior da Rede (SAE) através de um conjunto de nós de acesso. O SAL é materializado pelos módulos:

a. Nó de Acesso

O Nó de Acesso (NA) visa dotar os utilizadores dos PC de uma Unidade de escalão Brigada, com um conjunto de meios de CSI, necessários ao apoio da ação de C2 do respetivo Cmdt, possuindo meios de transmissão de FHz para ligação a outros módulos, por princípio ao SAE e a Unidades subordinadas (escalão Batalhão).

b. Centro de Comunicações de Batalhão

O Centro de Comunicações de Batalhão (CCB) procura dotar os utilizadores dos PC de uma Unidade de escalão Batalhão, com um conjunto de meios de CSI, necessários ao apoio da ação de C2 do respetivo Cmdt, possuindo meios de transmissão de FHz e de Rádio de Banda Larga[15] para ligação por princípio ao escalão superior (Brigada), a Unidades subordinadas (Companhia) e ao SUM.

c. Centro de Comunicações de Companhia

O Centro de Comunicações de Companhia (CCC) pretende dotar os utilizadores dos PC de uma Unidade de escalão Companhia, com um conjunto de meios de CSI, necessários ao apoio da ação de C2 do respetivo Cmdt. Os meios de transmissão do CCC são semelhantes aos do CCB, onde a ligação às Unidades subordinadas é baseada em RBL.

[15] O Rádio de Banda Larga (RBL) é um Meio de Comunicação rádio, que opera normalmente na banda VHF/UHF, fornece os serviços de dados e voz em simultâneo e estabelece a Rede entre RBL de forma dinâmica, do tipo *Mobile Ad Hoc Network* (MANET).

d. Módulos de Estado-Maior

Os Módulos de EM são constituídos por um conjunto de equipamentos terminais, necessários à montagem do PC do escalão respetivo. Materializa-se num conjunto de equipamentos tais como telefones, impressoras, computadores, projetores, etc. Este material é armazenado em caixas robustas, adequadas ao armazenamento e transporte por terra, ar e mar, conferindo a proteção adicional a estes equipamentos.

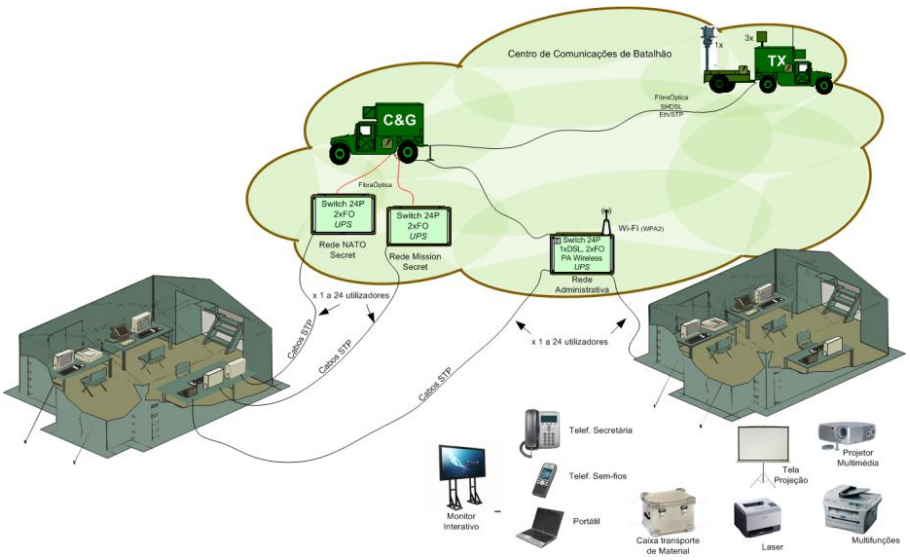

Figura 2-5 - Cenário de emprego do Módulo de Estado-Maior de Batalhão e respetivos equipamentos

(1) Módulo Estado-Maior de Brigada (EMBrig)

Conjunto de equipamentos destinados a equipar o EM de uma Brigada, de forma a dotar o Cmdt e os elementos do EMBrig com os meios necessários ao planeamento e execução das suas missões operacionais.

(2) Módulo Estado-Maior de Batalhão (EMBat)

Conjunto de equipamentos destinados a equipar o EM de um Batalhão, de forma a dotar o Cmdt e os elementos do EMBat com os meios necessários ao planeamento e execução das suas missões operacionais.

214. Subsistema de Utilizadores Móveis

O SUM pretende garantir os serviços de voz e dados aos utilizadores móveis profusamente disseminados pela Área de Operações que não possuam ligação ao SAL, o que implica comummente a utilização de meios de transmissão sem fios de propagação não diretiva. Porquanto, este subsistema integra os utilizadores móveis na Rede SIC-T através das Redes Rádio de Combate (*Combat Radio Nets* – CRN), nomeadamente através do módulo de comunicações Ponto de Acesso Rádio (PAR) que integra o SUM.

a. Ponto de Acesso Rádio

O PAR assegura a integração de utilizadores móveis na Rede de Comunicações Tática e a integração de sistemas de comunicações específicos que veiculem informação proveniente de sensores e outras fontes de informação digital ou analógica originada na Área de Operações. Com o fim de se ligar à restante Rede SIC-T, além das interfaces de ligação filares comuns a todos os módulos de comunicações, o PAR possui também meios de FHz. A integração com outros sistemas de comunicações rádio é conseguida através de *interfaces* próprias desses sistemas ou com recurso a equipamentos integradores específicos.

b. Redes Rádio de Combate

As CRN são redes de comunicações sem fios implementadas por rádios táticos que interligam diversas entidades, desde o Cmdt da Força até ao mais baixo escalão do combatente individual. São normalmente constituídas por rádios de várias tipologias, de acordo com as capacidades de comunicações que implementam e o escalão onde são empregues, nomeadamente: Rádio Multifuncional[16], RBL, Rádio de Baixos Escalões[17] e Rádio Individual[18].

A conceção das CRN procuram favorecer uma atuação mais independente dos utilizadores, não obstante permitirem a integração dos serviços de voz e dados na Rede tática, através dos Pontos de Acesso Rádio (PAR).

---

[16] O Rádio Multifuncional (RM), é a tipologia base usada nos escalões táticos das Forças terrestres, também designado por CRN, normalmente associado aos escalões Batalhão, Companhia e Pelotão, como o Meio de Comunicação utilizado entre os Cmdt destes escalões para a transmissão de ordens, coordenação da manobra, troca de informação sobre a perceção situacional comum e para atualização da imagem operacional comum (*Common Operational Picture* - COP). Esta tipologia de rádio, opera nas bandas H/V/UHF e implementa formas de onda seguras com o serviço de voz e serviço de dados (ainda que limitado), nas configurações de montagem fixa, veicular ou ligeira (*manpack,* transportado e operado pelo combatente apeado). O RM implementa formas de onda que cumprem os principais *standards* em fonia em claro. No Exército Português, o equipamento que atualmente desempenha esta função é o GRC-525.

[17] O Rádio de Baixos Escalões (RBE) ou Rádio Tático de Secção (RTS) é um equipamento do tipo *handheld* utilizado pelos Cmdt dos baixos escalões quando apeados (normalmente inferior a Batalhão) para transmissão de ordens, coordenação da manobra e troca de informação sobre a perceção situacional comum, com recurso a formas de onda seguras com serviço de voz e dados em simultâneo. Garante a ligação entre os combatentes e a sua estrutura de Comando, permitindo o acesso e atualização permanente da COP, como base essencial para a compreensão da situação operacional.

[18] O Rádio Individual (RInd) ou *Personal Role Radi*o (PRR) é o Meio de Comunicação utilizado pelo combatente apeado (normalmente ao nível da Secção por todos os Soldados e pelo seu Cmdt). Esta tipologia suporta os serviços de voz e dados pelo que os elementos equipados com o RInd também contribuem para a COP, através do fluxo de informação de georreferenciação entre os terminais.

Página intencionalmente em branco

CAPÍTULO 3 – SISTEMAS DE INFORMAÇÃO

SECÇÃO I – INTRODUÇÃO

301. Generalidades

Os SI são a segunda área nuclear da capacidade Superioridade de Informação. Ao contrário do sistema de comunicações, que é tendencialmente único, os SI são múltiplos, vocacionados para áreas funcionais distintas e para grupos de utilizadores específicos.

De acordo com estas premissas, os SI classificam-se em dois tipos: os SI de Gestão (SIG) e os SI para Operações (SIO). Ambos são acessíveis aos utilizadores através duma miríade de serviços essenciais e de tecnologias de informação.

Neste capítulo, apresentam-se os princípios e conceitos basilares desta área nuclear e distinguem-se os SIG, de nível estratégico e operacional, bem como os SIO, de nível operacional e tático.

302. Princípios dos Sistemas de Informação

O Cmdt de uma Força Terrestre para atingir os objetivos deve considerar e aplicar, em todas as fases de uma Operação ou Campanha, os princípios de SI. A correta aplicação destes princípios permite assegurar que os Sistemas possuem os elementos essenciais para o seu funcionamento eficaz numa ampla variedade de condições. Embora este parágrafo aborde estes princípios separadamente, podem estabelecer-se inter-relações entre os mesmos.

a. Fluxo de Informação

A gestão do fluxo de informação contempla a recolha, compilação, armazenamento, processamento, encaminhamento e relato da informação. O fluxo de informação é regulado através de relatos estruturados, relatórios e formatos de mensagens de texto *standards*, capacidades de precedência, atribuição de indicativos de chamada, indicadores de roteamento, minimização de procedimentos e outras medidas físicas e processuais.

No planeamento de uma Operação, os utilizadores dos SI devem identificar os seus requisitos de informação necessários para a condução dessa Operação. Esses requisitos de informação materializam-se em IER, necessários para o planeamento dos SI e da gestão da informação.

b. Interoperabilidade

Os objetivos gerais subjacentes às operações terrestres exigem que as estruturas de SI que habilitam o Comando das Forças Terrestres Nacionais e aliadas sejam normalizadas, tanto quanto possível de forma a atingir a interoperabilidade. Por ordem

crescente, os níveis de padronização são a compatibilidade, a permutabilidade e a uniformização. Os planos de SI devem assegurar que os requisitos essenciais de normalização de todas Forças Nacionais e aliadas são especificados. A eficácia das operações terrestres multinacionais exige SI interoperáveis que permitam ao Comando da Componente Terrestre e aos seus Cmdt subordinados o exercício do C2 eficaz entre os elementos da Força. Estabelecem-se os seguintes pré-requisitos para facilitar a interoperabilidade:

(1) Desenvolver um conceito SI conjunto para a Força;
(2) Harmonizar a informação, a semântica e desenvolver a gestão de dados;
(3) Disponibilizar e implementar acordos operacionais, procedimentos e normas técnicas;
(4) Partilhar informação e serviços com outros elementos da Força.

c. Flexibilidade

A flexibilidade deve garantir que os sistemas SI projetados possam responder às mudanças dos níveis de empenhamento, ao ritmo operacional e à postura da Força. A flexibilidade é necessária para responder a situações de mudança e à diversidade das Operações com o mínimo de perturbação ou atraso. Por exemplo, uma mudança de postura da Força, de manutenção para imposição da paz, pode resultar em pequenas alterações na estrutura da Força, que poderão resultar em requisitos SI consideravelmente diferentes. A flexibilidade é conseguida através dos seguintes fatores:

(1) Desenvolvimento e ensaio de planos de contingência;
(2) Uso de infraestruturas e sistemas comerciais;
(3) Existência de meios de reserva;
(4) Serviços e processos normalizados;
(5) Fazer uso de meios alternativos.

d. Redundância

É um elemento vital para a flexibilidade SI, pois garante os meios necessários para disponibilizar os serviços por sistemas e/ou equipamentos alternativos, o que aumenta significativamente a probabilidade de não disrupção dos SI.

e. Partilha da Informação

A partilha da informação permite o uso mútuo de serviços de informação ou partilha de recursos entre áreas funcionais (por exemplo: operacional, saúde, logística e financeira). Os requisitos de partilha de informação devem ser publicados para uma determinada comunidade de interesse e especificados nos IER. A partilha de

informação pode atravessar domínios funcionais e organizacionais, e até mesmo a fronteira da Rede. Por exemplo, no seio de uma Força Conjunta, a informação pode ser partilhada num *Common Operational Picture* (COP). Para efetivamente partilhar informação, devem ser claramente estabelecidas as regras e os regulamentos para anunciar, aceder e distribuir a informação. A ênfase deve ser colocada na "responsabilidade-de-partilha", balanceado com o princípio de segurança da "necessidade-de-saber". Estas regras e princípios devem ser geridos para facilitar o acesso, a partilha, a otimização, a reutilização, a redução e a duplicação da informação, de acordo com os princípios de segurança, legalidade e obrigação de privacidade.

f. Priorização

Os Cmdt e seus EM devem estar cientes que os SI necessários para apoiar uma Operação são aproximadamente proporcionais à escala da Operação. Todavia, devem também ser considerados outros fatores. Necessidade de uma capacidade mínima de meios de SI para suportar o Comando de uma Força Terrestre, ao nível do seu Cmdt, do PC e dos seus PC subordinados, independentemente do escalão da Força operacional empregue. Esta consideração torna-se importante quando existe o envolvimento simultâneo em várias Operações, mesmo de escala moderada. Em todas as Operações, há uma necessidade de estabelecer prioridades rigorosas para a alocação dos limitados recursos dos SI, incluindo largura de banda, com base nos IER e na intenção do Cmdt.

g. Resiliência

A disponibilidade, a permanência e a formação, são fatores que contribuem para a resiliência. A disponibilidade dos SI, devido ao papel crítico da informação armazenada e processada nos mesmos nas Operações, apresenta alta prioridade. Todavia, os meios de SI disponíveis e resistentes não são necessariamente resilientes sem pessoal devidamente treinado para os operar e gerir. A permanência é um elemento relevante da resiliência, alcançável através da redundância. Isto inclui a distribuição e a replicação dos SI e dos seus dados associados, mas também a proteção contra um ataque físico, eletrónico ou ambiental.

h. Capacidade

Embora a capacidade dos SI seja invariavelmente finita, os avanços tecnológicos aumentaram significativamente a capacidade de processamento e armazenamento dos mesmos. Para evitar atrasos no processo de decisão, devem ser tomados os necessários cuidados para garantir uma capacidade em SI adequada, para apoiar a

gestão e os requisitos de exploração da informação. Deve-se disponibilizar uma capacidade ajustada à procura previsível, mas podem sempre surgir situações operacionais em que limitações dos SI precipitam a adoção de diferentes estratégias da gestão da informação. Sempre que possível, tecnologias e procedimentos tais como a utilização de máquinas virtuais, sistemas de hiperconvergência ou *clusters* de dados, podem ser utilizadas para maximizar a capacidade.

i. Versatilidade

Capacidade das tecnologias de informação para integrar, na mesma infraestrutura, serviços comuns, serviços de controlo e gestão, dados e outros serviços indispensáveis ao funcionamento e fluidez da Informação.

303. Conceitos

a. Informação

É o conhecimento sobre objetos (por exemplo: factos, eventos, processos ou ideias e conceitos) que, dentro de um determinado contexto, têm um significado particular. As informações podem ser usadas na produção de informações, consciência da situação ou todo o tipo de dados (por exemplo: operacionais e logísticos) que precisam ser trocados durante uma Operação militar.

b. Sistema de Informação

Conjunto de equipamentos, métodos e procedimentos e, se necessário, pessoal, organizados para realizar processamento e armazenamento de informação.

c. Tecnologias de Informação

Equipamentos informáticos necessários para criar, processar, armazenar e recuperar informação em formato eletrónico, bem como converter dados eletrónicos em dados físicos e vice-versa. Incluem os seguintes componentes:

(1) Servidores de aplicações;

(2) Armazenamento (*storage*) e cópia de segurança (*backup*);

(3) Equipamentos clientes terminais (Computadores e *Thin Clients*[19]);

(4) Impressoras, scanners e equipamentos multifunções.

d. Centro de Sistemas Operacionais

Centro de Sistemas Operacionais (CSO) é a designação atribuída aos *data centers* do Exército. O CSO é o local onde estão residentes os serviços de informação comuns, os serviços de Rede, os serviços de comunicações, as aplicações, as bases de dados,

[19] *Thin Clients* – Clientes com funcionalidades básicas para funcionamento em ambientes virtualizados.

o armazenamento de informação e os sistemas de comunicações que asseguram a continuidade dos mesmos, e cujo modelo ideal obriga a uma disponibilidade permanente.

e. Serviços de rede

Os serviços de Rede constituem a componente base e vital para o eficaz funcionamento de todos os sistemas das redes de computadores (por exemplo RDE). Os serviços de Rede em produção na RDE são os seguintes:

(1) Distribuição automática de endereços IP (DHCP);
(2) Sincronização horária (NTP);
(3) Resolução de nomes (DNS);
(4) Qualidade de serviço (QOS);
(5) Distribuição automática de atualizações de *software* (WSUS);
(6) Segurança (Auditoria, distribuição e atualização do software antivírus);
(7) Serviços de diretoria e autenticação[20].

f. Serviços de informação comuns

Os serviços de informação comuns são os serviços disponíveis para utilização comum por todos os utilizadores dos sistemas integradores do Exército (SIC-Op e SIC-T):

(1) Sistemas de Correio Eletrónico e Transmissão de Mensagens;
(2) Sistemas Operativos (Servidores e Clientes);
(3) Sistemas de Portais;
(4) Virtualização;
(5) Sistemas de Controlo e Gestão de Redes e Serviços;
(6) Ferramentas de Produtividade (por exemplo *Office*).
(7) Bases de dados;
(8) Serviços de impressão;
(9) Serviços de armazenamento de ficheiros e de cópias de segurança (*backup*).

g. Controlo e Gestão de Redes e Serviços

(1) O controlo e gestão de SIC materializa-se através de um conjunto de ferramentas informáticas que permitem a realização de ações de sustentação, operação e controlo dos recursos de um sistema, para garantir a contínua operacionalidade dos serviços disponibilizados;
(2) A implementação de plataformas de gestão é uma necessidade transversal a todas as camadas da arquitetura dos SIC do Exército e possibilita a monitorização

[20] Diretório de informação e gestão relativa a utilizadores, recursos, políticas de segurança, e todo e qualquer tipo de objetos definidos por utilizadores.

e diagnóstico de falhas, a configuração e a realização de medições de desempenho dos vários equipamentos, redes e sistemas, garantindo o fornecimento de serviços SIC de alta qualidade;

(3) As ações de Gestão estão agrupadas em quatro áreas funcionais:

(a) Gestão de Falhas

Engloba a deteção, análise, isolamento e a respetiva correção de falhas/avarias que causam anomalias no funcionamento dos equipamentos, das redes e dos serviços disponibilizados.

(b) Gestão de Configuração

Engloba a identificação, controlo, recolha e envio de dados para equipamentos, redes e sistemas para a inicialização, funcionamento contínuo e garantia de interligação de serviços.

(c) Gestão de Desempenho

Engloba a avaliação do comportamento e eficácia do funcionamento dos equipamentos, redes e sistemas.

(d) Gestão de Segurança

Tem como objetivo apoiar a aplicação de políticas de acesso às plataformas de gestão através de funcionalidades que incluem a criação, eliminação e controlo de utilizadores e do nível de serviços de gestão associados, a distribuição de informação de segurança pertinente e a notificação de eventos de segurança relevantes no âmbito dos sistemas de gestão de Rede e serviços.

SECÇÃO II – SISTEMAS DE INFORMAÇÃO DE GESTÃO

304. Enquadramento

Os SIG são compostos pelas plataformas que operam dados em grandes volumes com o propósito de apoiar o Cmdt/Dir/Ch nas suas decisões, na publicação e divulgação da imagem do Exército e na divulgação interna.

Os SIG podem dividir-se em níveis de aplicação conforme os conteúdos: Os SIG de nível Estratégico e os SIG de nível Operacional.

305. Sistemas de Informação de Gestão de nível Estratégico

Os SIG de nível estratégico têm como objetivo último cumprir com os objetivos estratégicos da organização, abrangem áreas transversais aos diferentes organismos do Ministério da Defesa e da estrutura superior das Forças Armadas, bem como a partilha

de dados com essas entidades, vocacionados para os assuntos de pessoal, de logística e financeiros, com capacidade de produção de relatórios integrados para apoio à decisão nestas áreas (por exemplo: Sistema Integrado de Gestão da Defesa Nacional, Sistema de Avaliação do Mérito dos Militares das Forças Armadas).

306. Sistemas de Informação de Gestão de nível Operacional

Os SIG de nível operacional têm como objetivo último cumprir com os objetivos do Exército, abrangendo áreas transversais às diferentes U/E/O do Exército, vocacionados para os assuntos de pessoal, de logística e financeiros, com capacidade de produção de relatórios integrados para apoio à decisão nestas áreas (por exemplo: *dashboards* de *Business Intellingence*, Portal Pessoal).

SECÇÃO III – SISTEMAS DE INFORMAÇÃO PARA OPERAÇÕES

307. Enquadramento

Os SIO ou Sistemas de Informação para o C2 (SIC2) são compostos pelas plataformas que operam dados com o propósito de apoiar os Órgãos de Comando nas suas decisões em exercícios e operações.

Os SIO orientam-se pelo princípio da superioridade de informação, constituindo-se como a base da cadeia de valor de uma Força centrada em Rede, de forma a aumentar a velocidade da tomada de decisão, com o objetivo de garantir um aumento contínuo das capacidades e uma maior eficácia no cumprimento da missão.

Os SIO podem dividir-se em níveis de aplicação conforme os conteúdos: SIO de nível Operacional e SIO de nível Tático. Embora os SIO possam ser divididos no nível de aplicabilidade, não são, porém, independentes. A sua integração e partilha de informação garantem uma maior qualidade da informação que veiculam, podendo existir uma relação hierárquica entre os vários sistemas que corresponde ao fluxo de informação entre os vários escalões. A figura 3-1 demonstra a relação hierárquica de SIC2, num contexto de Operações ao nível tático, ilustrando a complexidade crescente em consonância com a ascensão do escalão de emprego.

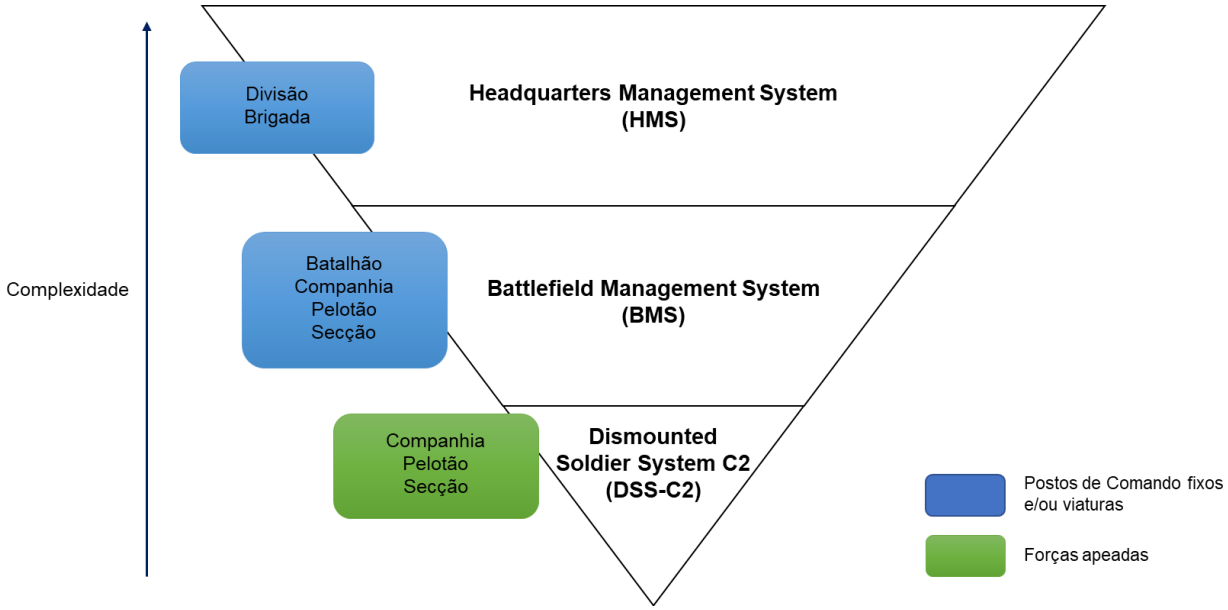

Figura 3-1 - Hierarquia dos SIC2 num contexto de Operações

308. Sistemas de Informação para Operações de nível Operacional

Os SIO de nível Operacional têm como objetivo último apoiar a decisão ao nível tático (Comando de Componente, Comando de Grandes Unidades [GU]) bem como permitir a partilha de informação com o Comando de nível operacional (por exemplo: *Headquarters Management System* [HMS], *Tool for Operational Planning, Force Activation and Simulation, Logistic Functional Area Services, The Interim Geo-Spatial Intelligence Tool*).

309. Sistemas de Informação para Operações de nível Tático

O SIO Tático tem como objetivo último o controlo das Forças em Exercícios ou Operações, bem como a partilha de informação entre Pequenas Unidades, as GU e Comando de Componente, englobando desde os mais baixos escalões (Soldado apeado) até ao Comando de Componente.

A informação contida nos SIO Táticos será preferencialmente para consumo interno das Unidades e baseado em protocolos simples com mensagens curtas, para serem veiculadas em ambientes com larguras de banda limitadas.

Como exemplo destes sistemas, temos o *Battlefield Management System* (BMS), *Advanced Field Artillery Tactical Data System*, *Dismounted Soldier System*-C2 (DSS-C2), *Torch*, entre outros.

CAPÍTULO 4 – GUERRA DE INFORMAÇÃO

SECÇÃO I – INTRODUÇÃO

401. Generalidades

O conceito de “Guerra de Informação” expressa, acima de tudo, a ideia de conflito e a posição que a informação ocupa neste contexto. Considera-se que é uma guerra que ocorre essencialmente no Ciberespaço, mas é sobretudo uma guerra de ideias. A informação é um dos domínios do ambiente operacional que molda o ambiente, influenciando os líderes, os decisores, os indivíduos e as organizações, pelo que todos os Cmdt utilizam a informação para moldar o ambiente operacional como parte das suas Operações. O ambiente de informação tem assumido uma importância crescente, fruto das dinâmicas de poder geradas no Ciberespaço e a partir dele. O Exército deverá ser capaz de extrair o valor decorrente de uma utilização cada vez mais coerente, integrada e segura do ambiente de informação. O objetivo passa por obter superioridade de informação, através da implementação de uma capacidade de GE, de Ciberdefesa, de medidas que garantam a segurança dos sistemas e tecnologias de informação e que assegurem a pronta resposta e investigação de incidentes.

Neste capítulo, apresentam-se sob o chapéu da GI, os conceitos, princípios e respetiva articulação operacional das áreas de atividade relacionadas com a Segurança dos SIC, das operações no Ciberespaço (OpsCiber) e da GE. As operações de Informação (INFO OPS), embora brevemente abordadas, não são tratadas nesta publicação.

402. Princípios da Guerra de Informação

Garantir a superioridade no Ciberespaço, bem como no espetro eletromagnético permite uma vantagem decisiva aos Cmdt a todos os níveis no moderno campo de batalha. Deste modo, o Cmdt e respetivo EM conduzem atividades ciber/eletromagnéticas (CEMA)[21] para projetar poder no, e através do Ciberespaço e na globalidade do espetro eletromagnético. A execução das CEMA permite ao Exército proteger e defender as redes de Forças Amigas e proteger pessoal, instalações e equipamentos. Deste modo, as CEMA representam o processo de planeamento, integração e sincronização das OpsCiber e da GE em apoio às operações terrestres. Dependendo do escalão da Força, poderão ser constituídas equipas CEMA, organizadas para a missão, a atuar de forma unificada. Contudo, importa também distinguir claramente entre os recursos Ciber e os recursos de GE, pois permite que cada um opere separadamente e ofereça apoio às

[21] Da terminologia inglesa: CEMA – *Cyberspace ElectroMagnetic Activities*

Operações de forma distinta. Nesse caso, isso também requer esforços de sincronização para evitar interferências indesejadas.

O rápido avanço e desenvolvimentos no Ciberespaço e no espaço eletromagnético desafiam qualquer suposição de vantagem do Exército neste domínio. Embora seja possível a defesa contra diversos tipos de intrusão, o Exército deve tomar medidas para identificar, priorizar e defender as suas redes e dados mais importantes. Os Cmdt e especialistas em OpsCiber devem também se adaptar de forma rápida e eficaz à presença do adversário/inimigo dentro dos nossos sistemas.

Constituindo a informação um domínio transversal a todas as atividades das Forças Armadas, e em particular no Exército, é importante a existência de uma visão de 360º do ambiente de informação, capaz de explorar sinergias e evitar esforços descoordenados que se possam traduzir numa resultante nula ou negativa. As atividades conduzidas no domínio da informação podem ser de apoio (CSI) ou assumirem um papel central no combate (GI), caracterizando-se este como um domínio em que decorrem operações de ataque e defesa, destinadas a proteger os sistemas de C2 das Forças Amigas e a afetar os de potenciais adversários. Assim, o ambiente de informação deve ser perspetivado de forma:

a. Multidimensional

Respeitando o modo como se estruturam os recursos de informação (Sinais, Dados, Informação, Conhecimento e Sabedoria) e se perspetivam os diferentes níveis em que tem lugar a sua utilização (Físico, Sintaxe e Semântico).

b. Flexível

Atendendo à especificidade estrutural e funcional dos sistemas que intervêm no apoio CSI e das várias componentes que permitem moldar o domínio da Informação, de maneira a garantir, na máxima extensão possível, a sua utilização tanta numa situação de Paz como de Campanha.

c. Integrada

Potenciando a exploração do valor da informação (recurso/arma) de forma a promover uma correta sincronização entre o apoio CSI e as atividades ligadas à GI;

d. Coerente

Promovendo uma visão global do ambiente de informação que permita perspetivar como se articulam e integram (horizontal e verticalmente) as diversas componentes e explorar sinergias de forma a facilitar o emprego de capacidades e a aumentar a sua eficácia individual e agregada.

403. Conceitos

a. Ambiente de Informação

O ambiente de informação é o espaço físico e virtual onde a informação é recebida processada e tratada. Consiste na informação em si e no conjunto de processos e SI. Pode ser entendido segundo três dimensões e a sua relação entre elas:

(1) Dimensão cognitiva (psicológica)

É onde a informação é interpretada, apreendida e as decisões são tomadas. Baseia-se em crenças, motivações, emoções, moral, educação, ideologias, etc. É centrada na natureza humana.

(2) Dimensão virtual

É onde a informação é recolhida, processada, armazenada, disseminada e protegida. Baseia-se em conteúdos e fluxos. É centrada nos dados.

(3) Dimensão física

É onde a informação está disponível, nomeadamente nas redes e Sistemas de C2. É a dimensão tangível (“mundo real”) onde assenta todo o ambiente de informação, o espaço onde as atividades físicas ocorrem e os indivíduos, os estados, as nações, as culturas e as sociedades interagem.

b. Guerra de Informação

A GI é um termo utilizado para a ameaça do uso orquestrado de atividades de informação (tais como OpsCiber, GE, etc.) para obter vantagem no ambiente da informação. Não é uma capacidade por si própria, mas sim um conjunto de capacidades/valências, integradas e coordenadas, com vista a um objetivo último: obter a superioridade de informação. A condução destas atividades pode ser entendida tanto ao nível do patamar Estratégico, uma vez que englobam atividades de cariz político e diplomático, como ao nível Operacional e Tático da condução das Operações. Deste modo, pode definir-se a GI como o conjunto de ações desenvolvidas para obter a superioridade de informação, afetando a informação, processos baseados em informação, SI e redes baseadas em computadores de um adversário, enquanto se defende a nossa informação, processos baseados em informação, SI e redes baseadas em computadores.

Já relativamente às INFO OPS estas podem ser entendidas como o emprego integrado, durante as operações militares, de capacidades relacionadas com a informação, coordenado com outras linhas de operações para influenciar, desorganizar, corromper ou usurpar o processo de decisão de adversários efetivos ou potenciais, protegendo simultaneamente o nosso.

Na figura 4-1 podem observar-se as três diferentes dimensões do ambiente de informação, alinhadas com a designada "pirâmide cognitiva" que é construída a partir dos seus níveis de abstração (sinais, dados, informação, conhecimento e sabedoria) e onde se desenvolvem algumas das áreas relacionadas com a GI: OpsCiber, GE e INFO OPS.

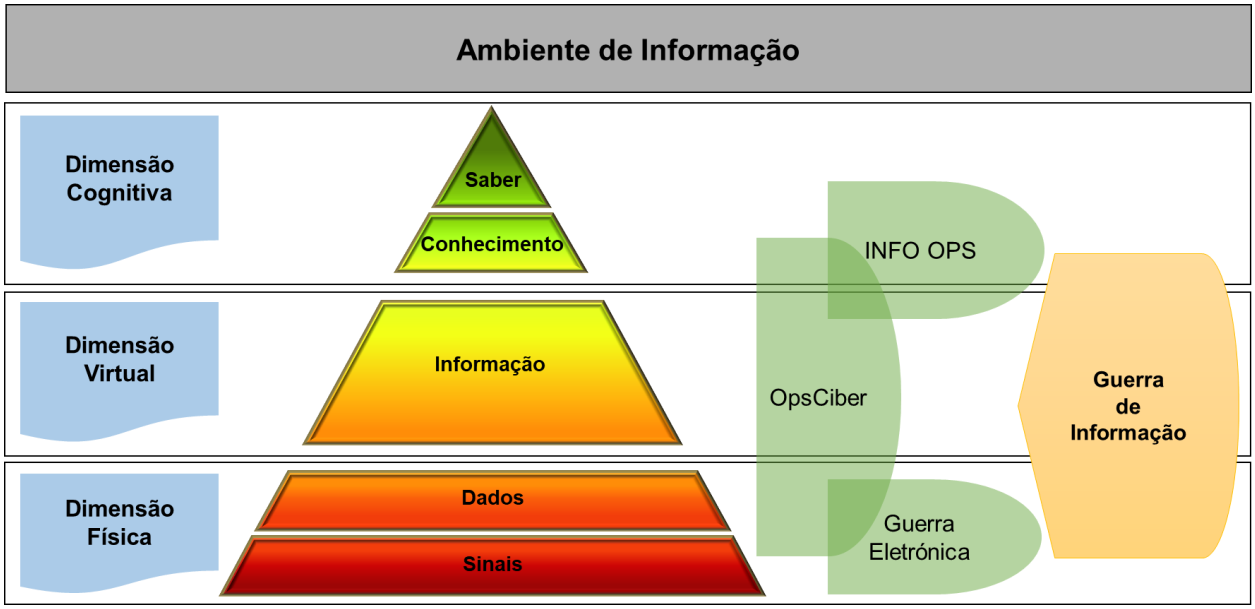

Figura 4-1 - O ambiente de informação

É, pois, a capacidade de atingir e manter a superioridade de informação que permite moldar o ambiente de informação, potenciando a realização de outras ações com vista a alcançar os efeitos pretendidos sobre um determinado adversário.

c. Garantia da Informação

A garantia da informação (*Information Assurance*) é o conjunto de medidas destinadas a alcançar um determinado nível de confiança na proteção da comunicação, da informação e de outros sistemas eletrónicos, não eletrónicos, bem como da informação que é armazenada, processada ou transmitida nesses sistemas com respeito à confidencialidade, integridade, disponibilidade, não-repúdio e autenticação. A aplicação de medidas de segurança para a proteção desses sistemas constitui o que se designa por Segurança SIC [22].

No entanto, além da garantia da informação importa ter em consideração o conceito de garantia do cumprimento da missão (*Mission Assurance*) como objetivo último relevante no contexto das operações militares.

[22] '*CIS Security'* na terminologia OTAN, anteriormente designado por INFOSEC.

d. Ciberespaço e Espetro Eletromagnético

No atual ambiente operacional, o Ciberespaço e o espetro eletromagnético são cada vez mais relevantes, podendo assumir-se como críticos para o sucesso, em virtude da tecnologia utilizada, quer pelas nossas Forças, quer pelo adversário, no âmbito do C2, da recolha de informação, da compreensão situacional e na aquisição de objetivos. Conseguir manter a superioridade no Ciberespaço e no espetro eletromagnético, garante uma clara vantagem em relação aos adversários. Por outro lado, a condução de OpsCiber e GE pelas nossas Forças, limita as modalidades de ação do adversário/inimigo, degradando o seu C2 e a capacidade de operar nos outros domínios.

O Ciberespaço é, evidentemente, um dos domínios das Operações e que utiliza parte do espetro eletromagnético, como por exemplo o *Bluetooth*, *Wi-Fi* e as Comunicações Satélite. Por isso, as OpsCiber e a GE necessitam de uma coordenação estreita, efetuada no âmbito da gestão do espetro eletromagnético. Deste modo, a efetiva utilização das OpsCiber e da GE requer por parte das Forças Terrestres a condução de CEMA. Estas atividades empregam uma abordagem de Armas Combinadas para as Operações, no domínio do Ciberespaço e no espetro eletromagnético, que por norma, é muito congestionado no moderno campo de batalha. As CEMA destinam-se a conquistar, reter e explorar as vantagens no Ciberespaço e no espetro eletromagnético. O resultado destas atividades permite às Forças militares manter a liberdade de ação e negar a liberdade de ação ao adversário/inimigo, contribuindo globalmente para o sucesso da Operação.

SECÇÃO II – ÁREAS DE ATIVIDADE

404. Segurança dos Sistemas de Informação e Comunicações

A Segurança SIC é a aplicação de medidas de segurança para a proteção de sistemas de comunicações, informação e outros sistemas eletrónicos, e da informação que é armazenada, processada ou transmitida nesses sistemas em matéria de confidencialidade, integridade, disponibilidade, autenticação e não-repúdio.

Este conceito, aplica-se a todas as fases do ciclo de vida de um SIC, desde a sua conceção até ao seu abate. Os aspetos de segurança condicionam sempre as soluções a implementar e têm impacto no seio da organização e fora da mesma. O planeamento dos mecanismos de segurança de um SIC envolve sempre uma forte coordenação entre o utilizador final do sistema, as entidades com responsabilidade de implementação e operação do SIC e a estrutura de acreditação do mesmo. Por outro lado, os utilizadores

dos SIC devem estar credenciados e autorizados a ter acesso, com base na necessidade de conhecer e de acordo com o grau de classificação de segurança da informação neles armazenada, processada ou transmitida.

Portanto, a segurança SIC rege-se por normas e procedimentos bem definidos, pelas diversas autoridades nesta matéria, que que devem fazer parte da formação e treino de todos os potenciais utilizadores do respetivo SIC.

a. Acreditação e Auditorias de Segurança

Como parte do processo de planeamento e acreditação de um SIC, certos elementos do *hardware*, *firmware* e/ou *software* carecem de ser avaliados e certificados. O processo de avaliação e certificação basear-se-á em critérios definidos pela Autoridade de Acreditação de Segurança (SAA), autoridade a quem compete a acreditação dos SIC. Estes processos de avaliação formal visam garantir que elementos específicos dos SIC são robustos e que quaisquer vulnerabilidades de segurança são devidamente geridas, e que as funcionalidades de segurança de determinado produto ou dispositivo atendem a normas específicas.

As auditorias de segurança desempenham um papel vital para garantir que os SIC continuam em conformidade com a legislação aplicável, normas técnicas e documentação de segurança específica do SIC. Todos os SIC que processem informação classificada estão sujeitos a auditorias de segurança periódicas por parte da SAA apropriada ou dos órgãos de inspeção competentes, eventualmente apoiados por outras entidades especializadas. Nas auditorias de segurança deverá ainda ser utilizado o Teste de Segurança e o Plano de Verificação de cada SIC para garantir a conformidade com os seus requisitos específicos.

b. Gestão de Riscos de Segurança

O processo de gestão de risco nos SIC deve ser aplicado para monitorizar, reduzir, eliminar, evitar ou aceitar os riscos. Deste modo, devem ser implementadas medidas de segurança de acordo com a análise de risco efetuada previamente e aprovadas pela SAA. Em contexto, operacional cabe ao Cmdt/Dir/Ch a decisão de aceitar ou não determinados riscos nas suas redes de C2, devendo estes riscos ser levantados e integradas no processo tomada de decisão militar. Contudo, no contexto de federação de redes, há que ter em conta os riscos que podem advir para redes terceiras, uma vez que as vulnerabilidades de uns podem afetar os restantes.

Os Cmdt/Dir/Ch podem controlar os riscos resultantes conduzindo ações de mitigação da ameaça, medidas de recuperação após o impacto, prioridades defensivas claras,

meios de comunicação alternativos e redundantes, bem como outras medidas para cumprir a sua missão e garantir a fiabilidade dos dados críticos.

c. Segurança Criptográfica

Cabe aos respetivos Cmdt/Dir/Ch, que tenham material cripto para uso nos SIC que exploram, a nomeação formal de custódios cripto para garantir o estrito controlo e salvaguarda desse material, que é crítico para a segurança do sistema e consequentemente para própria missão. Nesse sentido, o apoio logístico do material criptográfico assenta num canal próprio e diferenciado, que é o da cadeia de custódios de material cripto. Em tempo de paz, o custódio de material cripto do Exército é um Oficial ao qual incumbem todas as providências necessárias para a produção, aquisição, distribuição, transferência, transporte, registo, guarda, existência, conservação, reparação e utilização do material cripto distribuído ao Exército. Do mesmo modo, em Operações ou Exercícios deverá ser estabelecida uma Cadeia de Custódios de material cripto que garanta as salvaguardas especiais para proteger este material, conforme as normas e publicações em vigor.

405. Operações no Ciberespaço

a. O Ciberespaço é um domínio das Operações que está totalmente contido no ambiente de informação. É por isso, um meio através do qual as capacidades relacionadas com a informação podem ser empregues. As OpsCiber são operações militares que, no, ou através do, Ciberespaço, delimitadas no tempo e no espaço e através do emprego de capacidades de Ciberdefesa, se destinam a atingir objetivos militares.

b. As OpsCiber, bem como outras atividades e capacidades de informação, criam efeitos no ambiente de informação em apoio às operações conjuntas, sendo principalmente planeadas e conduzidas ao nível operacional. Embora seja possível para as OpsCiber produzirem efeitos táticos, operacionais ou estratégicos de forma autónoma e desta forma atingir os objetivos, os Cmdt integram as OpsCiber noutras Operações para criar efeitos coordenados e sincronizados, necessários para sustentar o cumprimento da missão. Assim, a existência de um órgão de Ciberdefesa no EMGFA destina-se a assegurar o exercício do Comando de operações militares no, e através do Ciberespaço, pelo Chefe de Estado-Maior General das Forças Armadas (CEMGFA), garantindo a sincronização das OpsCiber com as Operações nos outros domínios.

c. Ao nível do Exército, as OpsCiber são executadas por elementos/Unidades especializadas em OpsCiber que poderão ser orgânicas ou atribuídas aos Cmdt táticos para emprego numa determinada missão. Contudo, a produção de efeitos no, e

através do Ciberespaço (medidas ativas), deverá ser sempre coordenada e validada ao nível operacional.

d. As OpsCiber podem ser de vários tipos, consoante apliquem medias passivas ou ativas, e se desenrolem nos nossos sistemas em sistemas neutros ou do adversário (figura 4-2):

(1) Operações da Infraestrutura de Comunicações e Sistemas de Informação (CISIO);

(2) Operações Defensivas no Ciberespaço (DCO), que se subdividem em Medidas Defensivas Internas (DCO-IDM) e Ações de Resposta (DCO-RA);

(3) Operações de Informações, Vigilância e Reconhecimento no Ciberespaço (CISRO);

(4) Operações Ofensivas no Ciberespaço (OCO)[23].

e. As CISRO são coincidentes com o conceito de Segurança SIC, já apresentado anteriormente, e estas devem ser perfeitamente integradas nas Unidades de exploram os meios CSI, como seja e Batalhão de Transmissões.

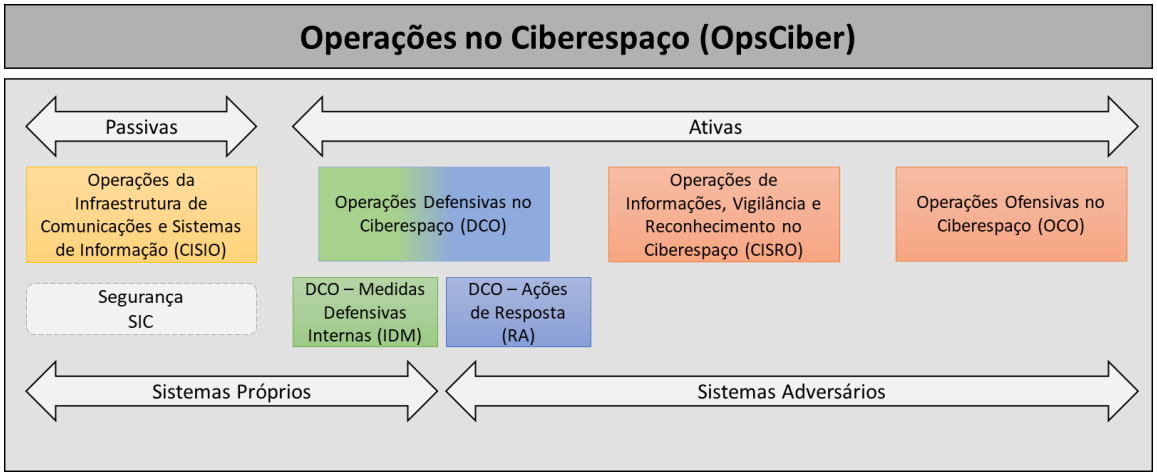

Figura 4-2 - As operações no Ciberespaço

f. Relativamente às DCO, estas são Operações executadas para preservar e/ou restaurar a capacidade de utilizar o Ciberespaço e proteger os dados, redes e SI. Deste modo, no âmbito das Forças Terrestres, a condução de OpsCiber defensivas visa:

(1) Assegurar a proteção aos SIC-T que asseguram a capacidade de C2 da Força;

[23] Na terminologia inglesa:
OCO – Offensive Cyberspace Operations
DCO – Defensive Cyberspace Operations
CISRO – Cyberspace Intelligence, Surveillance and Reconnaissance Operations
CISIO – Communication and Information Systems Infrastructure Operations

(2) Analisar vulnerabilidade e riscos associados às infraestruturas de comunicações táticas e aos SI, apoiando o Cmdt no processo de tomada de decisão.

g. Por sua vez, as CISRO e as OCO, podendo eventualmente vir a ser conduzidas por Forças Terrestres, estas são planeadas ao nível do órgão conjunto de Ciberdefesa das Forças Armadas.

406. Guerra Eletrónica

a. Como apresentado anteriormente, as OpsCiber e a GE são presentemente pilares essenciais da condução de operações terrestres. O Ciberespaço usa porções do espectro eletromagnético pelo que estas operações exigem atribuição, gestão de frequências e coordenação. Concorrentemente, os Cmdt deverão fazer um uso sinérgico destas capacidades com uma abordagem de armas combinadas, que lhes permita maximizar a exploração do espectro eletromagnético. As atividades no Ciberespaço e Eletromagnéticas, isto é, as CEMA, compreendem o processo de planeamento, integração e sincronização das OpsCiber e de GE em apoio das Operações da componente terrestre.

b. Num sentido mais lato, a GE refere-se à ação militar envolvendo o uso de energia eletromagnética e direcionada para controlar o espectro eletromagnético ou para atacar o adversário/inimigo. As capacidades de GE permitem que as Forças Terrestres criem condições e efeitos no espectro eletromagnético para apoiar a intenção do Cmdt e às Operações, negando a sua utilização ao adversário/inimigo.

c. A proliferação de novas tecnologias e a forma como as Operações são conduzidas no seio das alianças internacionais às quais Portugal pertence, levaram a que o centro de gravidade da GE passasse do espectro e gestão de frequências para um novo conceito mais abrangente de Operações no espectro eletromagnético como já referido anteriormente. Este compreende várias vertentes que atuam no espectro eletromagnético, sendo a GE considerada disciplina de combate.

d. Atualmente todas as Forças modernas conduzem Operações fazendo uso de equipamentos que recorrem ao uso do espectro eletromagnético de forma intensiva e permanente, ele próprio já saturado pela utilização de equipamentos de organizações civis e militares imersas no ambiente operacional. Estes equipamentos executam funções no âmbito de: vigilância, comunicações, georreferenciação, recolha de informações, C2, infraestruturas civis, transmissão de dados, etc. Assim, é responsabilidade dos Cmdt, modelar o espectro eletromagnético em seu proveito impedindo a sua utilização por Forças hostis, explorar o espectro eletromagnético em apoio às Operações e garantir a integração aos mais diferentes níveis, estratégico,

operacional e tático as ações no espectro eletromagnético no planeamento operacional.

e. A figura 4-3 ilustra de que forma se articulam os efeitos eletromagnéticos, ações, medidas e tarefas da GE na visão doutrinária atual, e que tem sido adotada como referência para o desenho das capacidades em edificação, bem como na elaboração de documentação doutrinária. Uma leitura atenta do quadro permite-nos perceber a transposição realizada da anterior catalogação dos diferentes domínios de atuação da GE tendo por base a tipologia das ações conduzidas (Medidas de Apoio Eletrónico, Medidas de Proteção Eletrónica e Contra Medidas Eletrónicas), para uma nova abordagem em que são planeadas e realizadas ações tendo como objetivo a produção de determinados efeitos.

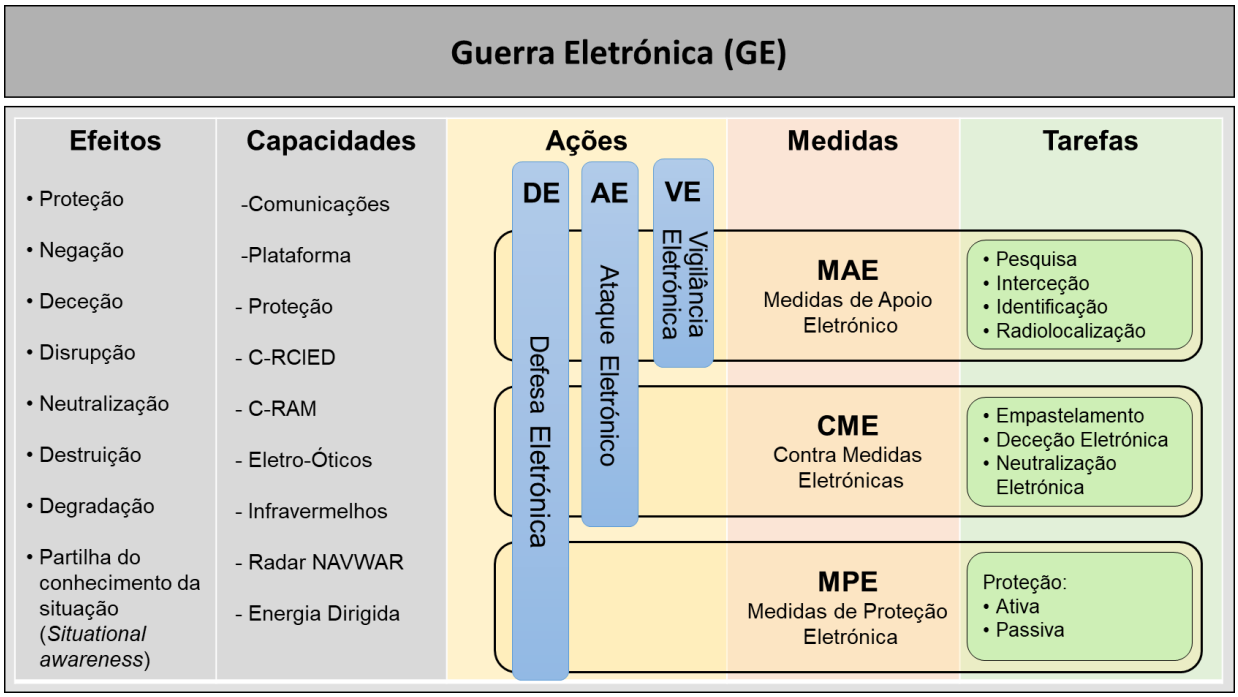

Figura 4-3 - A Guerra Eletrónica

f. Após selecionado o efeito que determinado Cmdt deseja ver produzido no ambiente operacional em que a sua Força está imersa, é possível tendo por referência as Capacidades base, percorrer as ações Defesa Eletrónica (DE), Ataque Eletrónico (AE) e Vigilância Eletrónica (VE) e as Medidas de Apoio Eletrónicas (MAE), Contra Medidas Eletrónicas (CME) e as Medidas de Proteção Eletrónica (MPE), e identificar quais as tarefas que deverão ser realizadas para o atingir.

(1) Medidas de Apoio Eletrónico

Ações tomadas para pesquisar, intercetar e identificar as emissões eletromagnéticas e para radiolocalizar as suas fontes, com o objetivo de

reconhecimento de ameaças imediatas. Fornecem informações necessárias para aplicação de contramedidas eletrónicas, medidas de proteção eletrónica e outras ações táticas. Caracterizam-se por: fornecerem informação sobre as intenções da Força Opositora e explorar as suas emissões; apoiar na recolha de Informação; apoiar as operações de CME; contribuir para o planeamento de ações de deceção. As MAE contemplam as seguintes tarefas:

(a) Pesquisa

Varrimento do espectro eletromagnético, na gama de interesse, com o objetivo de determinar a sua ocupação. A pesquisa subdivide-se em geral, dirigida e vigilância, de acordo com o grau de conhecimento de emissões existentes por parte do operador;

(b) Interceção

Receção e registo de emissões eletromagnéticas por parte de entidades que não os destinatários pretendidos;

(c) Identificação

Associação de todo um conjunto de informação técnica e tática com o objetivo de determinar que Unidade/Entidade adversária corresponde ao emissor alvo. A identificação poderá ser de índole tática ou técnica, consoante o conteúdo da informação;

(d) Radiolocalização

Determinação aproximada das coordenadas de um emissor, subdivide-se em aérea, tática e estratégica consoante a plataforma utilizada;

(2) Contra Medidas Eletrónicas

Ações tomadas para impedir ou degradar a utilização eficaz do espectro eletromagnético pela Força Opositora, através do uso de energia eletromagnética. Têm como objetivo primário retirar à Força Opositora, a confiança nos seus sistemas eletrónicos, limitando-lhe a sua prontidão e capacidade de resposta e ainda provocando desgaste e desmoralização. As CME contemplam as seguintes tarefas:

(a) Empastelamento

Consiste na deliberada irradiação, re-radiação ou reflexão de energia eletromagnética com o objetivo de prejudicar o uso eficaz de dispositivos, equipamentos ou sistemas eletrónicos, pela Força Opositora;

(b) Deceção

Deliberada radiação, re-radiação, alteração, absorção ou reflexão de energia eletromagnética de modo intencional para confundir, distrair ou seduzir a Força Opositora ou os seus sistemas eletrónicos;

(c) Neutralização Eletrónica

Uso deliberado da energia eletromagnética para danificar temporária ou definitivamente os dispositivos opositores que dependem exclusivamente do espectro eletromagnético.

(3) Medidas de Proteção Eletrónica

Compreende as ações que garantam a utilização eficaz do espectro eletromagnético pelas Nossas Forças, apesar deste também ser utilizado pela Força Opositora. As MPE podem ser de natureza ativa (alteração da frequência, alteração dos parâmetros do emissor, espalhamento espectral, transmissão em rajada, salto de frequência, encriptação, alteração da modulação e alteração da potência de emissão.

SECÇÃO III – ARTICULAÇÃO OPERACIONAL

407. Planeamento

Os Cmdt devem integrar as atividades relacionadas com a GI nas operações terrestres, sempre que assim seja possível. Deste modo, como parte do planeamento, deverão ser desenvolvidos estudos adequados e respetivos documentos para integrar os Planos e Ordens de Operações, quer na componente das operações defensivas no Ciberespaço, quer no que diz respeito às CEMA. Assim, os planos devem abordar a forma como integrar efetivamente as capacidades do Ciberespaço, como combater o uso do Ciberespaço pelo adversário, identificar e proteger o Ciberespaço considerado crítico para a missão, avaliar o terreno importante no Ciberespaço, como operar num Ciberespaço degradado, usando com eficiência recursos limitados do Ciberespaço e combinar os requisitos operacionais com as capacidades do Ciberespaço. As OpsCiber e a GE permitem enriquecer a COP disponibilizada em apoio da tomada de decisão dos Cmdt, com o objetivo permanente de afetar o desempenho dos Forças Opositoras. As OpsCiber, podem ser realizadas em diferentes segmentos do espectro eletromagnético (por exemplo: *Wi-Fi*, *Bluetooth*, bandas de satélite) pelo que a GE e as OpsCiber necessitam de uma abordagem conjunta com total articulação e integração. Esta complementaridade, é refletida nas capacidades de GE e de condução de OpsCiber, contribuindo para cada Função de Combate:

a. Comando Missão

Os Cmdt no Teatro de Operações baseiam a sua ação de Comando nos meios e serviços disponibilizados pelo SIC-T, e cabe às Unidades de GE em conjunto com as Unidades de Ciberdefesa efetuar a defesa destas redes. Esta defesa é realizada através de MPE e visam eliminar ou mitigar o impacto negativo de ações de Forças neutrais, inimigas ou amigas sobre o espectro eletromagnético.

b. Movimento e Manobra

A GE apoia a função Movimento e Manobra, através da disrupção ou neutralização de capacidades que utilizam o espectro eletromagnético ou através na negação do uso do espectro eletromagnético ao adversário/inimigo e consequentemente dos SIC adversário/inimigo, diminuindo a *situational awareness* dos Cmdt do inimigo e a sua capacidade de intervir. As Medidas de GE, apoiam igualmente o Movimento e Manobra protegendo as nossas Forças contra engenhos explosivos improvisados controlados acionados por meios-rádio, e simultaneamente fornecendo informação para que os Cmdt no Teatro de Operações possam transmitir em tempo útil as suas ordens às Forças em manobras.

c. Informações

As ações realizadas com recurso aos meios de GE e Ciberdefesa que funcionam como sensores, contribuem com informação durante todo o processo de decisão militar com especial ênfase durante o *Intelligence Preparation of the Battlefield* (IPB). Os especialistas em GE e OpsCiber, analisam a ocupação do espectro eletromagnético e do Ciberespaço pelas Forças Opositoras, com especial enfoque para:

(1) A ocupação do espectro eletromagnético;
(2) A dependência de redes de dados;
(3) A sofisticação das capacidades ciber ofensivas e defensivas opositoras;
(4) As capacidades de GE opositoras;
(5) As possíveis vulnerabilidades existentes em redes de dados;
(6) A capacidade das Forças Opositoras de sincronizar OpsCiber com a restante atividade operacional;
(7) A capacidade das Forças Opositoras de fazer uso das redes sociais e engenharia social em proveito das Operações.

d. Fogos

As ações ofensivas de GE são parte integrante da função “Fogos”, contribuindo pela negação aos sistemas das Forças Opositoras a capacidade de comunicarem, efetuarem o seguimento ou o *targetting* de Forças Amigas. Cumulativamente, a GE

apoia a função Fogos, ao apoiar eletronicamente na pesquisa, localização e identificação de fontes adversárias/inimigo de radiação de energia eletromagnética. As ações de GE são articuladas e coordenadas de forma estreita com ações ofensivas no Ciberespaço por forma impedir às Forças Opositoras a possibilidade da sua utilização, bem como a negação da utilização do espectro eletromagnético.

e. Apoio de serviços

A GE e as Forças que atuam no Ciberespaço, contribuem para a função Apoio de Serviços na medida em que através da execução de ações que garantem a proteção sistemas CSI, permitem a coordenação e articulação das operações de sustentação.

f. Proteção

No que respeita à função de combate Proteção, as ações conduzidas no Ciberespaço pelas nossas Forças permitem identificar e mitigar possíveis ameaças a redes e sistemas de comunicações amigos. Concorrentemente, as ações de GE realizadas visam a proteção de Forças Amigas, pessoal e material assegurando em coordenação com os vários escalões, a desconflitualização na utilização do espectro eletromagnético.

408. Funções e responsabilidades

a. Os Cmdt táticos usam as OpsCiber e a GE para compreender o ambiente operacional, apoiar o processo de decisão militar e afetar o adversário. Concretamente ao nível do escalão brigada, a constituição de uma célula CEMA irá permitir tirar melhor partido destas capacidades. A função da célula CEMA é fornecer opções de utilização do Ciberespaço e da GE para que o Cmdt atinja seu objetivo e conta com elementos de cada uma das capacidades que contribuem para as operações no espectro eletromagnético:

(1) O Oficial de GE, que no caso da Brigada é o Cmdt da Companhia de GE;

(2) O Cmdt da Unidade que conduz OpsCiber;

(3) Um elemento do âmbito das INFO OPS;

(4) Um elemento gestor do espectro eletromagnético para a desconflitualização da sua utilização pelas diferentes capacidades.

b. Neste contexto, a tradicional designação de Oficial de GE mantém-se sendo que este pode acumular com as responsabilidades ao nível da OpsCiber.

c. Na eventualidade de não existir um Oficial específico para a área das OpsCiber, o Oficial de GE deverá acumular essas novas responsabilidades, garantindo a integração e sincronização das CEMA, nomeadamente com as Funções de Combate Fogos, Informações e Proteção. Em ambos os casos, terá de coordenar as suas

atividades e trabalhar em estreia colaboração com a estrutura de GE e/ou OpsCiber do escalão superior. Os Cmdt táticos, em coordenação com o Órgão Conjunto de Ciberdefesa e outros Comandos orquestram os esforços de planeamento para as OpsCiber, indicam os efeitos pretendidos das OpsCiber e determinam o *timing* para as OpsCiber realizarem as suas missões produzindo os efeitos desejados.

d. No que concerne concretamente SIC-Op, o Exército possui uma estrutura de Ciberdefesa, que em coordenação com o EMGFA, deverá ser capaz de garantir a capacidade de resposta a incidentes de segurança e defesa do Ciberespaço e da informação do Exército.

e. Por sua vez, o órgão conjunto de Ciberdefesa das Forças Armadas é a entidade responsável por planear, dirigir, coordenar, controlar e executar as operações militares que garantam a liberdade de ação das Forças Armadas no Ciberespaço. No âmbito destas Operações, realiza as ações necessárias para garantir a sobrevivência dos elementos físicos, lógicos e virtuais críticos para a Defesa e para as Forças Armadas.

Página intencionalmente em branco

CAPÍTULO 5 – GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO

SECÇÃO I – INTRODUÇÃO

501. Generalidades

A GIC é uma área estratégica e uma capacidade de grande importância. A forma como o Exército gere a informação e facilita a circulação do conhecimento teve um notável incremento nos últimos tempos devido ao desenvolvimento das tecnologias de informação e do trabalho em Rede. Reconhecendo que a capacidade de gerir eficientemente o conhecimento é essencial para um Comando efetivo, o Exército implementou órgãos de GIC em toda a sua estrutura de Comando (Comando do Exército, Órgãos Centrais de Administração e Direção, Comando das Forças Terrestres e restantes U/E/O) que proporcionam os meios para uma partilha eficiente do conhecimento e estabelecem a ponte entre a arte de comandar e a ciência do controlo e tomada de decisão.

O conhecimento individual e o dos pequenos grupos, não pode ser partilhado de forma abrangente sem os meios para o fazer. O volume da informação disponível torna-a difícil de identificar e de utilizar a considerada relevante. A GIC proporciona os meios para eficientemente partilhar conhecimento, permitindo dessa forma compreensão e aprendizagem comuns nas organizações. Realça a capacidade de uma organização para detetar e remover obstáculos ao fluxo de conhecimento, permitindo o sucesso da missão. Sendo a partilha de informação um contributo chave para a GIC é imperativo que todas as pessoas estejam envolvidas neste processo: desde a geração de Forças, responsável pelo treino e sustentação das subunidades, até às Forças Operacionais.

502. Princípios da Gestão de Informação e do Conhecimento

a. Princípios da Gestão de Informação:

(1) Simplicidade (Reconhecer e gerir a complexidade)

A gestão das U/E/O do Exército em tempo de paz e em Operações é uma tarefa exigente, complexa e que precisa e gera um volume de informação muito grande. A arte de conseguir organizar corretamente a informação e disponibilizá-la em tempo oportuno aos destinatários é o cerne da Gestão da Informação. Obter Informação relevante e apresentá-la de forma simples é o objetivo primordial, permitindo ao Cmdt/Dir/Ch ter uma visão completa sobre todos os assuntos e Operações. Desta forma a decisão do Cmdt/Dir/Ch é assertiva e isenta de ambiguidades. Todavia os Cmdt/Dir/Ch não devem deixar de reconhecer e gerir a

complexidade. Para se alcançar o princípio da simplicidade é fundamental atribuir pessoas e recursos para uma Gestão da Informação eficaz, pois o volume de informação, sobretudo nas GU e em Operações complexas, poderá ser colossal.

(2) Objetividade

Os resultados da Gestão da Informação deverão ser precisos. O Cmdt/Dir/Ch deverá ter respostas tão exatas quanto possível e sem ambiguidades. O excesso de Informação, a sua imprecisão ou impertinência poderá causar perturbações no processo de tomada de decisão. Deve-se evitar sobrecarregar o Cmdt/Dir/Ch com informação, que apesar de poder ser interessante, não contribui para a tomada de decisão. Todavia os Cmdt/Dir/Ch determinam a forma e a quantidade que querem receber de informação.

(3) Oportunidade

A Gestão da Informação deve apoiar o Cmdt/Dir/Ch no momento certo, com informação pertinente e adequada para a tomada de decisão. A disponibilização da Informação deverá assentar nas necessidades dos intervenientes, local e tempo certo.

(4) Comunicação e partilha

A Gestão da Informação só tem valor no momento da comunicação e partilha, só assim a informação acrescenta valor à U/E/O. Com a informação partilhada o EM dispõe de ferramentas úteis de trabalho, o Cmdt/Dir/Ch fica com uma visão partilhada de todos os assuntos e Operações e gera-se conhecimento que permite obter uma superioridade no momento da tomada de decisão. O Cmdt/Dir/Ch e os seus subordinados deverão estar cientes de que a partilha de informação gera poder.

Exceto no caso de restrições devidas à Segurança Nacional, à Segurança das Operações, à privacidade, sensibilidade ou de direitos de autor, a informação deve ser sempre tratada como um recurso partilhado e disponibilizada a todos os que necessitem e estiverem autorizados a aceder, para poderem executar as suas tarefas. A premissa da necessidade de saber, tem de estar sempre presente, nunca podendo descurar a proteção de dados pessoais inerentes aos indivíduos.

(5) Continuidade e confiança

A Gestão da Informação, durante as Operações, é uma atividade sempre por concluir. O pessoal afeto à Gestão da Informação opera continuamente, pois a produção de informação também é contínua. Toda a atividade de Gestão da Informação deve pautar-se por produzir informação relevante e fiável. Informação

baseada em palpites ou em suposições nunca é aceitável, exceto quando assumido e decidido pelo Cmdt, sendo tal facto comunicado previamente.

b. Princípios da Gestão do Conhecimento

(1) Compreensão

Através da colaboração e do diálogo, a partilha de conhecimento possibilita uma melhor compreensão do ambiente operacional, facilita a identificação dos problemas e ajuda a encontrar soluções para os resolver. A melhoria contínua de uma compreensão partilhada entre os Cmdt, o EM e os subordinados sustenta a tomada de decisão e a condução de Operações. O diálogo informal, a partilha de perspetivas, pontos de vista, preocupações e possibilidades, levam a uma compreensão abrangente dos problemas ao mesmo tempo que ajudam a criar confiança e formam a base para a unidade de esforço. A compreensão está intimamente ligada aos anseios, preocupações sociais e pessoais e deve ser promovida, constantemente, a todos os níveis.

(2) Partilha

A partilha de conhecimento gera poder. O conhecimento é um recurso transferível que tende a incrementar com o uso e aplicação. Encorajar a interação entre as pessoas ligando as fontes de conhecimento tácito, a todos os níveis, ajuda o Exército a obter e a partilhar conhecimento para melhor atingir os objetivos, quer em tempo de paz quer em campanha. A aprendizagem, o treino, o ensino e a tutoria ocorrem mais facilmente, e muitas vezes de forma mais eficiente, num ambiente face a face.

(3) Integração

As Unidades do Exército podem integrar Unidades Conjuntas e Combinadas, ou operar de forma isolada. As Unidade apresentam alguma dependência de apoios exteriores à organização. Uma integração efetiva do conhecimento entre os diversos participantes nas Operações é necessária para a criação de um entendimento comum entre todos. Esta integração ajuda a eliminar constrangimentos entre os diferentes intervenientes e permite uma visão única das Operações.

(4) Ligação interpessoal

Ligar as pessoas com o conhecimento a outras que precisam desse conhecimento é fundamental. Só esta partilha de conhecimento permite criar valor acrescentado à tomada de decisão do Cmdt/Dir/Ch . A criação de conhecimento depende da sua transferência por parte de quem detém a experiência, a sabedoria ou

perspicácia, para as outras pessoas. O conhecimento que não for partilhado e transferido é inútil. A transferência de conhecimento só é eficaz se houver uma ligação eficaz entre as pessoas, e uma visão alargada do bem da organização.

(5) Aprendizagem

A Gestão do Conhecimento ajuda os militares e as organizações a aprender e a adaptarem-se. O aumento da colaboração e interação entre Cmdt/Dir/Ch e subordinados melhora a flexibilidade, adaptabilidade e integração. A Gestão do Conhecimento facilita a partilha e integra estratégias de aprendizagem informais e organizacionais para promover a aprendizagem. Ela envolve a transferência de conhecimentos durante a interação e colaboração, aproveitando recursos dentro e fora da organização. As organizações adaptam-se mais depressa quando se promove a aprendizagem.

(6) Confiança

A confiança é a base das relações interpessoais, havendo também a necessidade de ser cultivada incessantemente entre as pessoas e organizações. Só desta forma é possível formar equipas coesas, incentivar as equipas a terem iniciativas, dentro dos limites das Operações, a aceitarem riscos calculados e a explorarem o sucesso compreendendo a intenção do Cmdt.

503. Conceitos

No presente capítulo apresenta-se separadamente a Gestão da Informação e a Gestão do Conhecimento, ainda que, no decorrer da parte dedicada à Gestão do Conhecimento constate-se que a Gestão da Informação não é mais que uma das etapas da Gestão do Conhecimento. Nesse sentido, quando se fala em Gestão do Conhecimento fala-se numa perspetiva lata e quando se fala de Gestão da Informação considera-se a perspetiva estrita do processamento de itens documentais ou registos.

a. O conhecimento é a base objetiva e subjetiva que serve para a tomada de decisões. Este conhecimento adquire-se de diversas formas e a partir de diferentes fontes de informação. Assim é fundamental gerir a informação de forma judiciosa para se poder criar conhecimento pessoal e organizacional. A Gestão da Informação e a Gestão do Conhecimento estão ligadas e complementam-se. Na figura 5-1 apresenta-se um esquema que relaciona estes conceitos. O objetivo é fornecer às U/E/O e aos seus Cmdt/Dir/Ch a sabedoria necessária para tomar decisões acertadas no momento oportuno.

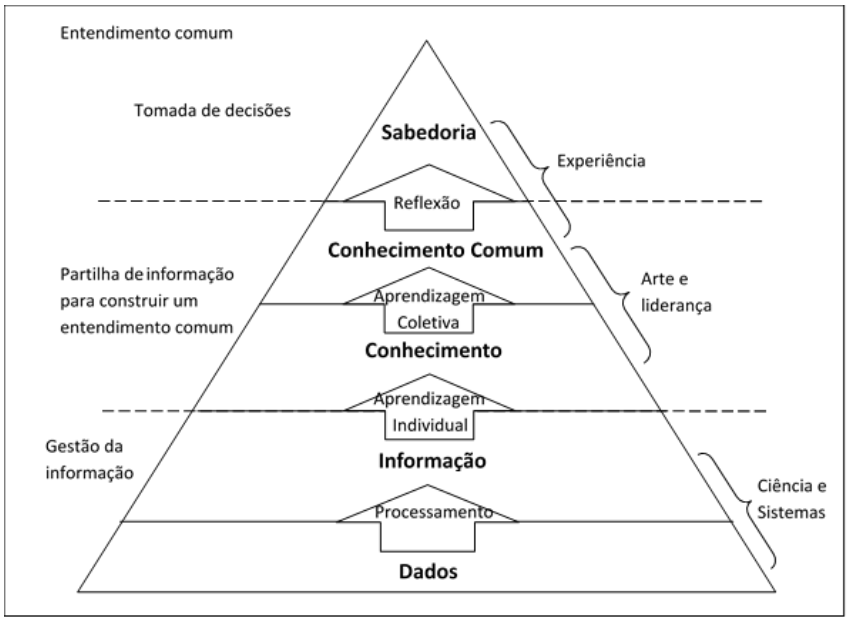

Figura 5-1 – Dos dados à sabedoria

b. A Gestão da informação é a ciência do uso de procedimentos e SI para receber, processar, analisar, armazenar, divulgar e proteger produtos de conhecimento, dados e informações, assim como, a produção de informações oportunas e a disseminação de informações protegidas relevantes para os Cmdt/Dir/Ch e EM.

c. A Gestão do Conhecimento é a arte de criar, organizar, aplicar e transferir conhecimento para facilitar a compreensão situacional e a tomada de decisão. A Gestão do Conhecimento apoia a melhoria organizacional, a inovação e performance.

d. O Cmdt é a figura central no Comando-Missão. Os Cmdt conduzem Operações através da compreensão, da visualização, da descrição, da liderança e da avaliação e o EM apoia-o no planeamento e execução de Operações. A Gestão do Conhecimento é essencial para os Cmdt e seu EM na realização destas tarefas. Os Cmdt usam a sua reflexão e experiência para transformar conhecimento em sabedoria.

SECÇÃO II – GESTÃO DA INFORMAÇÃO

504. Enquadramento

A Gestão da Informação está relacionada com a obtenção, processamento, armazenamento, proteção e distribuição dos dados e informações antes de se tornarem conhecimento.

O Cmdt/Dir/Ch é o responsável pela GIC. É designada uma equipa/secção ou pessoa, consoante o escalão, a missão e o tempo disponível para apoiar o Cmdt/Dir/Ch nesta tarefa (Gestor de Informação ou secção GIC). As necessidades explícitas de informação,

a organização da Gestão da Informação dentro da sua U/E/O, de acordo com os regulamentos em vigor, são responsabilidades únicas do Cmdt/Dir/Ch.

A Gestão da Informação, ao nível do EM, tem a responsabilidade, entre outras, de responder às necessidades explícitas de informação do Cmdt/Dir/Ch. Mantém uma atividade permanente de obtenção, tratamento e análise da informação apoiando a ação de Comando. Todas as áreas do EM geram um volume abundante de informação que deve ser criteriosamente gerida, de forma a acrescentar valor e rapidez à tomada de decisão.

505. Ciclo de Gestão da Informação

A figura 5-2, adaptada do manual da OTAN[24], mostra o ciclo de Gestão da Informação. Não devemos entender esta figura como um modelo de fluxo de informação. O objetivo é mostrar que todas estas fases se sobrepõem e podem ocorrer simultaneamente ou em diferentes sequências.

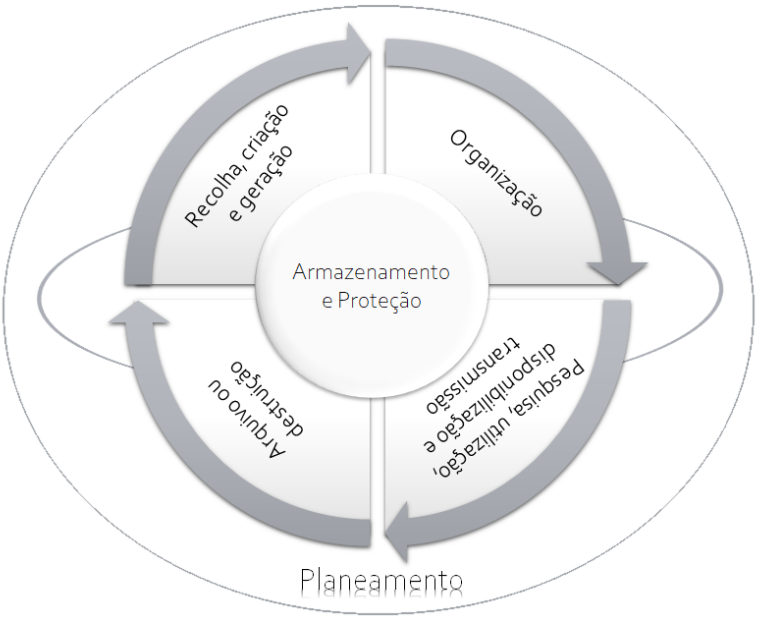

Figura 5-2 - Ciclo da Gestão da Informação

a. Planeamento

O planeamento é importante para determinar os processos e produtos a obter em função da missão da U/E/O. O volume de informação depende da missão, do escalão, do local onde vai decorrer a Operação e do tempo da Operação. O planeamento

[24] *NATO Information Management Manual, 07Mar2013, Document AC/324-D(2013)0001, Conseil de L'Atlantique Nord, Pg. 1-2*

deverá ter em conta estes fatores, conjugados com o conhecimento e lições aprendidas de outras U/E/O que tenham participado em Operações similares.

b. Recolha, criação e geração

Nesta etapa definem-se as normas para recolher, criar ou gerar os itens de informação nas U/E/O do Exército. A informação pode ter múltiplas origens (documentos, imagens, vídeo, bases de dados) e todos os intervenientes na recolha, criação ou geração de informação devem refletir sobre a pertinência dessa informação. Muita informação pode ser redundante, não ter significado ou ser importante apenas num tempo de vida útil que já foi ultrapassado. O objetivo é evitar um volume colossal de informação para ser tratada e armazenada.

c. Organização

O objetivo desta etapa prende-se com o aproveitamento eficaz dos recursos de informação para se obter uma superioridade no uso da informação. O Cmdt/Dir/Ch tem à sua disposição informação assertiva, fiável e em tempo oportuno para poder decidir mais depressa e mais acertadamente. A organização judiciosa e metódica da informação permite acrescentar-lhe valor garantindo, ao mesmo tempo, a sua proteção.

d. Pesquisa, utilização, disponibilização e transmissão

A informação só acrescenta valor decisivo ao processo de tomada de decisão, se a informação correta for disponibilizada à pessoa certa, no momento oportuno e no formato correto. Todos os meios de acesso, uso e transmissão de informação devem ser orientados para este objetivo. Em simultâneo, todos os sistemas e pessoas que manipulam e distribuem a informação devem estar preparados e treinados para prevenir o seu uso indevido. O comprometimento de informação, sobretudo quando ignorado, pode prejudicar gravemente o emprego dessa informação para o processo de tomada de decisão.

e. Armazenamento e proteção

O armazenamento prende-se com a guarda e manutenção da informação, em formatos e sistemas adequados, para o seu uso correto. A proteção garante a salvaguarda da confidencialidade da informação e manutenção da sua integridade, é um objetivo que carece de uma atenção constante em todas as etapas e processos de uso e tratamento da informação.

f. Arquivo ou destruição

A decisão de guarda ou de destruição deverá ser tomada de forma criteriosa e segundo as normas e procedimentos estabelecidos, de acordo com as normas legais. Todos os

documentos processados para destruição terão de ter um registo dessa autorização. Pelo que deverão ser estabelecidas políticas e normas de arquivo ou destruição da Informação em fim de vida útil.

506. Bases de Dados

Criar, aceder e gerir dados e informação só é possível quando a mesma se encontra arquivada ou guardada em suportes físicos ou digitais. Enquanto o papel permanece em suporte físicos, como capas de arquivo, os dados digitais são armazenados em base de dados com determinada tecnologia associada. Uma base de dados é uma ferramenta de recolha e organização de informação e dados. As bases de dados podem armazenar diferentes tipologias de dados, desde pessoas, produtos, encomendas, podendo ser mais ou menos pormenorizadas.

a. Numa fase primordial, a base de dados era vista como um ficheiro de texto ou uma folha de cálculo, onde o utilizador inseria os dados, o que é válido para pequenas estruturas e dados relativamente pequenos. Em estruturas com grande quantidade de dados, comumente era visível repetição de dados, inconsistência dos mesmos e a pesquisa de informação era difícil ou demorada, pelo que houve a necessidade de melhorar esses aspetos, sendo criadas base de dados em tecnologia apropriada para que não fossem utilizadas folhas de cálculo e de processamento de texto.

b. Vantagens de utilização de base de dados:

(1) Adicionar dados de forma simples e rápida, como um novo item num inventário, um militar ao apresentar-se numa U/E/O;

(2) Editar dados existentes de forma acessível e rápida, como alterar as características relativas a um item (cor, tamanho, ano de produção), morada de um militar;

(3) Eliminar itens desatualizados. Campos que deixem de fazer sentido, ou dados que já não são utilizados por não possuírem valor;

(4) Partilhar dados com outras pessoas através de relatórios e mensagens de e-mail;

(5) Organizar e visualizar os dados de diversas formas.

c. Estrutura de uma base de dados

(1) Uma base de dados estruturada deve assentar em dois princípios:

(a) O princípio da duplicação de dados e o princípio da exatidão e integridade. O princípio da duplicação de dados, como pilar para não existirem dados repetidos, a fim de evitar a ocupação de espaço em disco desnecessariamente, bem com o aumento da probabilidade de ocorrer erros e inconsistências.

(b) Relativamente ao segundo princípio, exatidão e integridade, deve estar sempre em permanência para que os dados sejam reais e fidedignos, caso contrário, os dados extraídos para relatórios e outros locais serão incorretos, levando a que as decisões tomadas com base nessa informação não sejam as mais acertadas.

(2) Uma boa estrutura de base de dados deve:

(a) Dividir os dados em tabelas baseadas em assuntos para reduzir o número de dados redundantes;

(b) Ajudar a suportar e garantir a precisão e a integridade dos dados da base de dados;

(c) Gerar relatórios e processamento de dados de acordo com as necessidades;

(d) Possibilitar a escalabilidade da base de dados.

d. Processo de estruturação de uma base de dados

Para a estruturação de uma base de dados deve considerar-se o seguinte:

(1) Determinar o objetivo da base de dados;

(2) Localizar e organizar as informações necessárias;

Reunir todos os tipos de dados e informação que se pretende registar na base de dados.

(3) Dividir informações em tabelas;

Dividir os itens de informação em assuntos/pontos principais, por tipologia como por exemplo produtos ou encomendas, fornecedores, clientes. Para cada assunto ocorre a atribuição de uma tabela.

(4) Transformar itens de informação em colunas;

Definir que tipo de informação se pretende armazenar em cada tabela. A informação é associada a campos, que são apresentados como colunas na tabela. Por exemplo, uma tabela designada Utilizadores poderá incluir campos como NIM, Posto, Nome completo, U/E/O.

(5) Especificar chaves primárias;

Escolher a chave primária de cada tabela. A chave primária é uma coluna utilizada para identificar cada linha (registo), funciona como identificador único. Por exemplo, pode ser o identificador (ID) do produto, o ID do utilizador.

(6) Estabelecer relações de tabelas.

Analisar as tabelas e os seus campos, a fim de verificar de que forma é que os dados numa tabela estão relacionados com os dados de outras tabelas. Adicionar

campos às tabelas ou criar novas tabelas para definir as relações, conforme necessário.

e. Modelo de base de dados

(1) Um modelo de base de dados é um conjunto de regras e métodos que permite representar conjuntos de dados (entidades) especificando as relações entre cada um deles, determinando como os dados podem ser armazenados e acedidos.

(2) Existem dois modelos de base de dados:

(a) Modelos de base de dados baseados em objetos procuram representar a realidade através de objetos, contendo informação relevante sobre as entidades reais que representam.

(b) Modelos de base de dados baseados em registos procuram representar a realidade através de registos. Estes registos equivalem aos registos utilizado em programação contendo informação estruturada com formato de campo. Neste tipo de modelo, destacam-se o modelo hierárquico, o modelo de Rede e o modelo relacional.

(3) Após criar um diagrama de modelo de base de dados, por vezes é necessário aperfeiçoar o diagrama para refletir as necessidades existentes de informação e de relação. É possível adicionar e personalizar os três componentes principais de um modelo: tabelas (entidades), colunas (descrição dos registos da tabela) e relações (associações entre tabelas, que podem ser de um para um, um para muitos ou de muitos para muitos).

f. Disponibilização

(1) Antes de criar uma base de dados é necessário analisar qual vai ser o seu intuito, quem vai aceder à mesma, que dados estarão presentes e a forma de disponibilizá-los. As bases de dados devem ter associado o intuito para o qual foram criadas, bem como o princípio da necessidade de saber. Para tal existem diferentes tipos de acesso, com permissões e capacidades diferenciadas:

(a) Privilégios de leitura a quem apenas necessite de visualizar e consultar dados das tabelas existentes na base de dados;

(b) De escrita a quem efetivamente tenha de inserir, manter e apagar registos das tabelas da base de dados.

(2) O administrador tem privilégios totais, tendo a possibilidade de controlo total ao nível dos registos inseridos, bem como na especificação de campos da base de dados e na atribuição de privilégios aos utilizadores.

SECÇÃO III – GESTÃO DO CONHECIMENTO

507. Enquadramento

A Gestão do Conhecimento usa a informação já processada para criar, organizar e transferir conhecimento, atingindo-se, desta forma, um entendimento partilhado que permita a tomada de decisões. A finalidade da Gestão do Conhecimento é a criação de um entendimento comum através da conjugação das pessoas, processos e ferramentas dentro da organização, promovendo uma cultura de partilha de conhecimento e interação entre os Cmdt/Dir/Ch e os subordinados. A Gestão do Conhecimento apoia a melhoria da organização, a inovação e o desempenho da U/E/O. A Gestão do Conhecimento potência o sucesso da missão por:

a. Apoiar a tomada de decisão do Cmdt em todo o espetro de Operações;

b. Facilitar o diálogo e a interação necessária para o sucesso da missão através de ferramentas e processos colaborativos;

c. Facilitar o acervo e a transferência de conhecimento tácito e explícito partilhado na organização;

d. Ajudar o EM a fornecer informações e conhecimentos relevantes em tempo oportuno;

e. Permitir a aprendizagem e adaptação das organizações;

f. Apoiar as tarefas da U/E/O.

508. Tipos de Conhecimento

O conhecimento acrescenta valor para e durante as Operações. É adquirido através do estudo, da experiência, da prática e interação humana e é a base para a segurança de uma decisão fundamentada.

a. Conhecimento tácito

O conhecimento tácito é aquele que as pessoas detêm; um acervo único e pessoal, de conhecimentos adquiridos a partir de experiências de vida, formação e redes de contactos. Inclui nuances aprendidas e sutilezas. A intuição, a agilidade mental e o improviso na resposta a crises são também formas de conhecimento tácito.

b. Conhecimento explícito

O conhecimento explícito é conhecimento formalmente documentado, organizado e transferido para outros através de meios digitais ou não-digitais. O conhecimento explícito tem regras, limites e significados precisos. Como exemplos: documentos de computador, dicionários, livros didáticos e publicações doutrinárias do Exército.

509. Modelo de Gestão do Conhecimento

a. A Gestão do Conhecimento usa um processo de cinco etapas para criar entendimento partilhado. A figura 5-3 mostra a Gestão do Conhecimento como um ciclo interativo.

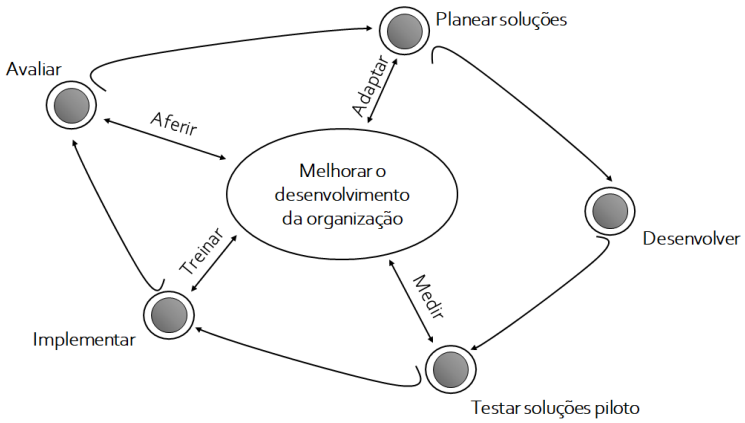

Figura 5-3 - Ciclo Iterativo da Gestão do Conhecimento

(1) Avaliar

A avaliação, como o primeiro passo do processo de Gestão do Conhecimento, analisa as necessidades de conhecimento da U/E/O e estabelece abordagens que melhoram a compreensão, a tomada de decisão e a aprendizagem de todos os elementos. O conhecimento melhora o desempenho das Unidades. A avaliação da Gestão do Conhecimento envolve a monitorização do desempenho da Unidade para compreender como é gerido o tempo e a informação e, ainda, tudo aquilo que é considerado crítico ou prioritário para a tomada de decisão. A equipa da Gestão do Conhecimento avalia como o conhecimento e a informação se dinamizam na U/E/O, observando a interação das pessoas, processos e ferramentas envolvidas.

No decurso de Operações, os Cmdt e todas as secções do seu EM avaliam a situação para compreender as condições vigentes e perspetivar a evolução das atividades operacionais.

A avaliação ajuda a equipa da Gestão do Conhecimento a melhor compreender as condições existentes e as que se pretendem atingir e envolve as seguintes quatro etapas:

(a) Etapa 1: Definir a Organização e seu ambiente; pessoas, processos, ferramentas e organização;

(b) Etapa 2: Descrever ligações e dependências internas e externas da organização;

(c) Etapa 3: Analisar a Organização e avaliar o seu conhecimento e desempenho e as lacunas no seu conhecimento e desempenho;

(d) Etapa 4: Representar a conectividade e alinhamento dos componentes da Gestão do Conhecimento da Organização em representações gráficas de fácil compreensão.

(2) Planear soluções

Nesta etapa pretende-se realizar o planeamento de soluções para as áreas problemáticas identificadas durante a avaliação. Inicia-se com a visão geral da etapa de planeamento seguindo-se uma descrição de soluções para problemas comuns como padronização, gestão de tempo, reuniões, relatórios, sistemas técnicos e Gestão da Informação.

Neste contexto, planear é identificar e desenhar soluções para eliminar ou mitigar os hiatos ou os problemas identificados durante a avaliação. As soluções podem traduzir-se apenas em refinamentos de processos ou ferramentas existentes, em formação e treino de pessoal, mudanças na estrutura ou cultura organizacional e no alinhamento de todos estes fatores de forma a alcançar os melhores resultados através de uma solução viável.

Durante esta etapa, é questionado qual a melhor abordagem para criar um entendimento comum para melhorar o desempenho na execução da missão da U/E/O, cujo objetivo é fornecer a informação certa, às pessoas certas, no formato certo, na hora certa para alcançar a melhor decisão e garante que as soluções:

(a) Sejam adequadas aos problemas identificados e os corrijam;

(b) Sejam satisfatórias às partes interessadas sem aumentar o volume de trabalho;

(c) Possam ser desenvolvidas, dirigidas e implementadas dentro dos constrangimentos de recursos da U/E/O, com os meios disponíveis e com um nível de esforço considerado razoável;

(d) Permitam continuidade de eficácia ao longo do tempo no cumprimento da sua finalidade.

(3) Desenvolver soluções

A etapa de desenvolvimento do processo da Gestão do Conhecimento constrói-se com base nas dificuldades resultantes da fase da avaliação e do planeamento. O Oficial responsável pela Gestão do Conhecimento deverá verificar se as soluções desenvolvidas são adequadas para preencher as dificuldades existentes no âmbito do conhecimento e do desempenho na U/E/O estando em estreita

coordenação com o Chefe de Estado-Maior, Comandante, Diretor ou Chefe (Cmdt/Dir/Ch).

O desenvolvimento é um processo de construção passo a passo, detalhado que deverá resultar numa solução completa, pronta a ser testada e validada. Geralmente, requer uma estreita colaboração entre o Oficial responsável pela GIC e da equipa de SIC.

Quando existe mais do que uma solução em desenvolvimento, o Oficial responsável pela Gestão do Conhecimento identifica as áreas coincidentes (por exemplo, normas e relatórios entre outros) para coordenar os esforços e evitar redundâncias desnecessárias. A coordenação é particularmente importante no desenvolvimento do treino que normalmente deve acompanhar novas soluções. O Oficial responsável pela Gestão do Conhecimento confirma as prioridades para garantir a correta orientação do esforço no desenvolvimento de soluções.

As seguintes etapas do desenvolvimento ajudam-nos a encontrar a solução mais adequada para ser implementada:

(a) Confirmar as prioridades da U/E/O, requisitos de informação críticos do Cmdt/Dir/Ch e estado da U/E/O;

(b) Esquematizar as ações necessárias para criar a solução;

(c) Construir a solução.

Durante as Operações, o Oficial da Gestão do Conhecimento tem de ter o conhecimento de quais os requisitos de informação críticos do Cmdt e a solução proposta vai centrar-se sobre estes, tendo em conta as capacidades atuais da Unidade para as áreas específicas a desenvolver. Isto requer uma revisão das avaliações efetuadas.

(4) Testar Soluções Piloto

Testar soluções para a Gestão do Conhecimento é um passo de aprendizagem necessário no processo de Gestão do Conhecimento que deverá ser realizado antes da implementação em larga escala de uma qualquer solução. Esta fase refere-se ao desempenho de um teste preliminar realizado em pequena escala para avaliar e validar a viabilidade, o tempo, o custo e os efeitos de uma determinada solução.

Um projeto piloto de uma solução de Gestão do Conhecimento permitirá identificar e corrigir problemas e prepará-lo para a plena implementação numa organização. Uma solução piloto limitada pode ser realizada, modificando a solução proposta

se necessário, tendo por base uma análise qualitativa e quantitativa, o *feedback* dos participantes e uma perceção profissional de Gestão do Conhecimento.

Um projeto piloto, como teste incremental, destina-se a validar a utilidade das soluções. Esta é a fase na qual muitas das soluções deverão ser modificadas tendo por base os testes a que são submetidas. Isto é fundamental para garantir que uma solução é adequada, viável e aceitável.

Em resumo, um ciclo de teste eficaz de um processo de Gestão do Conhecimento são planear, preparar, executar e avaliar.

(5) Implementar soluções

A implementação, ou a execução de um plano é o passo mais importante no processo e foca-se nas melhorias funcionais da área de Gestão do Conhecimento. No passo implementação a solução desenvolvida é finalizada, apresentada para aceitação e aplicada. A implementação coloca o plano em ação e depende de uma compreensão partilhada para avaliar o progresso e realizar ajustes das decisões. Este passo utiliza as soluções de Gestão do Conhecimento validadas do utilizador e implementa-as nos processos e sistemas pertencentes à organização.

O passo da implementação envolve avaliação contínua das soluções aplicadas e ajustes através da monitorização objetiva da performance de acordo com os objetivos determinados. O processo de Gestão do Conhecimento é um ciclo funcional recursivo. Quando a solução está numa fase de execução estável, é monitorizada e os seus impactos são avaliados para assegurar que está de acordo com a melhoria do processo estabelecido.

b. As cinco etapas do processo de Gestão do Conhecimento abordadas anteriormente congregam as quatro componentes geradoras de conhecimento para uma cultura de colaboração e partilha de entendimento entre os Cmdt/Dir/Ch e subordinados. As quatro componentes são:

(1) Pessoas

As pessoas são importantes para uma gestão eficaz da informação e do conhecimento. A informação e o conhecimento só têm sentido num contexto humano e é fruto da experiência individual, das aprendizagens e da visão pessoal. Os Cmdt/Dir/Ch usam o conhecimento tácito para resolver problemas e tomar decisões. Empregam o conhecimento tácito dos subordinados para melhorar aprendizagem organizacional, reforçar a inovação e o desempenho da U/E/O.

Os gestores de conhecimento ligam pessoas e constroem redes formais e informais para transferir conhecimento. A transferência de conhecimento é mover conhecimento, incluindo o conhecimento baseado em experiências ou juízos fundamentados, de uma pessoa para outra.

(2) Processos

A Gestão do Conhecimento e as atividades associadas são integradas nas Operações, nos processos organizacionais e em todos os indivíduos do EM. Esta integração permite a transferência de conhecimento entre pessoas e entre organizações. Formalmente a transferência de conhecimento ocorre através de processos e procedimentos existentes na organização e informalmente, através da colaboração e diálogo.

(3) Ferramentas

As ferramentas de GIC partilham e preservam o conhecimento. Vários fatores determinam as ferramentas utilizadas, incluindo a missão, a disponibilidade e a simplicidade. As ferramentas podem ser não-digitais, digitais ou ambas. As ferramentas não-digitais incluem a transferência de conhecimento através de meios manuais, visuais ou táteis. As ferramentas digitais incluem:

(a) SI e o *software*, incluindo, armazenamento, entradas, processamento, saídas, formatos e conteúdos;

(b) As ferramentas de colaboração que incluem recursos que tornam possível o desenvolvimento e a colaboração da equipa, por exemplo o Portal de *Intranet*;

(c) Ferramenta de localização de peritos que permitem encontrar especialistas nos assuntos;

(d) Ferramentas de análise de dados que suportam a síntese de dados que identifica padrões e estabelece relações entre os elementos de dados;

(e) Ferramentas de pesquisa e descoberta incluindo motores de busca que permitem a procura de temas, sugestão de temas ou autores semelhantes e apresentam relações com outros tópicos;

(f) Ferramentas de desenvolvimento de especialização, que incluem simulações de emprego e aprendizagem experimental para apoiarem o desenvolvimento de experiências, conhecimentos e tomadas de decisão.

(4) Organização

A GIC deverá ser implementada no Exército. Uma organização é uma matriz onde as pessoas, os processos e as ferramentas funcionam para integrar o conhecimento individual e organizacional e as estratégias de aprendizagem.

Conhecimento individual pode incluir ideias adquiridas, crenças, valores e conhecimentos. As capacidades de GIC contribuem para uma promoção da aprendizagem dentro da organização. A cultura de uma organização fornece a perspetiva com que se olha para a informação, objetivos e motivações. Isso permite adquirir uma visão alargada da situação através de relatórios, partilha de conhecimento e uma compreensão precisa. O Cmdt/Dir/Ch e o EM devem compreender como a cultura organizacional pode afetar a mudança organizacional.

510. *Business Intelligence*

a. Enquadramento

(1) O conceito de *Business Intelligence* (BI) abrange um conjunto de metodologias, processos, arquiteturas e tecnologias usadas para recolher, organizar e transformar os dados brutos em informação significativa e útil usada para obter uma visão estratégica e uma tomada de decisão mais eficaz.

(2) O BI surgiu da necessidade cada vez maior das organizações tornarem o crescente volume dados proveniente de várias fontes, em informação útil, de modo a agilizar e tornar mais eficientes os processos de decisão das organizações. Esta necessidade das organizações fez com que procurassem instrumentos que facilitassem a aquisição, processamento e análise eficazes de grandes quantidades de dados provenientes de diferentes fontes que serviriam de base para a descoberta de novos conhecimentos. De modo a poderem reagir rapidamente às mudanças que ocorrem nos diferentes contextos das suas Operações, as organizações precisam de SI que permitam realizar diferentes análises de causa e efeito nas mesmas. Neste cenário, os SI têm vindo a evoluir dos tradicionais sistemas de suporte à decisão para sistemas de BI altamente inteligentes.

(3) O BI simplifica a descoberta e análise de informações e apresenta as mesmas sob a forma de páginas interativas designadas por *dashboards*, possibilitando que os decisores nos diferentes níveis de uma organização acedam, analisem, colaborem e atuem com mais facilidade nas informações, a qualquer instante e local.

(4) As tecnologias de BI fornecem visões históricas, atuais e preditivas das operações corporativas, podendo lidar com grandes quantidades de dados estruturados e por vezes não estruturados para ajudar a identificar, desenvolver e criar novos conhecimentos estratégicos. Estas tecnologias visam permitir a fácil interpretação dos dados de modo a identificar novas oportunidades e implementar uma

estratégia eficaz com base em *insights*, que podem fornecer às organizações uma vantagem competitiva e maior estabilidade a longo prazo. O BI pode ser usado pelas organizações para oferecer suporte a uma ampla gama de decisões, desde operacionais a estratégicas.

(5) Os sistemas de BI têm vindo a tornar-se um componente permanente na tomada de decisões em várias organizações.

(6) Perante o paradigma de BI, no ano de 2017 foi criado um órgão para o desenvolvimento aplicacional e de BI na entidade do Exército que dirige as CSI, com a responsabilidade de desenvolvimento e coordenação do BI no Exército.

b. Benefícios

O BI apresenta benefícios às organizações dos quais se destacam os seguintes:

(1) Análise mais rápida da informação

As plataformas de BI são projetadas para realizar processamento de grandes quantidades de dados nos servidores da organização. As ferramentas de BI extraem, transformam e carregam os dados de várias fontes para uma base de dados central designada por *data warehous*e (DW) e de seguida pesquisam os dados de acordo com as consultas dos utilizadores nos *dashboards*, permitindo um acesso mais rápido à informação.

(2) Maior eficiência organizacional

O BI oferece aos decisores a capacidade de aceder aos dados e obter uma visão holística das Operações e atividades. Com esta visão os decisores podem identificar novas informações e conhecimentos e tomar decisões de modo a melhorar a eficiência da organização.

Com as ferramentas de BI as organizações gastam menos horas na análise de dados e na compilação de relatórios, rentabilizando tempo, permitindo utilizar os dados de modo a encontrar e implementar novas soluções.

(3) Decisões baseadas em dados

O BI fornece um acesso mais fácil e rápido a dados precisos e atualizados que podem ser visualizados sobre várias dimensões e indicadores em visuais interativos que permitem tomar melhores decisões.

(4) Maior satisfação dos utilizadores

As U/E/O despendem menos tempo a responder às solicitações de informação das várias áreas. As U/E/O que não tinham acesso aos seus próprios dados, tendo necessidade de o solicitar a outras entidades, podem com estas novas tecnologias realizar a análise de dados de uma forma mais rápida e simplificada, necessitando

de reduzida formação. O BI foi projetado para ser escalável, fornecendo soluções para as entidades que necessitam de dados aos vários níveis. O *software* de BI permite uma experiência de utilizador otimizada e intuitiva para que utilizadores não técnicos visualizem os dados.

(5) Dados confiáveis e controlados

Os sistemas de BI melhoram a organização e análise de dados. Na análise de dados tradicional, os dados de diferentes departamentos são isolados e os utilizadores têm que aceder a várias fontes de dados para responder às suas necessidades. Com as plataformas de BI modernas é possível combinar todas estas fontes de dados num único DW e os vários organismos podem aceder aos mesmos dados de uma só vez.

c. Implementação

O BI encontra-se implementado no Exército através de um conjunto de ferramentas e mecanismos que permitem a extração, transformação e carregamento de dados (ETL) num DW. A partir do DW são criados vários modelos de dados que são usados para o desenvolvimento de *dashboards*.

Para o desenvolvimento de *dashboards* são utilizadas ferramentas proprietárias de *BI* que possibilitam de uma forma intuitiva usar os dados provenientes do DW e de outras fontes para criar visuais interativos, que permitem de uma forma simples e rápida visualizar os dados de forma agregada em métricas que podem ser filtradas por várias dimensões. No âmbito do Exército, encontram-se materializados na área de Apoio à Decisão do Portal de Intranet onde se encontram *dashboards* das áreas “Produto Operacional”, “Recursos Humanos”, “Finanças”, “Logística” e “Formação”.

Página intencionalmente em branco

ANEXO A – GLOSSÁRIO DE TERMOS

As definições que se seguem advêm dos documentos fundamentais de CSI da OTAN ou são utilizadas em função do propósito da presente publicação.

	A
Arquitetura	Organização fundamental de um sistema refletido nos seus componentes e nas relações entre eles, na sua relação com os restantes sistemas, bem como os princípios que orientam o seu desenho e evolução.
	B
Battlefield Managment System	Sistema de informação para Operações que interliga as Unidades escalão Batalhão aos escalões Companhia e Pelotão, interliga-se ao HMS e ao DSS-C2, permitindo a troca de informação para implementar a COP e contribui para melhorar a perceção da situação operacional (*Situational Awareness*).
	C
Centro de Sistemas Operacionais	Designação atribuída aos *data centers* do Exército. O CSO é o local onde estão residentes os serviços de informação comuns, os serviços de Rede, os serviços de comunicações, as aplicações, as bases de dados, o armazenamento de informação e os sistemas de comunicações que asseguram a continuidade dos mesmos, e cujo modelo ideal obriga a uma disponibilidade permanente.
Ciberespaço	Domínio global dentro do Ambiente Informacional que consiste na interdependência de redes e infraestruturas de tecnologia de informação, tais como a internet, redes de computadores, entre outros.
Comando	É o processo pelo qual a vontade do Cmdt, os planos, e as intenções são transmitidas aos subordinados. O Comando engloba a autoridade e a responsabilidade para projetar Forças no cumprimento de uma determinada missão.
Conhecimento Explícito	Conhecimento formalmente documentado, organizado e transferido para os outros através de meios digitais ou não digitais. O conhecimento explícito tem regras, limites e significados precisos. São exemplos: documentos de

	computador, dicionários, livros didáticos e publicações doutrinárias do Exército.
Conhecimento Tácito	O conhecimento tácito é aquele que as pessoas detêm; um acervo único e pessoal, de conhecimentos adquiridos a partir de experiências de vida, formação e redes de contactos.
Controlo	É o processo através do qual o Cmdt, assistido pelo seu EM, organiza, dirige e coordena as atividades das Forças que lhe são atribuídas. Para alcançar este objetivo o Cmdt e o seu EM utilizam procedimentos normalizados, em conjugação com o equipamento CSI disponível.
Comando e Controlo	Os processos de Comando e Controlo constituem o Sistema que o Cmdt, EM e subordinados utilizam para planear, dirigir, coordenar e controlar as Operações.
	D
Dismounted Soldier System	Sistema de informação para Operações utilizado pelo combatente apeado, normalmente, pelos Cmdt de Pelotão e de Secção, contribui para a COP e permite a receção da informação necessária ao desempenho da sua missão.
Domínio Não Classificado	Integra a infraestrutura CSI não classificada dos Sistemas de Informação e Comunicações do Exército, SIC-Op e SIC-T, com acesso à internet, destinados a garantir o processamento, armazenamento e transmissão de informação não classificada.
Domínio Classificado	Integra a infraestrutura CSI classificada dos SIC do Exército, SIC-Op e SIC-T, sem acesso à internet, destinados a garantir o processamento, armazenamento e transmissão de informação com classificação de segurança até SECRETO, nas diversas marcas de classificação de segurança.
Domínio de Missão	Estabelecido para uma missão específica no tempo e no âmbito de nações da OTAN e entidades não pertencentes à OTAN (governamentais ou não governamentais), que integram as infraestruturas CSI específicas da missão, sendo as políticas de implementação estabelecidas e acordadas por todos os participantes. Dependendo da situação, das tarefas da missão e das entidades participantes, um domínio de missão pode ou não ter um caráter subsidiário em relação aos domínios da OTAN.

	F
Federação de Redes	Agregação de múltiplas redes independentes que têm diferentes ou iguais características técnicas, procedimentos ou segurança. Essas redes são estabelecidas e operadas independentemente, no entanto, elas seguem os padrões e protocolos acordados para executar a operação adequada da Rede abrangente como um todo.
Federated Mission Networking	Abordagem da OTAN para unificar redes de diferentes membros de uma coligação para fornecer serviços de troca de informações, permitir troca de informação entre os membros da coligação e orientar o estabelecimento de relações da Rede de missão entre a OTAN, nações da OTAN e entidades não-OTAN nas quais se podem realizar toda a gama de atividades operacionais dentro das Operações lideradas pela OTAN.
	G
Gestão de Conhecimento	É a arte de criar, organizar, aplicar e transferir conhecimento para facilitar a compreensão situacional e a tomada de decisão. A gestão do conhecimento apoia a melhoria organizacional, a inovação e performance.
Gestão da Informação	É a ciência do uso de procedimentos e SI para receber, processar, analisar, armazenar, divulgar e proteger produtos de conhecimento, dados e informações, assim como, a produção de informações oportunas e a disseminação de informações protegidas relevantes para os Cmdt e EM.
Guerra de Informação	A capacidade de Ciberdefesa, GE e a implementação de medidas que garantam a segurança da informação, das comunicações e dos sistemas e tecnologias de informação no âmbito das operações em redes de computadores e a pronta resposta e investigação de incidentes, asseguram a garantia da informação.
Guerra Eletrónica	A guerra eletrónica visa a utilização de energia eletromagnética com a finalidade de controlar o espectro eletromagnético ou atacar o adversário/inimigo, subdividindo-se em três tipologias distintas de atividades: ataque eletrónico, proteção eletrónica e apoio eletrónico.

	H
Headquarters Managment System	Sistema de informação para Operações que interliga os escalões Batalhão e superiores até Corpo de Exército, garantindo a interoperabilidade com sistemas C2 aliados.
	I
Informação	Conhecimento sobre objetos (por exemplo: factos, eventos, processos ou ideias e conceitos) que, dentro de um determinado contexto, têm um significado particular.
Information Exchange Requirements	Os IER definem as necessidades para troca de informação entre duas ou mais entidades envolvidas num determinado processo. Os IER descrevem a origem e destino do fluxo de informação, o conteúdo e, normalmente, outras características do fluxo de informação (formato, classificação de segurança, tamanho, atributos, entre outros).
	M
Metadados	Um conjunto de dados que descreve e dá informações sobre outros dados.
Módulo de Estado-Maior	Conjunto de equipamentos terminais, necessários à montagem do PC do escalão respetivo, materializando-se num conjunto de equipamentos tais como telefones, impressoras, computadores, projetores, etc.
	N
NATO *Network Enabled Capability*	Conceito NATO para as operações centradas em Rede.
Network Centric Operations	Conceito relativo a uma operação apoiada / valorizada pela Rede (infraestrutura tecnológica e pessoas colaborativas numa estrutura organizacional).
Network Centric Warfare	Materializa o NCO numa Operação militar.
	O
Operações de Informação (INFO OPS)	Ações coordenadas que visam influenciarem os decisores e o processo de decisão do inimigo ou terceiros, em apoio dos nossos objetivos políticos e militares, afetando os seus sistemas de Comando e Controlo e Informações (C2I) e os seus Sistemas de Informação e Comunicações (SIC), ao mesmo tempo que exploram/protegem os nossos sistemas C2I e SIC.

	R
Rede de Dados do Exército	Componente do Sistema de Comunicações de nível operacional, garante a ligação em malha das Redes locais das U/E/O do Exército, bem como a ligação às Redes exteriores. Assenta no estabelecimento de um ambiente de Rede suportado nos protocolos IP, o qual permite suportar toda a gama de serviços de Rede e aplicações, nas componentes de voz, dados e vídeo, sendo responsável pelo roteamento da informação no SIC-Op.
Rede de Transmissão do Exército	Componente do Sistema de Comunicações de nível operacional, é uma estrutura de comunicações de suporte ao transporte de dados, sem restrições, entre os equipamentos da RDE e simultaneamente possibilitar o acesso a essa informação, às U/E/O e ao SIC-T, ao longo de todo o Território Nacional, com o objetivo de potenciar o exercício do C2 do Exército, nos diferentes níveis das Operações (estratégico, operacional e tático).
Redes Rádio de Combate	Redes de comunicações sem fios implementadas por rádios táticos que interligam diversas entidades, desde o Cmdt da Força até ao mais baixo escalão do combatente individual.
Router	Equipamento de Rede que faz o encaminhamento de pacotes de dados entre redes de computadores
	S
Serviço	Capacidade fornecida para beneficiar ou apoiar comunidades de utilizadores.
Sistema de Comunicações	Conjunto de equipamentos, métodos, procedimentos e, se necessário, pessoal, organizado para assegurar a transmissão de informação entre entidades.
Sistema de Informação	Conjunto de equipamentos, métodos e procedimentos e, se necessário, pessoal, organizados para realizar processamento e armazenamento de informação.
Sistemas de Informação de Gestão	Compostos pelas plataformas que operam dados em grandes volumes com o propósito de apoiar os Órgãos de Comando nas suas decisões, na publicação e divulgação da imagem do

	Exército e na divulgação interna. Dividem-se em SIG de nível Estratégico e SIG de nível Operacional.
Sistemas de Informação para Operações	Compostos pelas plataformas que operam dados com o propósito de apoiar os Órgãos de Comando nas suas decisões em Exercícios, Operações de combate, de estabilização e operações de Apoio Civil (por exemplo, Apoio Militar de Emergência). Dividem-se em SIO de nível Operacional e SIO de nível Tático. Podem também ser designados por SI para o C2.
Sistemas de Informação para o C2	Ver Sistemas de Informação para Operações
Sistema de Informação e Comunicações	Sistema que permite armazenar, processar e transmitir informação e compreende todos os ativos necessários ao seu funcionamento, designadamente infraestrutura, organização, pessoal e recursos.
Sistema de Informação e Comunicações Operacional	Sistema integrador de natureza estrutural, no nível operacional, das componentes de Comunicações, de Informação e de Segurança dos Sistemas de Informação e Comunicações.
Sistema de Informação e Comunicações Tático	Sistema integrador de natureza conjuntural, no nível tático, das componentes de Comunicações, de Informação e de Segurança dos Sistemas de Informação e Comunicações.
Subsistema de Área Estendida	Subsistema do SIC-T, constitui a espinha dorsal (*backbone*) da Rede, composto por um conjunto de Nós de comutação interligados, fundamentalmente por ligações (links) rádio multicanal (Feixes Hertzianos) ou, em casos específicos, com terminais de satélite de banda larga.
Subsistema de Área Local	Subsistema do SIC-T, proporciona a um determinado grupo de utilizadores, normalmente localizados num PC de um determinado escalão de forças, as diversas categorias de serviços (voz, dados, C2, mensagens ou vídeo) disponíveis em cada domínio de informação e, adicionalmente, garante o acesso do PC apoiado à estrutura superior da Rede (SAE) através de um conjunto de Nós de acesso.
Subsistema de Utilizadores Móveis	Subsistema do SIC-T, garante os serviços de voz e dados aos utilizadores móveis disseminados pela área de Operações que

	não possuam ligação ao SAL, o que implica a utilização de meios de transmissão sem fios de propagação não diretiva.
Superioridade de Informação	Situação de vantagem no domínio da informação, resultante da capacidade para reunir, processar e disseminar um fluxo ininterrupto de informação enquanto se explora ou nega a capacidade de um competidor/adversário poder fazer o mesmo.
Switch	Equipamento de Rede que liga dispositivos numa Rede de computadores, recebendo pacotes de dados e encaminhando-os para o dispositivo de destino.
	T
Tecnologias de Informação e Comunicações	Conjunto de artefactos tecnológicos com que instrumentamos o habitat humano, que facilitam e aumentam as capacidades individuais e coletivas na comunicação, na recolha, no tratamento, na preservação de informação e no suporte às ações que desencadeamos em consequência das decisões que tomamos, nos diversos contextos em que nos situamos ao longo do tempo (Tribolet, 2011).
	W
Wiki	Um *site* que permite a fácil criação e edição de um rol de páginas *web* interligadas através de um navegador *web*. Os *wikis* são geralmente acionados por um *software wiki* e frequentemente são usados para criar *sites* colaborativos *wiki*, alimentar *sites* de comunidades, tomada de notas pessoais, em redes corporativas internas e em sistemas de gestão do conhecimento.

Página intencionalmente em branco

ANEXO B – LISTA DE ABREVIATURAS E ACRÓNIMOS

ABREVIATURA	TERMO OTAN *(ou em Inglês)* (*)	TERMO EXÉRCITO
	A	
AC	*Alternating Current*	Corrente Alternada
AE	---	Ataque Eletrónico
AAP	*Allied Administrative Publication*	---
ACP	*Allied Communications Publication*	---
AJP	*Allied Joint Publication*	---
	B	
BD	*Database*	Base de Dados
BI	*Business Intelligence*	---
BMS	*Battlefield Management System*	---
	C	
C2	*Command and Control*	Comando e Controlo
C4I	*Command, Control, Communications, Computers and Information*	Comando, Controlo, Comunicações, Computadores e Informação
CCB	*Battalion Communications Center*	Centro de Comunicações de Batalhão
CCC	*Company Communications Center*	Centro de Comunicações de Companhia
CEMA	*Cyberspace ElectroMagnetic Activities*	Atividades ciber/eletromagnéticas
CEMGFA		Chefe de Estado-Maior General das Forças Armadas
CI	*Communications and Information*	Comunicações e Informação
CISIO	*Communication and Information Systems Infrastructure Operations*	Operações da Infraestrutura de Comunicações e Sistemas de Informação
CISRO	*Cyberspace Intelligence, Surveillance and Reconnaissance Operations*	Operações de Informações, Vigilância e Reconhecimento no Ciberespaço
Cmdt	---	Comandante

Cmdt/Dir/Ch	---	Comandante, Diretor ou Chefe
CME	*Electronic Countermeasures*	Contra Medidas Eletrónicas
Com	---	Comunicações
CONOPS	*Concept of operations*	---
COP	*Common Operational Picture*	Imagem Operacional Comum
CSI	*Communications and Information Systems*	Comunicações e Sistemas de Informação
CRAM	*Counter rocket, artillery, and mortar*	Contra-foguetes, artilharia e morteiros
C-RCIED	*Counter - Radio Controlled Improvised Explosive Device*	---
CSO	---	Centro de Sistemas Operacionais
CRN	*Combat Radio Net*	Rede Rádio de Combate
	D	
DC	*Direct Current*	Corrente Contínua
DClas	---	Domínio Classificado
DCO	*Defensive Cyberspace Operations*	Operações Defensivas no Ciberespaço
DCO-IDM	---	Medidas Defensivas Internas das DCO
DCO-RA	---	Ações de Resposta das DCO
DDNLA	---	Divisão de Doutrina, Normalização e Lições Aprendidas
DE	---	Defesa Eletrónica
DHCP	*Dynamic Host Configuration Protocol*	Distribuição automática de endereços IP
DNClas	---	Domínio Não Classificado
DNS	*Domain Name System*	---
DOTMLPF-I	*Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities – Interoperability*	Doutrina, Organização, Treino, Material, Liderança, Pessoal, Instalações – Interoperabilidade
DSS	*Dismounted Soldier System*	---
DW	*Data Warehouse*	---
	E	
ECOSF	---	Elementos da Componente Operacional do Sistema de Forças

EM		Estado-Maior
EMBat	---	Módulo de Estado-Maior de Batalhão
EMBrig	---	Módulo de Estado-Maior de Brigada
EMCON	*Emission Control*	Controlo de Emissões
EME	*Army Staff Headquarters*	Estado-Maior do Exército
EMGFA	*Armed Forces Staff Headquarters*	Estado-Maior-General das Forças Armadas
EPR	---	Elementos Primariamente Responsáveis
ETL	Extract, Transform, Load	Extração, transformação e carregamento de dados
	F	
FHz	---	Feixes Hertzianos
FMN	*Federated Mission Networking*	---
FND	---	Força Nacional Destacada
	G	
GI	*Information Warfare*	Guerra de Informação
GIC	*Knowledge Management*	Gestão da Informação e do Conhecimento
GE	*Electronic warfare*	Guerra Eletrónica
GU		Grande Unidade
	H	
HF	*High Frequency*	Alta Frequência
HMS	*Headquarters Managment System*	---
HQ	*Headquarters*	Quartel-General
	I	
ID	---	Identificador
IER	*Information Exchange Requirements*	Requisitos de Intercâmbio de Informação
IP	*Internet Protocol*	Protocolo da Internet
IPB	*Intelligence Preparation of the Battlefield*	Preparação do Campo de Batalha pelas Informações
INFO OPS	*Information Operations*	Operações de Informação
IPSEC	*Internet Protocol Security*	Segurança do Protocolo da Internet

	J	
JFC	*Joint Force Command*	Comando de Força Conjunta
	L	
LAN	*Local Area Network*	Rede de Área Local
	M	
MANET	*Mobile AdHoc Network*	---
MAE	---	Medidas de Apoio Eletrónicas
MDN	---	Ministério da Defesa Nacional
METL	*Mission Essential Task List*	Lista de Tarefas Essenciais da Missão
MPE	---	Medidas de Proteção Eletrónica
	N	
NA		Nó de Acesso
NAVWAR	*Naval Information Warfare Systems Command*	Comando de Sistemas de Guerra de Informação Naval
NCO	*Network Centric Operations*	Operações Centradas em Rede
NCW	*Network Centric Warfare*	Guerra Centrada em Rede
NEP	*Standing/Standard Operating Procedure*	Norma de Execução Permanente
NNEC	NATO *Network Enabled Capability*	---
NT	*Transit Node*	Nó de Trânsito
NTP	*Network Time Protocol*	--
	O	
OCC	---	Órgão Central de Comando
OCO	*Offensive Cyberspace Operations*	Operações Ofensivas no Ciberespaço
OpsCiber	---	Operações no Ciberespaço
OTAN	*North Atlantic Treaty Organization*	Organização do Tratado do Atlântico Norte
	P	
PAR	*Radio Access Point*	Ponto de Acesso Rádio
PC	*Command Post*	Posto de Comando
PDE	---	Publicação Doutrinária do Exército
POC	*Point of Contact*	Ponto de Contacto
PRR	*Personal Role Radio*	Rádio Individual

	Q	
QoS	*Quality of Service*	Qualidade de Serviço
	R	
RBE	---	Rádio de Baixos Escalões
RBL	*Broadband Radio*	Rádio de Banda Larga
RDE	---	Rede de Dados do Exército
RF	*Radio Frequency*	Rádio Frequência
RInd	*Personal Role Radio*	Rádio Individual
RL	*Rear-Link*	---
RM	*Multifunctional Radio*	Rádio Multifuncional
RTE	---	Rede de Transmissão do Exército
RTS	---	Rádio Tático de Secção
	S	
SAA	---	Autoridade de Acreditação de Segurança
SAE	---	Subsistema de Área Estendida
SAL	---	Subsistema de Área Local
SI	*Information Systems*	Sistemas de Informação
SIC	*Communications and Informations System*	Sistema de Informação e Comunicações
SIC2	*Command and Control Information System*	Sistemas de Informação para o C2
SIG	--	Sistemas de Informação de Gestão
SIO	--	Sistemas de Informação para Operações
SIC-Op	---	Sistema de Informação e Comunicações Operacional
SIC-T	---	Sistema de Informação e Comunicações Tático
SUM	---	Subsistema de Utilizadores Móveis
	T	
TIC	---	Tecnologias de Informação e Comunicações
	U	
U/E/O	---	Unidade, Estabelecimento ou Órgão

UE	*European Union*	União Europeia
UHF	*Ultra High Frequency*	Frequência Ultra Alta
UPS	*Uninterruptible power supply*	Fonte de Energia Ininterrupta
	V	
VE	---	Vigilância Eletrónica
VHF	*Very High Frequency*	Frequência Muito Alta
VPN	*Virtual Private Network*	Rede Privada Virtual
VSAT	*Very Small Aperture Terminal*	Terminal Comunicações Satélite
	W	
WAN	Wide Area Network	Rede de Área Alargada
WSUS	*Windows Server Update Services*	--

(*) As abreviaturas e os acrónimos OTAN têm plural. O plural forma-se com a adição de um “s” no final, por exemplo: SOP (singular) – SOPs (plural).

Página intencionalmente em branco


EXÉRCITO
PORTUGAL