INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE ESTADO-MAIOR CONJUNTO

2007/2008

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

O TEXTO CORRESPONDE A UM TRABALHO ELABORADO DURANTE A FREQUÊNCIA DO CURSO DE ESTADO-MAIOR CONJUNTO NO IESM, SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DA MARINHA PORTUGUESA / DO EXÉRCITO PORTUGUÊS / DA FORÇA AÉREA PORTUGUESA.

O Sistema de Informação e Comunicações Táctico (SIC-T) do Exército Português. Implicações doutrinárias.

JOÃO ALBUQUERQUE BARROSO
MAJ TM

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

O Sistema de Informação e Comunicações Táctico (SIC-T) do Exército Português. Implicações doutrinárias.

Maj Tm João Barroso

Trabalho de Investigação Individual do CEMC 2007/08

Orientador:
TCOR/TM José Vieira

Lisboa – 2008

Agradecimentos

As minhas primeiras palavras de agradecimento vão para os entrevistados, digníssimos oficiais das Forças Armadas Portuguesas com responsabilidades nas áreas de Sistemas de Informação e Comunicações, pela oportunidade e brilhantismo que deram a este trabalho, contribuindo para o enriquecimento do conteúdo do mesmo.

As seguintes são dirigidas aos meus camaradas do Curso de Estado Maior Conjunto 2007/2008, pelo prazer de ter privado da vossa companhia e do espírito de entreajuda e camaradagem. O meu eterno agradecimento, pois muito do que fiz só foi possível graças aos vossos contributos e permanente disponibilidade para troca de ideias e opiniões.

Ao meu orientador, o Sr. TCor Tm José Veira, os meus sinceros agradecimentos pela permanente disponibilidade e liberdade académica com que encarou esta tarefa.

Ao Sr. Director do Curso de Curso de Estado Maior Conjunto 2007/2008, Cor Xavier de Sousa, pelo apoio que me deu num momento difícil.

E acima de tudo, à minha família: à Manuela, à Joana e ao João Pedro pela paciência que tiveram comigo durante estes últimos 16 meses.

A todos, muito obrigado.

Índice

1. Introdução 1
2. Generalidades e Conceitos de Transmissões 3
a. A necessidade de um novo Sistema de Informação e Comunicações Táctico 3
b. O papel dos Sistemas de Informação e Comunicações na acção de C2 5
c. Network Centric Warfare e NATO Network Enabled Capability 9
d. A Guerra da Informação 11
e. Funções e Princípios dos SIC 16
(1) Interoperabilidade 18
(2) Agilidade 19
(3) Confiança 19
(4) Partilha 22
3. Emprego Táctico das Transmissões 23
a. O sistema *Mobile Subscriber Equipment* do Exército dos EUA 23
b. O conceito LandWarNet do Exército dos EUA aplicado aos *Brigade Combat Teams* 25
c. Enquadramento Conceptual e estruturas lógicas dos módulos SIC-T 30
(1) O Subsistema de Área Estendida 31
(2) O Subsistema de Área Local 32
(3) O Subsistema de Utilizadores Móveis 35
(4) O Subsistema de Segurança de Rede 37
(5) O Subsistema de Gestão de Rede 37
d. O SIC-T na manobra da brigada 38
(1) Relações de comando e apoio das unidades de Transmissões 39
(2) Operações de Combate Ofensivas 40
(3) Operações de Combate Defensivas 41
(4) Operações de Estabilização 42
4. Conclusões 44
5. Bibliografia 47

Índice de Figuras

Figura 1- Organização de um Sistema de C2 em 3 níveis Ap2-1
Figura 2 - Esquema Funcional do NII baseado no modelo OSI. Ap2-1
Figura 5 - Arquitectura do sistema MSE Ap2-3
Figura 6 - Constituição das BCT Ap2-3
Figura 7 - Apoio SIC de uma SBCT Ap2-4
Figura 8 - O SIC-T e os seus subsistemas Ap2-4
Figura 9 - Módulo Nó de Trânsito Ap2-5
Figura 10 - Módulo *rear link* Ap2-5
Figura 11 - Módulo Genérico do Nó de Acesso Ap2-6
Figura 12 - Shelter de Transmissão do Nó de Acesso Ap2-6
Figura 13 - Shelter de C2 e Gestão do Nó de Acesso Ap2-7
Figura 14 - Módulo do Centro de Comunicações do Batalhão Ap2-7
Figura 15 - Shelter de "Transmissão" do Centro de Comunicações de Batalhão Ap2-8
Figura 16 - Shelter de "C2 & Gestão" do Centro de Comunicações de Batalhão Ap2-8
Figura 17 - Módulo do Centro de Comunicações de Companhia Ap2-9
Figura 18 - Módulo do Ponto de Acesso Rádio Ap2-9
Figura 19 - Organigrama de CTm de Brigada Ap2-10
Figura 20 - Organigrama da CTm Apoio Ap2-10
Figura 21 - Exemplo do apoio de comunicações a uma Brigada Ap2-11
Figura 22 - Movimento de nós SAE Ap2-11
Figura 23 - Movimento de PAR Ap2-12
Figura 24 -Exemplo de movimento de um PC, sem duplicação de elementos Ap2-12
Figura 25 - O assinante restabelece a ligação (reafilia-se) noutro terminal Ap2-13
Figura 26 - Terminal, com assinante, restabelece a ligação noutro ponto de acesso .. Ap2-13
Figura 27 - Mover para outro PAR Ap2-13
Figura 28 - Funções de segurança de equipamentos de cifra IP Ap3-2
Figura 29 - Núcleo Protegido constituído a partir de múltiplos segmentos Ap3-4
Figura 30 - Expansão do núcleo Ap3-7
Figura 31 – Nível de Maturidade 1 ..... Ap3-9
Figura 32 – Nível de maturidade 2 ..... Ap3-10
Figura 33 – Nível de maturidade 3 ..... Ap3-11
Figura 34 - Equipamento NINE utilizado para conexões em múltiplos cenários Ap3-12

Figura 35 - Princípio de nó auto-protegido Ap11-1

Índice de Tabelas

Tabela 1: Critérios de Qualidade da Informação……...……6
Tabela 2: Elementos/Capacidades das Operações de Informação – NATO……....16
Tabela 3: Sub-redes existentes na Brigada Stryker…...……...28

Índice de Apêndices

Apêndice 1: Entrevistas realizadas
Apêndice 2: Figuras
Apêndice 3: Segurança dos Sistemas de Comunicações e Informação
Apêndice 4: Arquitectura de Segurança em Redes IP NATO
Apêndice 5: Funcionamento de uma Infra-estrutura PKI
Apêndice 6: O conceito LandWarNet do Exército dos EUA
Apêndice 7: Responsabilidade para Estabelecimento de Comunicações
Apêndice 8: Possibilidades das CTm da FOPE
Apêndice 9: Possíveis cenários de Interoperabilidade e Mobilidade no SIC-T
Apêndice 10: Serviços Disponibilizados nos Diferentes Domínios de Rede
Apêndice 11 - Proposta de Arquitectura de Segurança de Rede para o SIC-T

Índice de Anexos

Anexo 1: TACOMS 2000 Top Level Architecture

Resumo

Neste estudo foi empregue o método científico, com recurso ao modelo dedutivo, para se encontrar resposta ao problema em análise, consubstanciado na questão central "*A doutrina das Transmissões de Campanha no Exército Português altera-se substancialmente com a adopção do Sistema de Informação e Comunicações-Táctico?*".

O estudo está organizado em duas partes dotadas de um encadeamento lógico: na primeira, denominada de generalidades e conceitos de Transmissões, abordam-se as razões que levaram à necessidade de um novo sistema de informação e comunicações táctico para o Exército, bem como dois conceitos enquadrantes da nova realidade das comunicações militares, a guerra da informação e as operações centradas em rede. Com base nestes conceitos avança-se para uma definição de funções e princípios que guiam os Sistemas de Informação e Comunicações na actualidade.

Na segunda parte é abordado o emprego táctico das transmissões, estudando-se os sistemas *Mobile Subscriber Equipment* e o conceito de *LandWarNet* aplicado às novas brigadas norte-americanas. Após um enquadramento conceptual e uma análise à estrutura lógica e modular do Sistema de Informação e Comunicações-Táctico, apresenta-se um possível emprego do mesmo na manobra de uma brigada.

Conclui-se que, face à nova filosofia modular do Sistema de Informação e Comunicações-Táctico, à sua utilização de protocolos standard, à sua capacidade de implementação de serviços diferenciados e à sua versatilidade e potencial interoperabilidade, ***a doutrina das transmissões de campanha no Exército se altera substancialmente com a adopção do Sistema de Informação e Comunicações-Táctico.***

Em complemento, apresentam-se contributos para a implementação da componente de segurança no Sistema de Informação e Comunicações-Táctico.

Abstract

In this study a scientific methodology was used, resorting to a deductive model to find an answer to the problem in analysis summed up in the main question: *"Does the introduction of the Tactical Communications and Information System significantly change the tactical signal support doctrine in the Portuguese army?"*

The study is organized in two parts according to a logical sequence: in the first one, named signals concepts and generalities, the reasons behind the need of a new Army tactical communications and information system are addressed, as well as two structuring concepts of the new military communications environment, information warfare and network centric operations. Starting from these concepts the study moves on to define the new functions and principles that drive Communications and Information Systems nowadays.

In the second part the study addresses the tactical employment of signals, by studying the *Mobile Subscriber Equipment* system and the *LandWarNet* concept as applied to the new North American brigades. Following a conceptual framing and an analysis of the modular and logical structure of the Tactical Communications and Information System, its possible employment in the brigade maneuver is presented.

It is concluded that, because of the Tactical Communications and Information System's modular philosophy, its adherence to standard protocols, its differentiated services implementation capability and its potential versatility and interoperability, *the introduction of Tactical Communications and Information System significantly changes the tactical signal support doctrine in the Portuguese army.*

In addition, some contributions to the implementation of the security component of Tactical Communications and Information System are presented.

Palavras Chave

Sistema de Informação e Comunicações

Operações Centradas em Rede

Operações de Informação

Conjunto

Combinado

Interoperabilidade

Apoio de Transmissões

Lista de Abreviaturas

ABCS	*Army Battle Command System*
AC	Autoridade Certificadora
ACCS1	*Allied Command and Control System 1*
ACUS	*Area Common-User System*
A/D	Apoio Directo
ADAMS	*Allied Deployment And Movement System*
AEHF	*Advanced Extreme High Frequency*
A/G	Apoio Geral
ANS	Autoridade Nacional de Segurança
AViD	Áudio, Video e Dados
BCT	*Brigade Combat Team*
BE	*Bulk Encryption*
BFT	*Blue Force Tracker*
BICES	*Battlefield Information, Collection, & Exploitation System*
BPD	Baixa probabilidade de detecção
BPI	Baixa probabilidade de intercepção
BPS	*Boundary Protection Service*
BTCOM	*Battle Command on the Move*
BVTC	*Battlefield Video Tele-Conferencing*
C2	Comando e Controlo
C2W	*Command and Control Warfare*
C4ISR	*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*
CCB	Centro de Comunicações de Batalhão
CCC	Centro de Comunicações de Companhia
CCIS	*Command and Control Information System*
CCOM	Centro de Comunicações
CE	Corpo de Exército
CIMIC	*Civilian and Military Cooperation*
CIS	*Communications and Information Systems*
CMDT	Comandante
CMSM	Campo Militar de Santa Margarida
CNR	*Combat Net Radio*
COT	Centro de Operações Táctico
COTS	*Commercial Off The Shelf*
CSI	Comunicações e Sistemas de Informação
CTmAp	Companhia de Transmissões de Apoio
DCSI	Direcção de Comunicações e Sistemas de Informação
DNS	*Domain Name System*
DTMF	*Dual Tone Multi Frequency*
EHF	*Extreme High Frequency*
EME	Estado Maior do Exército
EMGFA	Estado Maior General das Forças Armadas
EPLRS	*Enhanced Position Location Reporting System*
FA	Forças Armadas
FBCB2	*Force XXI Battle Command Brigade and Below*
FEC	*Forward Error Correction*

GCM	Grupo de Comando Móvel
GestInfo	Gestão da Informação
GEA	Grande Extensão de Acesso
GI	Guerra da Informação
GIG	*Global Information Grid*
GPS	*Global Positioning System*
GRSTA	*Ground Reconnaissance, surveillance, and targetting aquisition.*
HF	High Frequency
HICON	*Higher Control*
HMMWV	*High Mobility Multipurpose Wheeled Vehicle*
HVT	*High Value Target*
IA	*Information Assurance*
IAEM	Instituto de Altos Estudos Militares
ICC	*Integrated Command and Control*
IDS	*Intrusion Detection System*
IEG	*Information Exchange Gateway*
IM	*Information Management*
INFOOPS	*Information Operations*
IOC	Imagem Operacional Comum
IO	*Information Operations*
IP	*Internet Protocol*
IPsec	*Internet Protocol Security*
IPv6	*Internet Protocol Version 6*
ISP	*Internet Service Provider*
ISSO	*International Organization for Standardization*
ISTAR	*Intelligence, Surveillance, Targetting, Acquisition and Reconnaissance*
ISYSCON	*Integrated System Control*
IT	*Information Technology*
IW	*Information Warfare*
JCOP	*Joint Common Operational Picture*
JFLCC	*Joint Force Land Component Commander*
JNN	*Joint Network Node*
JTRS	*Joint Tactical Radio System*
JWICS	*Joint Worldwide Intelligence Communications System*
LEO	*Low Earth Orbit*
LOCE	*Linked Operational Intelligence Centers Europe*
LWN	*LandWarNet*
MCCIS	*Military Maritime Command and Control system*
MCS	*Maneuver Control System*
MEO	*Medium Earth Orbit*
GEOMETOC	*Geological and Meteoroligical Conditions*
MILSTAR	*Military Strategic and Tactical Relay*
NA	Nó de Acesso
NAC	Conselho do Atlântico Norte
NC3A	*NATO Consultation, Command and Control Agency*
NC3B	*NATO Consultation, Command and Control Board*
NCW	*Network Centric Warfare*
NEC	*Network Enabled Capability*
NINE	*NNEC NII IP Network Encryption*

NNEC	*NATO Network Enabled Capability*
NNEC –FS	*NATO Network Enabled Capability Feasability Study*
NNI	*Networking and Information Infrastrucure*
NNNI	*NATO Networking and Information Infrastructure*
NP	Núcleo Protegido
NRF	*NATO Response Forces*
NSA	*National Security Agency*
NSWAN	*NATO Secret Wide Area Network*
NT	Nó de Trânsito
OAZR	Orla Anterior da Zona de Resistência
ONG	Organização Não-Governamental
OSI	*Open Systems Interconnection*
PAR	Ponto de Acesso Rádio
PC	Posto de Comando
PCPrinc	Posto de Comando Principal
PCTact	Posto de Comando Táctico
PEA	Pequena Extensão de Acesso
PKI	*Public Key Infrastructure*
PNR	Protecção do Núcleo da Rede
RDE	Rede de Dados do Exército
RL	*Rear Link*
ROE	Regra de Empenhamento
SAE	Subsistema de Área Estendida
SAL	Subsistema de Área Local
SATCOM	*Satellite Communications*
SecOP	*Security Operating Procedures*
SGR	Subsistema de Gestão de Rede
SHDSL	*Symetric High-Speed Subscriber Line*
SIBE	Sistema de Informação para Baixos Escalões
SIC	Sistema de Informação e Comunicações
SICOM	Sistema Integrado de Comunicações Militares
SIC-E	Sistema de Informação e Comunicações – Estratégico
SIC-T	Sistema de Informação e Comunicações – Táctico
SINCGARS	*Single Channel Ground and Airborne Radio System*
SITACO	Sistema de Comunicações Táctico
SLA	*Service Level Agreement*
SNPC	Serviço Nacional de Protecção Civil
SOA	*Service Oriented Architecture*
SPI	Sistema Político Internacional
SSA	*Shared Situational Awareness*
SSR	Subsistema de Segurança de Rede
SUM	Subsistema de Utilizadores Móveis
TACP	*Tactical Air Controller Party*
TACSAT	*Tactical Satellite*
TETRA	*Terrestrial Trunked Radio*
TI	Tecnologias de Informação
Tm	Transmissões
TOA	*Transformational Objective Areas*
TSWG	*TACOMS Security Working Group*
UAV	*Unmanned Aerial Vehicle*

UEB	Unidade de Escalão Batalhão
UEC	Unidade de Escalão Companhia
VHF	Very High Frequency
VHF-FM	Very High Frequency – Frequency Modulation
VPN	*Virtual Private Network*
VTC	Video Tele Conferência
WIN-T	*Warfighter Information Network-Tactical*
WISE	*Worldwide Information System Exchange*

1. Introdução

> *"The edge in the competition will flow from the speed of inovation, the willingness to change, and the agility in integrating the technology with changes in military structure, organization and operational concepts that can take advantage of what techology offers."*
>
> *Arthur Cebrowski, Vice-almirante USN*

O objectivo primário das comunicações é «SERVIR O COMANDO». A arquitectura e as capacidades do novo Sistema de Informação e Comunicações Táctico (SIC-T) irão obrigatoriamente alterar o apoio de Transmissões (Tm) no Exército Português. Este sistema foi concebido e irá ser implementado como o pilar base de dois conceitos fundamentais para as futuras operações do Exército: Guerra Centrada em Rede (*Network Centric Warfare - NCW*) e Guerra da Informação (GI). Estes dois conceitos estão presentes em todos os modernos SIC-T a nível internacional.

A componente de Comunicações é por outro lado contemporaneamente indissociável da componente Informação, o que por si só é suficiente para alterar o conceito de Apoio de Transmissões para Apoio de SIC. Acontece porém que as publicações em vigor que versam sobre a Táctica de Transmissões são demasiado generalistas ou estão obsoletas, contendo conceitos de apoio, estruturas e sistemas de transmissões bastante ultrapassados. Neste quadro, torna-se assim necessário rever a doutrina e situar as transmissões no contexto actual da Guerra Centrada em Rede, da Guerra da Informação e do novo SIC-T do Exército Português. Urge igualmente redefinir as subdivisões do Apoio de Tm (Comunicações, Sistemas de Informação, INFOSEC[1]) e definir o papel dos SIC no âmbito do Comando e Controlo (C2). É também indispensável aclarar o novo emprego táctico das Tm nas diversas operações militares em que o Exército se pode ver envolvido.

O ***objectivo deste estudo*** foi o de contribuir para a elaboração da doutrina das Transmissões de Campanha nos campos de **Conceitos de Apoio de Sistemas de Informação e Comunicações**, **Emprego Táctico das Tm em Operações** e **Segurança dos Sistemas de Informação e Comunicações**.

[1] Termo em inglês - *Information Security*, que compreende a segurança dos computadores, das comunicações e redes. Designa a protecção da informação nos sistemas de comunicação, nos sistemas de informação e noutros sistemas electrónicos (tais como sistemas de sensores) por forma a manter a confidencialidade, a integridade e a disponibilidade da informação (EME, 2005: A-9).

A proposta de realização deste estudo partiu da nossa compreensão de que é necessário rescrever a doutrina de Apoio Táctico de Transmissões no Exército à luz da nova realidade introduzida pelo SIC-T.

A metodologia assentou numa pesquisa documental e bibliográfica e em entrevistas a entidades ou personalidades que, pela sua experiência relacionada com estes assuntos ou pela função desempenhada em estruturas conjuntas e combinadas, nacionais e internacionais, podiam contribuir para o esclarecimento desta questão.

No âmbito deste trabalho, ***delimitou-se*** o estudo à doutrina NATO e á doutrina dos EUA. Não se investigou igualmente SICs de outros ramos das FAs.

Concluída esta fase foi possível definir a questão central que orientou o resto da investigação: **A doutrina das Transmissões de Campanha no Exército Português altera-se substancialmente com a adopção do SIC-T?**

Associada a esta questão central, surgiu um conjunto de questões derivadas, que de alguma forma contribuíram para a construção deste trabalho de investigação:

(1) Quais são os novos conceitos de apoio introduzidos pelo SIC- T?

(2) Como deverá ser efectuado o emprego táctico das Transmissões em operações?

(3) Qual a nova arquitectura de segurança para o SIC-T?

Para dar resposta à questão central e às questões derivadas, foi construído um modelo teórico de análise, que permite deduzir o modelo estrutural que melhor se adequa aos interesses de uma organização a partir da caracterização de um conjunto de variáveis base. Esse modelo teórico tem também como objectivo testar as seguintes hipóteses:

(1) Com a introdução de novos sistemas, novas tecnologias e de princípios como a NCW e a GI, e a participação em Operações Conjuntas e Combinadas (OCC), o apoio de SIC no Exército passa a ser encarado de forma diferente da realidade actual, constituindo-se o novo SIC-T do Exército Português como um componente fundamental mas não único.

(2) Os componentes do SIC-T reflectem uma organização modular, muito diferente da anterior estrutura de Tm que preconizava um apoio mais estático assente em Centros de Comunicações (CCom) de Comando e CCom de Área. Esta organização modular irá alterar a forma como é prestado o apoio de SIC nas operações militares, permitindo uma maior flexibilidade, e facilitando a integração com outros sistemas (combinados e conjuntos).

(3) A nova arquitectura de segurança para o SIC-T reflecte as últimas inovações na área de segurança de redes integradas de voz, vídeo e dados.

2. Generalidades e Conceitos de Transmissões

a. A necessidade de um novo Sistema de Informação e Comunicações Táctico

O acentuado progresso da tecnologia da Idade da Informação, com especial ênfase na área das telecomunicações e dos sistemas informáticos de elevado desempenho e capacidade de armazenamento, acoplado ao desenvolvimento de sistemas de armas cada vez mais poderosos e precisos, fazem com que actualmente no espaço de batalha ocorram frequentes mudanças de situação e que o ritmo das operações seja cada vez mais elevado. Tal facto obriga a que os sectores da Defesa à escala mundial procurem fazer pesquisa contínua na tentativa de optimizar o exercício do C2 no campo de batalha moderno (DST, 2003: 3-5).

As modernas Tecnologias da Informação (TI) afectam o C2 pela integração da tecnologia, estruturas de comando, e procedimentos, para apoiar o Comandante (CMDT) e aumentar a eficácia a todos os níveis de Comando. Os CMDTs devem definir qual a informação necessária para um C2 efectivo; ao mesmo tempo, devem reconhecer as vulnerabilidades que as TI acarretam, já que estas transformam os SIC num alvo de elevado valor (HVT)[2]. Por definição, as funções de C2 são realizadas através de um conjunto de pessoal, equipamento, comunicações, instalações e procedimentos, empregues pelo CMDT, no planeamento, direcção, coordenação e controlo das forças e das operações no cumprimento da missão. Na figura 1, pode ver-se a decomposição das funções de C2 em três níveis ou camadas, que se integram e complementam, através de interfaces em "diálogo" vertical, respectivamente, solicitando serviços de cima para baixo e fornecendo serviços de baixo para cima (DST, 2003: 4):

No **Nível 1** - As Comunicações, como infra-estrutura de transporte da Informação;

No **Nível 2** - O CCIS (Sistema de Informação de C2), onde através de *software* aplicacional, se trabalha toda a informação para ajuda à tomada de decisão;

No **Nível 3**- O CMDT, a componente Humana, com capacidade de chefia e liderança, para tomar decisões.

O futuro cenário operacional, quer de guerra ou não guerra (CRO[3]), será menos denso, multi-direccional e multi-dimensional (contíguo e não contíguo), com ênfase acrescida para operações conjuntas e combinadas, e com múltiplos agentes. Tal facto implica a necessidade de operação com forças mais dispersas, sobre grandes áreas ou zonas

[2] HVT - *High Value Target*
[3] CRO - *Crisis Response Operations*

de interesse e de operações, maior extensão e profundidade das infra-estruturas de comunicações e, consequentemente, com necessidade de um maior nível de coordenação.

A Informação deve circular, quer na vertical quer na horizontal, entre todas as entidades do cenário operacional, incluindo organizações militares, organizações governamentais não-militares, organizações não-governamentais e organizações de nações anfitriãs. Para assegurar uma acção coesa e evitar erros que poderiam inverter o progresso em curso nesses ambientes sensíveis, todas as organizações trabalham sobre os mesmos dados, devendo ter uma pertinente visão comum para uma determinada área operacional.

Os CCIS podem não só processar grandes quantidades de informação, necessária à realização dessa visão comum, como também devem processá-la de uma maneira rápida e oportuna. Neste contexto, a eficácia da capacidade de C2, com a garantia de interoperabilidade entre as formações, realizada através da troca de informação pertinente, relevante e oportuna, é vital para o eficaz desempenho do processo de decisão militar. Para o Exército Português foi eleito como prioritário o âmbito táctico e, nesse sentido, a capacidade de C2 insere-se no conceito integrado de SIC-T, com garantia de interoperabilidade ao nível conjunto e combinado, e que contempla:

(1) Aplicações operacionais devidamente integradas e com interface simples e amigável para os utilizadores, em especial nas componentes das células de Estado Maior (G1, G2, G3, G4...G6), a dois níveis:
   (a) Um Sistema de Informação de C2 (SICCE[4]);
   (b) Um Serviço de Mensagens ou correio electrónico militar, p. ex. MMHS[5].

(2) Uma infra-estrutura de transporte da informação, isto é, de comunicações tácticas, de acordo no essencial com os objectivos e requisitos do SITACO[6].

Assim, na génese da criação do Grupo de Projecto para o SIC-T, foi definido o seguinte objectivo: "Definir, desenvolver e implementar, de forma faseada e modular, a estrutura, a organização, bem como a tecnologia, as funcionalidades, os serviços e as interoperabilidades de um SIC-T para o Exército Português, constituindo unidades/órgãos ou módulos SIC destacáveis, típicos do escalão Brigada/Batalhão, com especial ênfase para a sua aplicabilidade em ambientes de actuação das FNDs" (DST, 2003: 5).

Este SIC-T apresenta uma capacidade real de integração operacional, para um melhor e mais eficaz desempenho nas operações militares terrestres, explorando o estado-

[4] SICCE – Sistema de informação de Comando e Controlo do Exército.
[5] MMHS – *Military Message Handling System.*
[6] SITACO – Sistema Táctico de Comunicações.

de-arte das comunicações, dos computadores, dos sensores e sistemas de armas, constituindo-se num verdadeiro embrião para a digitalização do Sistema de Forças Nacional (SFN), de forma a proporcionar vantagens técnicas que, como factor "substituto da força" no espaço da batalha, permita alcançar ao nível táctico e nas capacidades de C2, os desafios do novo milénio, através de:

(1) Eficaz adaptação e integração com o conceito NCW[7].

(2) Apoio eficaz às principais funções de planeamento e Estado Maior, reduzindo ao mínimo o tempo consumido, libertando assim o pessoal para uma concentração nas tarefas essenciais, em especial as operacionais.

(3) Imagem Operacional Comum (IOC) permanentemente actualizada (terreno, dispositivo e estado das forças amigas, opositoras e neutrais) como base essencial para a criação e avaliação da compreensão da *situational awareness* (SA).

(4) Rápida e eficiente transmissão automática dos planos e ordens a todos os intervenientes.

(5) Fornecimento aos utilizadores de diferentes serviços totalmente integrados, (voz, mensagens, dados e imagem).

b. O papel dos Sistemas de Informação e Comunicações na acção de C2

O objectivo dos SIC é auxiliar o comando na sua acção de C2 de operações militares. Uma acção de C2 eficaz é vital para a sinergia de todas as funções de combate[8]. Nenhuma actividade militar é mais importante que o C2, mas por si só, o C2 não destruirá nenhum alvo, nem afectará nenhum deslocamento de forças. No entanto, nenhuma acção efectuada com sucesso por uma força é possível sem uma acção de C2 eficaz. Um SIC superior auxilia os CMDTs a manter a unidade de esforços para aplicar as capacidades das suas forças no tempo e local crítico, e a vencer.

Normalmente considera-se o C2 como uma função de combate distinta e especializada (como o apoio de serviços, informações ou apoio de fogos) com os seus métodos, considerações e vocabulário peculiares, e que decorre independentemente das outras funções de combate. Todavia, o C2 engloba todas as funções e operações militares, sincronizando-as num conjunto coerente. O C2 é o meio através do qual um CMDT identifica o que é necessário fazer, e se certifica que são tomadas as acções apropriadas

[7] NCW – *Network Centric Warfare*
[8] Manobra; Apoio de Fogos; Informações; Mobilidade, Contramobilidade e Sobrevivência; Defesa Aérea; Apoio de Serviços; Comando e Controlo. (RC-OPERAÇÕES, 2005: 2-1 a 2-50)

(JP-6.0, 2006: vii). Para que o sistema de C2 funcione é necessário que os seus dois componentes fundamentais funcionem em harmonia (JP 6.0, 2006: I-1).

O primeiro componente, e quiçá o mais decisivo, é o **factor humano** — os militares que adquirem a informação, tomam decisões, executam operações, comunicam e colaboram uns com os outros para atingir um objectivo comum. Os seres humanos – do CMDT que define uma missão detalhando a finalidade, tarefas chave e estado final desejado, ao operador que transmite uma mensagem para os CMDTs subordinados – são componentes integrais do sistema de C2 e não apenas utilizadores do mesmo.

O segundo componente do sistema de C2 engloba as **instalações**, **equipamentos**, **comunicações** e **procedimentos** essenciais para que um CMDT possa planear, dirigir e controlar operações de forças sob o seu comando, cumprindo a missão atribuída. Embora muitas vezes vários tipos de *hardware* sejam amíude referenciadas como sistemas, o sistema de C2 consiste em muito mais do que meros equipamentos. Sistemas topo de gama e tecnologia avançada não garantem um C2 eficaz por si só; um C2 eficaz começa a ser edificado com pessoas bem treinadas e qualificadas, com uma filosofia de eficiência e procedimentos correspondentes.

Tabela 1: Critérios de Qualidade da Informação (JP 6.0, 2006: I-3)

CRITÉRIOS DE QUALIDADE DA INFORMAÇÃO	
PRECISÃO	Informação que traduz a situação real.
RELEVÂNCIA	Informação aplicável à missão, tarefa ou situação posterior.
OPORTUNIDADE	Informação disponível a tempo da tomada de decisão.
INTEGRALIDADE	Toda a informação necessária requerida pelo decisor.
BREVIDADE	Informação que possui apenas o nível de detalhe necessário
INTELIGIBILIDADE	Informação compreensível e expressa em formato e apresentação inteligível.
SEGURANÇA	Informação à qual foi concedida protecção adequada onde foi necessário.

De uma maneira ou de outra, a acção do C2 é indissociável da informação[9]. É necessário obtê-la, avaliar o seu valor, processá-la num formato útil, actuar em conformidade com o seu valor e partilhá-la com outros. Podemos considerar duas utilizações básicas para a informação no âmbito descrito. A primeira é contribuir para a criação da ***situational awareness*** (SA), constituindo esta última a base para a tomada de decisão. A segunda é dirigir e coordenar acções na execução da decisão. O SIC tem de apresentar a informação num formato que seja simultaneamente útil e capaz de ser

[9] Adveio daqui o conceito de C4I: Comando, Controlo, Comunicações, Computadores e Informação. O conceito C4 foi no entanto descontinuado pelo DoD/EUA e substituído pela designação "*communications system*". (JP-6.0, 2006: iii)

rapidamente compreendido pelo receptor. Muitas fontes de informação são imperfeitas e susceptíveis a distorção e decepção. Os critérios apresentados na Tabela 1 auxiliam na caracterização da qualidade da informação[10].

O C2 é tanto um problema de Gestão da Informação (GestInfo) como de sincronizar e executar outras funções de combate. Uma boa GestInfo contribui para que a realização de outras tarefas seja menos complexa. A automatização e padronização de processos e procedimentos dos SIC melhoram a GestInfo e contribuem para a eficácia e velocidade do C2 do CMDT. Os avanços tecnológicos na mobilidade, sistemas de armas, sensores, e sistemas de comunicações continuam a reduzir o tempo de reacção, a aumentar o ritmo das operações e a gerar grandes quantidades de informação. Se a informação não for bem gerida, as reacções dos decisores, e por consequência a própria força, poderão ser degradadas. É essencial que o SIC complemente as capacidades humanas e reduza ou elimine limitações conhecidas.

Um conjunto de procedimentos integrados e interoperáveis é importante para a participação em operações que possuirão cada vez mais um carácter conjunto e combinado. Um SIC seguro e robusto fornece ao CMDT os meios para exercer a sua autoridade e orientar forças dispersas geograficamente ou em condições ambientais variadas. Um SIC que forneça conectividade por todo o espaço de batalha é vital ao planeamento, conduta e sustentação de operações. As operações requerem muitas vezes comunicações móveis de longo alcance. Qualquer CMDT tem de comunicar de uma maneira fiável e segura com CMDTs superiores e subordinados durante todas as fases de uma operação. O SIC tem por isso de ser tacticamente ágil e projectável para qualquer parte do mundo. Têm que ser tomadas em consideração as comunicações intra-teatro e extra-teatro, as comunicações durante a fase de projecção, e ainda a interacção com organizações governamentais e não-governamentais, autoridades locais e forças aliadas.

Um C2 eficaz, obtido através da troca de informação, integra as componentes da força, permitindo-lhe funcionar eficazmente através de grandes distâncias em ambientes austeros ou complexos e em todas as condições atmosféricas. A missão e estrutura da força condicionam as necessidades do fluxo e processamento da informação. A localização e as necessidades de informação da força condicionam a configuração específica do SIC. O

[10] Não confundir com os princípios das Informações: controlo centralizado, oportunidade, exploração sistemática, objectividade, acessibilidade, capacidade de resposta, protecção da fonte e revisão contínua (RC-Informações, 2006: I.1.2-3)

objectivo é fornecer uma partilha de informação rápida que facilite uma compreensão comum da situação actual – a IOC.

Processos e procedimentos ajudam a garantir disponibilidade da informação e a aceder a todo o ambiente operacional, facilitando (JP 6.0, 2006: I-4):

(1) A **coordenação em operações conjuntas e combinadas**, através do fornecimento da visualização detalhada do campo de batalha; da gestão da informação; do planeamento colaborativo distribuído, treino, execução e avaliação.

(2) A **Agilidade Estratégica**. O SIC deve apoiar a projecção e emprego de forças em qualquer parte do mundo. A partilha de informação à escala global permite o planeamento simultâneo e interactivo a partir de localizações dispersas, permitindo a Estados-Maiores dispersos elaborar e coordenar planos e ordens. Dá igualmente à força a possibilidade de aceder a repositórios de dados, aumentando a sua capacidade de projecção, reduzindo o espaço ocupado por equipamentos outrora necessários e alargando o seu acesso a recursos ISTAR[11] globais.

(3) O **Alcance Operacional**. O SIC suporta a sincronização das funções de combate, permitindo aos CMDTs localizar e identificar forças amigas no espaço de batalha e apoiar a conduta de operações *over-the-horizon* com comunicações em movimento e comunicações BLOS[12].

(4) A **Flexibilidade Táctica**. O SIC permite ao CMDT melhorar a *shared situation awareness* (SSA)[13] e a rápida tomada de decisões; identificar e adquirir alvos, bem como desenvolver e conduzir operações em todo o espectro das operações militares. O SIC apoia o desenvolvimento e emprego da intenção e directiva de planeamento do CMDT, fomentando a execução descentralizada. A entrega à força em tempo da informação respeitante a alvos, movimentos de forças, estado dos equipamentos, níveis de abastecimentos e disposição de recursos – amigos e inimigos - permite a execução descentralizada.

(5) As **Operações em rede**. Os SIC modernos possibilitam a interligação (rede) de forças geograficamente separadas, o que permite as operações em rede.

(6) A **Superioridade de Informação (IS)**. O SIC é um facilitador para a IS. A informação e a sua gestão são aspectos nucleares de toda a actividade militar.

[11] ISTAR: *Intelligence Surveillance Targeting Acquisition and Reconnaissance.*
[12] BLOS:*Beyond Line of Sight*
[13] VICENTE traduz este termo como "Consciência Situacional Partilhada". Não se considerou ser uma tradução feliz, pelo que se manteve a designação em língua inglesa (VICENTE, 2007: 45).

Através da História, os líderes militares sempre reconheceram que uma vantagem competitiva nesta área é crítica para a o sucesso da operação (JP 6.0, 2006: I-4;I-6).

c. Network Centric Warfare e NATO Network Enabled Capability

Após a Cimeira de Praga, uma das "*Transformational Objective Areas*" (TOA) chave levantada pelos Comandos Estratégicos (SCs) da NATO foi a "*Network Enabled Capability*" (NEC). Esta capacidade, tal como foi definida pelos SCs, envolve a junção de sensores, decisores e sistemas de armas, bem como de agências ou organizações multinacionais militares, governamentais e não-governamentais, num ambiente de planeamento, avaliação e execução colaborativo e fluido. Por outro lado, deverá providenciar a troca de informação segura em tempo útil, utilizando redes de comunicações interligadas, interoperáveis e robustas, as quais suportarão a recolha, fusão, análise e partilha da informação em tempo útil (NC3A, 2005: 1).

Esta nova capacidade no seio da NATO, a "*Nato Network Enabled Capability*" (NNEC), providencia o ambiente certo para o desenvolvimento de uma aproximação comum à conduta de futuras operações da Aliança, desenvolvendo as arquitecturas, standards, processos e procedimentos necessários para permitir a flexibilidade e agilidade necessários para a condução de futuras operações centradas em rede num contexto conjunto. No entanto, num curto espaço de tempo, o conceito de NNEC sofreu várias actualizações. Actualmente é proposta a seguinte definição: "a capacidade da Aliança federar os vários componentes do ambiente operacional, desde o nível estratégico (incluindo os quartéis-generais NATO) até aos níveis tácticos, através de uma infra-estrutura de informação em rede (VICENTE, 2007: 91). Esta conjuntura tem profundas implicações no desenho dos sistemas SIC (NC3A, 2005: 2).

Em primeiro lugar, torna-se fundamental estender as capacidades de comunicações em rede "aonde quer que estas sejam necessárias, sempre que forem necessárias", o que implica a necessidade de uma "capacidade de rede flexível e global". Em segundo lugar, surge a necessidade de prestar apoio a estruturas de forças de menor dimensão, modulares e de carácter multinacional, como as NATO *Response Forces* (NRF), o que gera novos requisitos de interoperabilidade, partilha de informação e segurança. Em terceiro lugar, existe a necessidade de apoiar a rotação dos elementos das forças nacionais dentro das NRF e de apoiar a interoperabilidade com elementos de forças de nações não pertencentes à NATO. Estes pontos identificam a necessidade de um grau sem precedentes de flexibilidade, agilidade, adaptabilidade e interoperabilidade na estruturação das forças

envolvidas e das redes de comunicações e sistemas de informações que as apoiam (NC3A, 2005: 3).

O desenvolvimento do conceito de NNEC começou com os princípios da *Network-Centric Warfare* (NCW) e a sua incorporação nos conceitos de operação da NATO. A definição de NCW normalmente aceite nos EUA[14]é a "ligação de pessoas, sistemas e plataformas numa força em rede e auto-sincronizada, com vista a criar a consciência partilhada do espaço de batalha ("*shared battlespace awareness*") que garanta a superioridade da informação e aumente a velocidade da acção de comando" (BRAUNLINGER, 2005: 65). Os princípios da NCW são quatro, e podem ser relacionados com três componentes: Redes, Informação e Pessoas (ALBERTS, 2000: 88-91):

(1) Uma força ligada em rede de forma robusta melhora a partilha de informação.
(2) A partilha de informação aumenta a qualidade da informação e da SSA.
(3) A SSA permite a colaboração e auto-sincronização, e aumenta a capacidade de sustentação e a velocidade da acção de comando.
(4) Estas, por sua vez, aumentam drasticamente a eficácia da missão.

O que começou por ser uma adaptação do modelo americano de NCW, rapidamente evoluiu de uma perspectiva centrada em rede para uma aproximação "possível" em rede. Saliente-se que o conceito geralmente empregue, centrado/cêntrico ("*centric"*) em rede, indica que a rede/redes são fundamentos centrais para um dado conceito ou capacidade. O termo "*enabled*" empregue pela NATO, reflecte que uma capacidade é tornada possível ou efectiva, em rede. Embora a distinção seja ténue, reflecte a rejeição da rede como aspecto central deste processo (VICENTE, 2007:. 91).

A estratégia para o desenvolvimento das componentes de rede e partilha de informação da NNEC tem o seu enfoque na junção de sistemas de redes e de sistemas de informação da NATO e dos seus países membros, com vista a formar uma capacidade de Federação de Sistemas (FoS) que implemente a *Networking and Information Infrastrucure* (NII)[15]. O conceito de FoS refere-se a um conjunto de diferentes sistemas, os quais não são geridos centralmente, mas estão ligados de modo a alcançar capacidades que estão para além das atingíveis pelos sistemas individuais separadamente (NC3A, 2005: 5).

[14] A definição de NCW não é uniforme nos vários Ramos das Forças Armadas dos EUA.
[15] Ao nível do Exército, teríamos pois de considerar todas as redes que servem a instituição, desde o SIC-T ao SIC-E (Sistema de Informação e Comunicações Estratégico).

A componente de comunicações do NII[16] é caracterizada pelo uso do protocolo IP (Internet Protocol), o que permite o uso de um mecanismo de transporte seguro e comum para todo o tipo de informação, sobre qualquer tipo de meio de transmissão. O processo de adopção do protocolo IP demorará o seu tempo. A sua adopção começará em infra-estruturas de rede estáticas[17], sendo depois acelerada a sua adopção consumada em redes destacáveis. Uma peça chave neste processo será a padronização de interfaces entre terminais de Comunicações Satélite (SATCOM) destacáveis e as redes estratégicas e a optimização destas redes destacáveis para suportarem tráfego IP (NC3A, 2005: 6).

A utilização de equipamentos de encriptação IP flexíveis, bem como de sistemas de gestão de chaves electrónicas é uma necessidade para todos os serviços NII. O rápido emprego operacional de equipamentos de encriptação IP interoperáveis é fundamental para o desenvolvimento da *core network black*[18], uma rede de redes única, virtual, operando no grau de segurança NÃO CLASSIFICADO, e que possa suportar tráfego de voz, vídeo e dados para múltiplos domínios de segurança e graus de classificação (NC3A, 2005: 7).

d. A Guerra da Informação

O constante evoluir das Tecnologias de Informação e Comunicações levou ao emergir de uma "sociedade em rede", onde nenhum actor se encontra isolado, sendo pelo contrário parte integrante de uma «rede de redes», na qual os sistemas permitem acesso permanente aos recursos de informação necessários aos ciclos de tomada de decisão (EME, 2007: 4). É a esta rede global que se encontram ligados os diferentes sistemas de gestão das infra-estruturas críticas do Estado (como por exemplo: os sistemas de gestão da Rede Eléctrica; das Redes de Transportes; das Redes de Serviços Públicos de Telecomunicações; e dos Mercados Financeiros) todos eles interdependentes e necessitando tanto do acesso em tempo oportuno a informação fiável, como de disseminar as decisões tomadas.

É fácil entender que a quebra dos fluxos de informação, a deterioração da sua fiabilidade ou dos sistemas de processamento necessários ao funcionamento destas infra-estruturas poderá ter consequências catastróficas para a política e economia do Estado. A consciência desta realidade leva a que Estados e outros actores, na competição entre eles

[16] O NII tem por base o modelo OSI (*Open Systems Interconnection*) da ISO (*International Organization for Standardization*). Ver figura 2.
[17] No caso Português a situação foi idêntica: foram estabelecidas em primeiro lugar as redes estratégicas, sendo posteriormente feita a ligação ao SIC-T.
[18] Uma rede *black* é por definição uma rede não segura. Uma rede segura é normalmente designada de rede *red*. No entanto, uma rede *black* pode ser utilizada para interligar várias redes *red* através do uso de *border protection devices* (BPD).

por um determinado objectivo, desenvolvam actividades com vista a proteger as suas necessidades de informação e negarem-nas ao opositor.

Assim, a existência de um Ambiente de Informação[19] (constituído pelas dimensões física[20], de informação[21] e cognitiva[22]), global, dinâmico e de fácil acesso, que proporciona o atingir de vantagem na capacidade de decisão a quem sobre ele souber actuar, nomeadamente, através da recolha, processamento e disseminação da informação relevante, enquanto se explora ou nega essa capacidade ao adversário.

É no actuar sobre o Ambiente de Informação que residem as acções de "Guerra de Informação", não existindo contudo uma "Guerra de Informação" individualizada mas sim um conjunto distinto de múltiplas acções de "Guerra de Informação", encaradas de maneira diferente por diferentes entidades[23].

Quando se actua sobre o Ambiente de Informação na procura da necessária superioridade de informação do Sistema Político Internacional (SPI), necessariamente resultam relações de conflitualidade entre os Estados e/ou outros actores. Neste contexto, encontramo-nos no patamar estratégico, onde todas as Estratégias Gerais devem estar coordenadas para que se atinja o domínio sobre o Ambiente de Informação. Verificamos assim que a Guerra de Informação constitui um conceito transversal a todas as áreas da vida de uma sociedade com maior, ou menor, desenvolvimento tecnológico. Este facto faz com que o conceito de Guerra da Informação seja considerado um conceito global, ao nível das Estratégias Gerais[24], influenciando necessariamente as doutrinas e formas de empregos da componente militar.

As acções de "Guerra de Informação" apresentam como alvo preferencial os aspectos cognitivos do processo de decisão. Alguns dos métodos e mecanismos utilizados

[19] Conjunto de indivíduos, organizações e sistemas que procedem à recolha, processamento, disseminação e actuação sobre a informação (JP 3-13, 2006: I-1).
[20] Sistemas de Comando e Controlo, infra-estruturas físicas e de comunicações onde circula a informação.
[21] Dimensão onde a informação é recolhida, processada, armazenada, disseminada, apresentada e protegida. Consiste no conteúdo e fluxo de informação.
[22] Dimensão associada à forma como a informação é interpretada e apreendida, influenciando as escolhas na tomada de decisão. Encontra-se dependente de factores intrínsecos à natureza humana (experiências vividas, convicções, formação moral e científica) e extrínseca (opinião pública, comunicação social, motivações).
23 Enquanto para uma determinada entidade, "Guerra de Informação" pode ser considerada como um conjunto de hackers procurando vulnerabilidades em redes de computadores e explorando-as através da utilização de malware (*Malicious Software*, compreende vírus informáticos, "bombas lógicas", Trojan), para outra entidade, "Guerra de Informação" poderá ser considerada como a capacidade de induzir comportamentos a um determinado grupo fazendo uso da manipulação psicológica através dos meios de comunicação social.
[24] Entram aqui em jogo os elementos do poder nacional, o conhecido DIME (Diplomático, Informacional, Militar e Económico).

têm como objectivo dificultar o acesso e a correcta utilização dos sistemas de informação e a manipulação dos dados que materializam a informação, alterando o seu contexto e significado. Apesar de na "Guerra de Informação" a maior parte das acções serem do tipo não violento (não implicando necessariamente a utilização de armas de destruição física), poderemos identificar, tal como na guerra convencional, acções de natureza ofensiva e defensiva, que diferem não pelas medidas utilizadas mas nos objectivos pretendidos.

Nas acções de **natureza ofensiva**, poderemos considerar a utilização: de armas de destruição física sobre nós/infra-estruturas de comunicações/sistemas de informação; de armas de sintaxe (por exemplo, vírus informáticos e *malware*), tendo como objectivo atacar a lógica operacional de um sistema de informação através da introdução de atrasos ou comportamentos imprevisíveis no seu funcionamento ou ainda adquirindo o controlo, ou desactivando, a lógica das redes e dos sistemas de informação visados; de armas de semântica, tendo como objectivo a destruição ou afectação da confiança que os utilizadores depositam tanto nos recursos de informação como nos vectores que os transportam (manipulação, modificação ou destruição dos modelos de apoio à decisão, afectando a percepção e a representação da realidade). Nas acções de **natureza defensiva**, após identificadas as vulnerabilidades dos nossos sistemas face a acções adversas, poderemos considerar a implementação de uma política de Segurança da Informação (INFOSEC)[25], incluindo as medidas necessárias para contrariar, detectar, documentar e responder a intrusões não autorizadas (COMPUSEC[26], COMSEC[27] e CERT[28]).

Neste contexto, "Guerra de Informação" aparece definida como o conjunto de acções desenvolvidas para obter a Superioridade de Informação[29,] afectando a informação, processos baseados em informação, sistemas de informação e redes baseadas em computadores, enquanto se defende a nossa informação, processos baseados em informação, sistemas de informação e redes baseadas em computadores (FM 100-6,1996: 2-2). É a capacidade de atingir e manter a Superioridade de Informação que permite moldar o Ambiente de Informação, potenciando a realização de outras acções com vista a alcançar os efeitos pretendidos sobre um determinado adversário.

[25] Entendida como a implementação de medidas com vista à protecção e defesa da informação e dos sistemas de informação contra o acesso não autorizado ou modificação da informação, quer esta esteja armazenada, em processamento ou em trânsito.
[26] Segurança dos Computadores.
[27] Segurança das Comunicações
[28] CERT: *Computer Emergency Response Team*
[29] Vantagem operacional derivada da capacidade de recolher, processar e disseminar um fluxo ininterrupto de informação enquanto se explora ou nega ao adversário essa mesma capacidade (JP 3-13, 2006:I-5).

Segundo a Doutrina NATO, o conceito de Information Operations (INFO OPS) interliga a Guerra de Comando e Controlo (Command and Control Warfare – C2W)[30] com actividades de cariz político, diplomático, CIMIC[31], Informação Pública, ou qualquer outra actividade conduzida pela Aliança, que possa afectar a percepção de determinado adversário ou parte envolvida (NATO, 2007a:4-3).

O alvo das acções de INFO OPS é assim extremamente amplo e a sua efectiva aplicação, durante tempo de paz, poderá evitar a necessidade de uma acção militar. Neste sentido, o planeamento de INFO OPS é considerado, devido às áreas de actividade que engloba (política, diplomática, civil e militar), ao nível estratégico e operacional, podendo as acções planeadas serem realizadas nos três níveis de condução das operações (estratégico, operacional e táctico). Contudo, a aplicação militar das INFO OPS encontra-se materializada pela C2W. A figura 3 ilustra a abrangência das INFO OPS.

A NATO definiu então Operações de Informação (INFO OPS) como o conjunto de acções tomadas com vista a influenciar os decisores relativamente ao apoio dos objectivos políticos e militares traçados, afectando a sua informação, processos baseados em informação, Sistemas de C2 e SICs, ao mesmo tempo que protegem a informação e sistemas de informação da Aliança (NATO, 2007a:4-3).

Consoante a natureza das acções desenvolvidas existem dois tipos de INFO OPS:

(1) **INFO OPS Defensivas**: acções desenvolvidas para manter o acesso e a utilização efectiva da informação, processos baseados em informação, sistemas de C2 e SIC durante situações de paz, crise ou conflito, bem como proteger a informação crítica da Aliança para a obtenção de determinados objectivos. A condução de INFO OPS defensivas no seio da NATO encontra-se enformada pelas políticas de segurança, doutrina e procedimentos, assegurando que a informação, processos baseados em informação e SIC da Aliança se encontram adequadamente protegidos contra as acções hostis com vista a adquirir, "explorar" ou manipular a informação necessária aos processos de tomada de decisão, ou consultadoria, política e objectivos operacionais da Aliança. (DST, 2007:8-9)

[30] Definida como a utilização integrada de todas as capacidades militares, incluindo a Segurança das Operações (OPSEC), Decepção, Operações Psicológicas (PSYOPS), Guerra Electrónica e Destruição física, apoiadas por todas as fontes de informações e Sistemas de Informação e Comunicações (SIC), com vista a negar informação a, influenciar, degradar ou destruir a capacidade de C2 de um adversário enquanto protege a capacidade de C2 das forças amigas contra acções similares (NATO, 2007a: 4-3).
[31] CIMIC: *Civilian-military cooperation* (cooperação civil-militar)

(2) **INFO OPS Ofensivas**: acções desenvolvidas para influenciar a disponibilidade de informação, processos baseados em informação, sistemas de C2 e SIC dum potencial adversário, em situação de paz, crise ou conflito, com vista à concretização de um determinado objectivo ou em resposta a uma ameaça específica. A condução das INFO OPS ofensivas será enformada pelas directivas politicas emanadas pelo Conselho do Atlântico Norte (NAC), seguidas do aconselhamento (de acordo com a situação) das Autoridades Militares da NATO.

Todo o processo de decisão, e a implementação das decisões tomadas, encontra-se intimamente ligado à percepção que o decisor tem da realidade envolvente, ou seja, o decisor deverá ter vontade de actuar, deverá conhecer a situação para actuar e deverá ter os meios (capacidades) para actuar. Se qualquer um destes factores for manipulado por entidades externas, a forma de actuação, ou não actuação, será condicionada.

Tendo presentes estes factores, as actividades coordenadas pelas INFO OPS serão focalizadas essencialmente: em influenciar a vontade, actuando directamente sobre os decisores capazes de influir na situação; agindo sobre o conhecimento e entendimento da situação, afectando e manipulando a informação disponível aos decisores; e afectando (dentro da Regras de Empenhamento e constrangimentos legais) as capacidades, que permitem ao decisor ter o entendimento da situação bem como aquelas que lhe permitem implementar a sua vontade (por exemplo, a infra-estrutura C4ISR[32]).

São desta forma desenvolvidas as seguintes áreas de actividade:

(1) **Actividades de Influência**, compreendendo qualquer actividade cujo objectivo primário é influenciar a vontade (persuadindo, convencendo, compelindo ou coagindo a adopção, ou o apoio à adopção, de uma dada modalidade de acção);

(2) **Actividades de Anti-Comando**, compreendendo a realização de acções sobre as capacidades (com vista a interromper, desorganizar, degradar, negar, enganar ou destruir a informação, comando, propaganda e sistemas associados, processos e redes adversárias), sendo utilizadas para afectar o fluxo de informação necessária a um determinado decisor, influenciando desta forma o seu entendimento da situação, a sua vontade ou a disseminação da sua decisão;

(3) **Actividades de Protecção da Informação**, compreendendo qualquer actividade que evite a um adversário obter informação sobre as operações da Aliança. Inclui,

[32] *Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance.*

sem estar limitado, a Segurança das Operações (OPSEC)[33], a Segurança da Informação (INFOSEC) e anti-ISTAR (NATO, 2007: xxiii).

Para a implementação destas actividades, a INFO OPS faz uso das Capacidades, Ferramentas e Técnicas e Actividades Nucleares Relacionadas apresentadas na tabela 2.

Tabela 2 - Elementos/Capacidades das Operações de Informação – NATO (DST, 2007:14)

		Capacidades, Ferramentas e Técnicas utilizadas em apoio das INFO OPS	Actividades Relacionadas
Capacidades Militares	C2W	*Guerra Electrónica (EW)* *Operações Psicológicas (PSYOPS)* *Segurança das Operações (OPSEC)* *Destruição Física* *Decepção*	
	Outras	*Operações em Redes de Computadores (CNO)* *Ataque a Redes de Computadores (CNA)* *Defesa de Redes de Computadores (CND)* *Exploração de Redes de Computadores (CNE)* *Segurança da Informação (INFOSEC)* *Presença, Postura e Perfil (PPP)*	
Capacidades não – Militares			*Informação Pública (PI)* *Cooperação Civil-Militar (CIMIC)*

e. Funções e Princípios dos SIC

Os SIC do Exército Português (e os dos outros ramos das FA) devem possuir a capacidade de se adaptarem rapidamente a ambientes dinâmicos. Para tal, devem estar aptos a fornecer ao comando a informação que é necessária (a informação certa), no sítio onde ela é necessária (no local certo) e quando ela é necessária (no tempo certo). Concorrentemente, esta informação deve ser protegida da intercepção e sua utilização por adversários, e deve ser disponibilizada ao utilizador num formato útil. Com o seu enfoque nestes objectivos fundamentais, os SIC permitem à força aproveitar oportunidades e ir de encontro aos objectivos da missão. Os SIC facilitam a partilha de informação e a tomada de decisão, constituindo-se como uma das pedras basilares do actual ambiente operacional.

Os modernos SIC, como o SIC-T, abrangem um alargado leque de funções relacionadas com o tratamento da informação. Estas funções, das quais várias têm sido

[33] Processo que, utilizando medidas activas e passivas, garante a uma operação ou exercício militar a segurança apropriada para negar ao inimigo informação acerca da disposição, capacidades e intenções das forças amigas (AAP 6, 2007, 2-O-4).

tradicionalmente desempenhadas pela Arma de Transmissões no Exército, sofrem uma nova requalificação no actual ambiente operacional de «rede», podendo ser reclassificadas em **aquisição**, **processamento**, **armazenamento**, **transporte**, **controlo**, **protecção**, **disseminação** e **apresentação**.

Por **aquisição** entende-se a introdução da informação no SIC. Fontes de informação incluem entradas de sensores autónomos ou guarnecidos, radares, capturas de vídeo, entradas manuais ou qualquer outra fonte que insira informação no SIC. O **processamento** é uma sequência determinada de operações efectuada sobre informação bem definida e que tem como objectivo produzir um produto final específico. Esta função é tipicamente usada para conformar dados, informação e/ou conhecimentos a um formato desejável, que possa apoiar a tomada de decisões. A **armazenamento** consiste na retenção, organização e disposição de dados, informação e conhecimentos, com vista a facilitar a partilha e a recuperação de informação. O SIC necessita de uma capacidade de **transporte** para suportar a troca e disseminação de informação *end-to-end* num ambiente global. O propósito da função **controlo** é dirigir, monitorizar e regular as outras funções do SIC tendo em mente o cumprimento das exigências da força dentro dos parâmetros de desempenho especificados. A **protecção** consiste na garantia da confidencialidade, integridade, disponibilidade e autenticidade da informação, o seu processamento seguro[34] e sua transmissão. O acesso deverá ser restringido ao pessoal autorizado. A **disseminação** é a distribuição da informação processada aos destinatários apropriados. No final, o SIC tem que interagir com os utilizadores. Referimo-nos a esta interacção como a função **apresentação**. Telefones, computadores, ecrãs de radar (entre outros) são os meios através dos quais os vários componentes da força partilham informação uns com os outros. Como tal, o SIC deve apresentar a informação ao destinatário da maneira que melhor facilite a compreensão e utilização da mesma (JP 6.0,2006: I-6,8).

A doutrina do Exército Português reconhece cinco princípios orientadores para a actividade das Transmissões: **Flexibilidade**, **Coordenação**, **Ligação**, **Objectivo** e **Economia de Meios** (EPT, 2003: 5). A actividade das Transmissões[35] circunscreveu-se durante muito tempo apenas aos aspectos tradicionalmente relacionados com as **comunicações** e o **transporte** da informação. Porém actualmente, o sistema de informação

[34] Incluindo a autenticidade e o não repúdio
[35] Embora sejam parte integral das missões da Arma de Transmissões no Exército Português, não iremos considerar neste trabalho as actividades de Guerra Electrónica.

pode ser dividido em dois subsistemas: o subsistema computacional responsável pelo armazenamento e processamento da informação (SI) e o subsistema de comunicações responsável pela sua transmissão (a *core network*), como é ilustrado na figura 4.

De uma força que esteja interligada e sincronizada no tempo e no objectivo podemos dizer que está a funcionar "em rede". Uma força "em rede" aumenta a sua eficácia operacional, pois permite a componentes dispersos comunicar e manobrar mais eficazmente, partilhando uma IOC e atingindo mais rapidamente o estado final desejado (JP 6.0, 2006, I-1). A componente de rede é pois um componente estrutural do SIC-T, e também um factor merecedor de uma reflexão sobre os princípios dos SIC no Exército Português (e por extensão aos outros Ramos das FA), particularmente tendo em vista o seu emprego em operações conjuntas e combinadas.

Recentemente, no Exército Português o conceito Transmissões passou a sinónimo de SIC (EME, 2005a: 72), o que torna necessária a uma reformulação dos princípios acima referidos, bem como à eventual adição de outros princípios. Consideramos assim mais adequados à realidade actual os princípios enunciados na JP 6.0 do DoD dos EUA: **interoperabilidade**, **agilidade**, **confiança** e **partilha**.(JP-6.0, 2006: I-8,11)

(1) Interoperabilidade

A **Interoperabilidade** é essencial para que qualquer força alcance a Superioridade de Informação no actual ambiente de rede. O SIC deve possuir o grau de interoperabilidade necessário que garanta o sucesso em operações conjuntas e combinadas, bem como a interacção com órgãos nacionais, Organizações Internacionais (OIs) e Organizações não Governamentais (ONGs). A interoperabilidade é atingida através do uso de **equipamentos e sistemas comuns**, **compatibilidade**, **padronização** e **ligação**.

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.

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 electromagnética 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.

Padronização. Os interfaces e protocolos dos SIC devem seguir standards padrão (nacionais e/ou NATO). Devem ser reduzidas ao mínimo as soluções de recurso para compensar faltas de conformidade com interfaces/protocolos padrão[36]. Esta característica facilita também o 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.

Ligação. A finalidade da ligação é assegurar a cooperação para uma acção conjunta e combinada bem sucedida. Os destacamentos de ligação devem ter os conhecimentos linguísticos e meios de ligação com os respectivos comandos. A presença de elementos de ligação contribui para a interoperabilidade entre forças conjuntas e combinadas, bem como para as interacções com OGs e ONGs. Em operações convencionais os comandantes devem assegurar-se através de directivas orientadoras claras que podem exercer o comando e o controlo em quaisquer circunstâncias. A menos que se defina de outra forma, a responsabilidade para o estabelecimento das comunicações é a indicada no Apêndice 7.

(2) Agilidade

Para apoiar forças e conceitos operacionais ágeis, um SIC deve igualmente ser ágil. Os requisitos básicos que contribuem para a agilidade de um SIC são a **capacidade de resposta** (reagir a alterações no ambiente operacional em tempo oportuno), a **flexibilidade** (utilização de múltiplos meios/caminhos para obter sucesso e capacidade de movimentação fluida da informação através de qualquer um deles), a **inovação** (capacidade de fazer coisas novas e capacidade de fazer coisas velhas de novas maneiras) e a **adaptabilidade** (capacidade de alterar processos de trabalho e capacidade de alterar a organização).

(3) Confiança

A rede deve ser transparente para os seus utilizadores. A força tem que confiar nas capacidades da rede e na validade da informação disponibilizada pela rede. Para tal o SIC deverá possuir as capacidades de **sobrevivência, protecção e sustentabilidade**.

(a) Sobrevivência

A segurança da informação e do SIC envolve igualmente aspectos técnicos e de procedimentos, os quais são parte integral da defesa do sistema. Incluem a **Segurança física** dos componentes e instalações do SIC; **a Segurança do pessoal,** ou seja dos elementos que possuem autorização para aceder aos SIC; por medidas de **Segurança das Operações (OPSEC)** aplicadas aos SIC**,** procedimentos e técnicas que protegem o

[36] `Foi uma das preocupações do TACOMS Post 2000, uma iniciativa de 13 nações da NATO para definir os novos regulamentos para as redes de telecomunicações tácticas emergentes e futuras.

emprego operacional dos componentes dos SIC; **negar** ao adversário informação acerca de configurações específicas de SIC, emprego operacional dos SIC e grau de importância dos componentes dos SIC para o cumprimento da missão; as técnicas e capacidades de **baixa probabilidade de intercepção** (LPI) e **baixa probabilidade de detecção** (LPD) desenhadas para derrotar tentativas adversárias de detecção e exploração de meios de transmissão dos SIC; os procedimentos de **controlo de emissões** designados para apoiar a OPSEC e LPI/LPD; o **desenho dos SIC e controlo de configurações**, nomeadamente sistemas de distribuição protegidos, mitigação de vulnerabilidades das Tecnologias de Informação e redundância de componentes críticos dos sistemas; a realização de **análises** de vulnerabilidades tecnológicas e processuais e de programas de avaliação; a **robustez**, no fundo a capacidade de manter a eficácia ao longo de uma série de tarefas, situações e condições; a **resiliência** ou capacidade de recuperar rapidamente ou reajustar-se face a situações adversas, danos ou acontecimentos desestabilizantes no ambiente operacional.

(b) Protecção

O CMDT da força conduz acções de protecção da força para proteger os elementos sob o seu comando ou controlo, incluindo recursos de SIC. Uma vez que o SIC e as forças a ele associadas são facilitadores cruciais para o exercer do C2, constituem um HVT para o adversário e devem ser protegidos para manter a integridade do sistema de C2. É dentro deste contexto que é aplicável o conceito de Information Assurance (IA)[37]com vista à protecção e defesa da disponibilidade de rede e de informação e da integridade dos dados.

Não existe uma grande diferenciação entre este termo e o conceito de segurança apresentado no RAD 280-1 (EME, 2003: 2): "A segurança é uma área dinâmica que deve ser considerada durante todo o ciclo de vida de um SIC. Os seus requisitos e efeitos devem ser objecto de revisão constante, em cada patamar do seu ciclo de vida, desde a sua concepção até ao seu abate". Os objectivos principais da protecção/segurança a aplicar aos SIC são os mesmos:

A **confidencialidade**: necessidade de protecção dos dados e informação classificada, de forma a poderem ser revelados apenas a quem está credenciado e tenha necessidade de conhecer;

[37] Implementação de medidas com vista à protecção e defesa da informação e sistemas de informação garantindo a sua disponibilidade, integridade, autenticidade, confidencialidade e não repúdio. Inclui o restaurar dos sistemas de informação incorporando a capacidade de protecção, detecção e reacção (JP 3-13, 2006: II-5).
A tradução para Português tal como foi feita na Informação Nº 457/ 2007- DivCSInfo do EME, *segurança da rede*, não parece adequada. Como tal decidiu-se manter a expressão em inglês.

A **integridade**: comprovar que a informação não tenha sido alterada ou se modificada apenas por quem está autorizado;

A **disponibilidade**: assegurar que todos os recursos estejam disponíveis semprre que uma entidade autorizada o solicite.

A **autenticidade**: garantir que a informação provém das fontes anunciadas.

O **não-repúdio**: garantir que uma acção não possa ser negada por quem a fez.

Consideramos duas áreas de aplicação do conceito de protecção referido aos SIC: Computer Network Defense (CND), incluindo a COMPUSEC, e COMSEC.

1. Computer Network Defense

A CND é o conjunto de acções tomadas para proteger, monitorizar, analisar, detectar e responder a actividades não autorizadas dentro de sistemas de informação e redes de computadores das nossas forças. Deve ser encarada como uma missão global, com enfoque na protecção e defesa de sistemas interligados e redes nacionais. Para proteger o SIC, será empregue uma estratégia de defesa em profundidade que englobará a **gestão dos riscos de segurança**, a **minimização**, o **menor privilégio**, a **auto-protecção**, a **justaposição da protecção** e a **implementação de verificações de segurança**[38].

2. Segurança das Comunicações (COMSEC)

Aplicação de medidas de segurança às comunicações, de forma a negar a pessoal não autorizado, informação valiosa que possa derivar da posse ou estudo dessas comunicações ou a assegurar a autenticidade das comunicações. Essas medidas incluem a segurança cripto (da transmissão e da emissão) e a segurança dos procedimentos, física, do pessoal e dos documentos (EME, 2003, A-3).

(c) Sustentabilidade

O SIC deverá apoiar de uma forma contínua operações de qualquer tipo e duração. Este requisito implica um desenho e emprego económicos do SIC, sem no entanto sacrificar as suas capacidades operacionais e de sobrevivência. Alguns exemplos serão a

[38] **Gestão dos Riscos de Segurança**: para os SIC do Exército serão aplicados processos de análise e gestão dos riscos de segurança, no sentido de monitorizar, reduzir, eliminar, evitar ou aceitar esses riscos; **Minimização**: apenas as funções, protocolos e serviços necessários ao desempenho operacional da missão serão instalados e usados; **Menor privilégio**: os utilizadores apenas terão os privilégios e as autorizações necessárias para o desempenho das suas funções; **Auto-protecção**: cada SIC tratará os outros sistemas com desconfiança, implementando medidas de segurança para controlar a troca de informação; **Justaposição da protecção**: as medidas de segurança serão implementadas a vários níveis. Uma única medida não constitui, geralmente, protecção suficiente, pelo que as medidas a aplicar têm de ser combinadas, de forma a obter-se uma sobreposição adequada. Alguma redundância na protecção será sempre um benefício, pois para ultrapassar uma dada medida, será necessário comprometer pelo menos dois mecanismos de segurança; **Implementação de verificações de segurança**: a aplicação destes princípios e a subsequente aplicação das medidas de protecção serão inicial e periodicamente verificadas.

colocação de módulos SIC fisicamente próximos sob o mesmo Comando., o meticuloso planeamento, desenho e aquisição de instalações e sistemas, a gestão e procedimentos eficientes e disciplina na utilização dos SIC, a utilização máxima dos subsistemas SIC militares (RDE, NSWAN, etc.), a utilização judiciosa de serviços de comunicações comerciais e a aderência a arquitecturas aprovadas.

(4) Partilha

Este princípio permite a utilização mútua de serviços ou capacidades de informação entre entidades presentes no ambiente operacional. De referir que neste princípio se prevê o cruzamento de dados entre diferentes comandos, componentes e outras organizações, ou seja, de uma forma conjunta e combinada.

3. Emprego Táctico das Transmissões

O SIC-T não aparece por acaso. Na sequência de estudos desenvolvidos por um grupo de trabalho do Exército, foram aprovados os requisitos operacionais do SITACO em Fev1997, por despacho do General CEME, cuja arquitectura respeitava o TACOMS 2000 da NATO (CARREIRA, 2002). No entanto, não deixa de ser curioso que a própria arquitectura TACOMS 2000 foi largamente inspirada na arquitectura MSE do Exército dos EUA (ver Anexo 1).

No entanto, o processo de transformação por que passam as Forças Armadas a nível mundial enfatiza cada vez mais os conceitos de modularidade e de operações conjuntas e combinadas. Consideramos pois que estas características, aliás bem patentes no novo conceito de LandWarNet/WIN-T[39] do Exército dos EUA, estão presentes no SIC-T e alteram substancialmente o emprego táctico das Tm no Exército Português.

a. O sistema *Mobile Subscriber Equipment* do Exército dos EUA

A arquitectura das comunicações tácticas do Exército dos EUA a partir da década de 90 é normalmente dividida em três componentes de rede: o *Area Common-User System* (ACUS), a *Combat Net Radio* (CNR) e o *Army Data Distribution System* (ADDS) (FM-11.43, 1999: I-3).

A componente ACUS para escalões abaixo de Corpo de Exército (CE) e inferiores foi consubstanciada no sistema MSE. A concepção deste sistema decorreu da necessidade prevista na doutrina de 1982 – *Airland Operations*, de comunicações mais robustas e transportáveis, em que era dada especial ênfase à manobra e à ofensiva em vez da defensiva e da atrição. Permite a ligação automática para utilizadores fixos e móveis, desde a retaguarda do CE até às unidades de escalão batalhão, e inclui ainda os serviços de telefone seguro, fax seguro, radiotelefone seguro, transmissão segura de dados e acesso à CNR (VIEIRA, 2007: 16). Começou a ser implementado no Exército dos EUA em Outubro de 1988, tendo tido o seu "baptismo de fogo" em 1990 nas operações "*Desert Shield*" e "*Desert Storm*". Está actualmente a ser substituído pelo sistema WIN-T (GLOBALSECURITY, 2008b). O papel do MSE é fornecer um sistema de comunicações de utilizador comum em apoio das operações dos escalões Corpo de Exército até Batalhão.

[39] *Warfighter Information Network-Tactical* (WIN-T) – novo (*Army XXI*) sistema de comunicações táctico do Exército dos EUA, o qual engloba a infra-estrutura de comunicações e componentes de rede desde as UEB de manobra até à área da retaguarda do teatro de operações (GLOBALSECURITY, 2008).

O sistema MSE é um sistema de comunicações comutado composto por nós de comutação interligados entre si. Os nós formam uma malha que providencia à força um sistema de área de utilizador comum (ACUS), o qual é ocupado por assinantes de unidade. Uma grelha divisionária típica é constituída por seis ou quatro[40] centros nodais que constituem a espinha dorsal (*backbone*) da rede. Em toda a área de operações, os assinantes fixos ligam-se a nós de comutação locais[41] por meios filares ou não filares. Estes comutadores, ou *nós de extensão* providenciam o acesso à rede ligando-se aos centros nodais através de feixes hertzianos ou cabo. Os centros nodais ligam-se entre si de forma redundante através de terminais de feixes hertzianos. São garantidas comunicações numa área que pode atingir os 39000 km^2, podendo apoiar um CE composto por um máximo de cinco Divisões. O sistema é digital, seguro, altamente flexível e apresentava características que á altura da sua concepção lhe permitiam lidar com quebras de ligação, excesso de tráfego e rápida movimentação dos utilizadores.

Os principais componentes do sistema incluem: Centros Nodais, a GEA, PEAs, Pontos de Acesso Rádio (PAR), dois centros de controlo do sistema redundantes, terminais de feixes hertzianos, terminais SATCOM e de comunicações troposféricas (TROPO), interfaces para redes externas, terminais de assinante e terminais de assinante radiotelefónicos móveis (ver figura 5).

As comunicações de voz e dados são fornecidas de forma automática utilizando uma técnica designada de "*flood search routing*". O sistema suporta assinantes móveis e filares, permitindo aos mesmos a troca de mensagens, dados e informações num ambiente táctico dinâmico. A componente Tactical Packet Network (TPN) do MSE consiste numa rede de comutação de pacotes justaposta sobre uma rede base de comutação de circuitos. Para além de garantir a comunicação de dados, a TPN garante a interligação desses dados a sistemas adjacentes, incluindo redes civis.

O conjunto representado pelo sistema MSE apresenta três características principais: tecnologia digital, segurança e flexibilidade. Possui características de compensação para perdas de ligações ou avarias de elementos funcionais, sobrecarga de tráfego, e movimentação rápida dos utilizadores. O MSE apoia assim assinantes móveis e fixos tendo em vista a troca de informação C4I (FM-11.55, 1999: 1-1). Um dos objectivos do sistema

[40] Consoante se trate de divisões pesadas ou ligeiras. Adicionalmente, na área de Operações do CE existem mais 22 Centros Nodais.
[41] As Grandes Extensões de Acesso (GEA) e as Pequenas Extensões de Acesso (PEA).

MSE foi providenciar às forças tácticas[42] uma mobilidade superior e a capacidade de RADA[43]. As funções de comutação, agregação rádio, COMSEC e gestão do sistema foram integradas num único sistema composto que veio substituir os sistemas de comunicações de comando e de área, na área de operações da divisão e do corpo de exército. O sistema MSE pretendeu fornecer aos seus utilizadores um meio de comunicar através do campo de batalha, independente da localização, e numa situação móvel ou dinâmica. O sistema reduziu significativamente a necessidade de instalação de fio ou cabo aquando do estabelecimento de postos de comando. (GLOBALSECURITY, 2008a).

Todo o sistema está assente em cabinas (*shelters*) montadas em viaturas HMMWV[44] e é facilmente transportável em aeronaves *roll-on* e *roll-off*. Terminais de satélite táctico (TACSAT) e equipamento de difusão troposférica garantem ao sistema MSE um aumento do seu alcance operacional. Igualmente importante é o sistema de controlo integrado (ISYSCON), o qual providencia ao G6 e ao seu Estado-Maior uma capacidade automatizada para planear, gerir e operar todos os sistemas e redes disponíveis à força. Este sistema faz igualmente a integração do MSE no *Army Battle Command System* (ABCS)[45] (FM-11.55, 1999: 1-3).

b. O conceito LandWarNet[46] do Exército dos EUA aplicado aos *Brigade Combat Teams*

No âmbito da reformulação em curso no Exército Norte-Americano, as novas brigadas[47] passaram a ser as principais unidades tácticas. Três tipos de BCT materializam o poder de manobra do exército modular: Brigadas pesadas (HBCT), Brigadas ligeiras (IBCT) e Brigadas Stryker (SBCT). Estes BCTs, ilustradas na figura 6, melhoraram significativamente as capacidades de C2 e de armas combinadas orgânicas, incluindo a manobra, fogos e reconhecimento ao escalão batalhão, e as subunidades logísticas. (FMI-6.02.50, 2005: 10-5)

A estrutura das BCT incorpora a flexibilidade táctica no C2 da brigada. Cada BCT possui dois postos de comando (PCPrinc e PCTact) e um grupo de comando móvel

[42] Até escalão Corpo de Exército.
[43] *Random Access Discrete Address* (RADA): Técnica de Comunicações na qual rádio-utilizadores partilham uma banda larga de frequências, ao invés de a cada utilizador ser atribuída uma banda estreita.
[44] HMMWV: *High Mobility Multipurpose Wheeled Vehicle*
[45] O ABCS consiste a combinação de todos os sistemas de C2 do Exército (actualmente são quinze). É basicamente um pacote de aplicações que apoia a manobra, fogos, informações, defesa aérea, e apoio de combate e de serviços aos vários escalões.
[46] Ver Apêndice 6.
[47] Três tipos de brigadas para Combate e Manobra e cinco tipos de brigadas de apoio.

(GCM). O PCTact é pequeno e muito móvel. O CMDT utiliza esse PC para controlar as operações correntes, ou para controlar toda a brigada temporariamente, quando o PCPrinc se está a deslocar. O PCPrinc, responsável pelo planeamento das operações e sustentação integrada, serve como ligação principal aos comandos adjacentes e superiores. Tanto o PCTact como o PCPrinc incluem equipas de controlo aéreo tácticas (TACP). O CMDT da BCT dispõe igualmente de um GCM possuidor de capacidade de comando da batalha em movimento. Os CMDTs utilizam o GCM para se movimentarem para o local do campo de batalha onde a sua presença pessoal mais possa contribuir para o cumprimento da missão.

Pretende-se que as comunicações das BCTs sejam mais robustas e fiáveis, permitindo desse modo um comando da batalha eficaz. Este pacote inclui a capacidade *Blue Force Tracking* até ao escalão Companhia, o que permite a detecção e partilha automática das localizações das unidades. Este factor, aliado a auxílios de navegação, elimina grande parte da incerteza nas decisões referentes à manobra terrestre e à coordenação de movimentos. O ABCS permite o uso de mapas digitais, automatizando os diagramas de situação, ferramentas colaborativas e outros auxiliares de apoio à decisão que ajudam o CMDT a visualizar possíveis modalidades de acção e a discutir estas com o seu Estado-Maior e outros CMDTs, subordinados, adjacentes ou superiores. As comunicações digitais melhoram o volume, qualidade, e segurança da informação que os CMDTs podem obter e partilhar. Estas capacidades também melhoram a conectividade a outras redes e a outras fontes de apoio externas. Uma maior quantidade de informações pode assim ser descarregada de escalões superiores do Exército ou conjuntos para melhorar o planeamento e orientar as capacidades orgânicas de reconhecimento, vigilância e *targetting*.

Tomando como caso de estudo dos três tipos de brigada de manobra, a Brigada Stryker, constata-se que a rede de informação da mesma fornece a conectividade de rede para o funcionamento do C4ISR. O sistema C4ISR integra a doutrina, procedimentos, estruturas organizacionais, pessoal, equipamento, instalações e comunicações. Têm como objectivo: (FM-6.02.2, 2003: 3-1,3-20)

(1) Providenciar a informação necessária para desenvolver a *situation awareness* em apoio da missão do CMDT;
(2) Apoiar a implementação do C2 do CMDT em todo o espectro das operações militares, regulando fogos e forças de acordo com a intenção do CMDT;
(3) Fornecer uma ligação para o desenvolvimento da IOC da situação;
(4) Localizar, seguir, e empenhar alvos críticos;
(5) Conduzir operações com meios letais e não-letais;

(6) Operar com forças conjuntas e combinadas;

(7) Reconhecer e proteger as suas próprias forças.

A rápida agregação e disseminação da informação relevante com maior velocidade e precisão tornam-se críticas dentro do conceito de operação. Esta situação permite que no planeamento e execução de efeitos de massa, exista um significativo aumento da sincronização de unidades altamente móveis e dispersas no terreno.

As características operacionais C4ISR que definem a sua arquitectura são:

(1) A projecção da Brigada Stryker garante uma força de combate credível 96 horas após a aterragem da primeira aeronave.

(2) Dependência do HICON[48] para garantia da informação.

(3) Confiança no JFLCC[49] para apoio e compreensão situacional conjunta do espaço de batalha.

(4) As operações conjuntas são conduzidas em áreas de operações não contíguas com unidades constituídas de acordo com a situação, altamente dispersas, móveis e letais.

(5) As actividades C4ISR apoiam a força do alerta à execução.

(6) As tecnologias dos SIC garantem acesso à *Global Information Grid* (GIG).

(7) A assinatura no terreno da Brigada Stryker é minimizada através de *reach-back*.

(8) Aumento da interacção com sistemas ou pessoal externos às Brigadas Stryker.

(9) Um maior e melhor sistema C4ISR permite ao CMDT concentrar efeitos em detrimento de forças.

A eficácia da Brigada Stryker como uma força de entrada inicial depende muito da sua capacidade de estabelecer comunicações *reach-back* para compensar a ausência inicial de capacidades de combate, apoio de combate e apoio de serviços. As comunicações *reach-back* expandem as capacidades da força, permitindo-lhe operar em todo o espectro das operações militares, ao mesmo tempo que reduz o seu *footprint* no teatro. Comunicações de C2 para um HICON terão de ser asseguradas através de meios não orgânicos da brigada Stryker[50], dado que esta depende do HICON para estes meios *reach-back*. Comunicações *reach-back* para aceder a bases de dados de informações e de

[48] HICON: *Higher Control*
[49] JFLCC: *Joint Force Land Component Commander*
[50] Ao contrário do que acontece no SIC-T, onde está previsto um módulo *rear-link*.

informação acerca de meios nacionais são efectuadas com meios orgânicos através da rede Trojan Spirit (FM-6.02.2, 2003: 3-5).[51]

A ligação da brigada Stryker à GIG permite-lhe alcançar e aceder a bases de dados, produtos e conhecimento existentes, nos recursos de vigilância e reconhecimento do ramo, conjuntos e nacionais. As comunicações *reach-back* permitem a colaboração, partilha de tarefas e acesso a bases de dados de escalões superiores. A capacidade de comunicações *reach-back* para expandir o poder e eficácia da força advém do facto de o CMDT poder utilizar recursos externos à sua área de responsabilidade. As comunicações *reach-back* apoiam directamente as áreas de fogos e efeitos, informações, planeamento e análise, protecção da força e apoio logístico.

As sub-redes existentes da Brigada Stryker estão apresentadas na Tabela 3.

Tabela 3. Sub-redes existentes na Brigada Stryker (FM-6.02.2, 2003: 3-5)

Órgão da Brigada Sryker	Sub-redes					
	WAN	TI	CNR	COT a COT	GBS	Rede de planeamento Colaborativo
PC Princ	X	X	X	X	X	X
PC Tact	X	X	X	X	X	
Escalão recuado (BSA)	X	X	X	X	X	X
GRSTA		X	X	X	X	X
BI (x3)		X	X	X	X	X
GAC		X	X	X	X	X

A **WAN** providencia serviços de telefonia, dados, planeamento colaborativo e BVTC[52] aos PCTact, PCPrinc e BSB da brigada Stryker. Esta capacidade orgânica BVTC não é estendida ao GRSTA[53] (a não ser que este esteja colocalizado com o PCPrinc) ou aos batalhões. A WAN da brigada Stryker assenta primariamente nos terminais tácticos orgânicos inteligentes AN/TSC-154, localizados nos PCs e BSA para alcançar conectividade intra-teatro. Estes terminais multicanais TACSAT, apoiados em satélites MILSTAR, fornecem a transmissão para voz, dados e vídeo com elevada largura de banda.

A **Internet táctica (IT)** integra os sistemas EPLRS, FBCB2 e os sistemas de comunicações que os apoiam numa rede de dados móvel. A IT fornece capacidades de troca de dados ao nível da SSA e do C2 a todas as plataformas equipadas com sistemas FBCB2. A IT também permite aceder à rede com o FBCB2 em qualquer lugar, desde que o sistema esteja em linha de vista com os outros meios de IT

[51] *Trojan* SPIRIT (*Special Purpose Integrated Remote Intelligence Terminal*). Rede SATCOM que liga utilizadores projectados às WANs de teatro TS/SCI JWICS e à National Security Agency (NSA).
[52] BVTC: *battlefield video teleconferencing*
[53] GRSTA: *Ground Reconnaissance, surveillance, and targetting aquisition.*

A **CNR** fornece à brigada Stryker capacidades VHF-FM, HF-AM e TACSAT-UHF Monocanal para executar o C2 das forças em todo o espaço de batalha da brigada. A CNR é utilizada principalmente para a transmissão de voz para C2.

A **rede de dados COT a COT** permite aos utilizadores trocar informação de C2 entre os Centros de Operações Tácticos (COT) e plataformas chave de C2. O rádio digital de curto alcance (NTDR)[54] é um substituto temporário do *Joint Tactical Radio System* (JTRS) e providencia a conectividade da rede de dados COT-a-COT dentro da brigada Stryker. A rede de dados COT-a-COT utiliza cada NTDR presente na rede como um relé.

O **Sistema de Difusão Global** (GBS)[55] permite ao Estado Maior da brigada Stryker receber produtos que requerem elevada largura de banda, tais como imagens, dados logísticos, dados meteorológicos e informação cartográfica digitalizada. O GBS está localizado primariamente nos PCs principal e táctico, e nos PCs das unidades de escalão batalhão. O GBS permite aos CMDTs tácticos receber, aceder, recolher e arquivar este tipo de dados. Exemplos de informação que pode ser enviado sobre o GBS incluem: difusão de vídeo, transmissões vídeo de UAVs, *overlays* da IOC, difusão de notícias de operadoras comerciais de televisão, e outros dados de grande volume.

A **rede de planeamento cooperativo** é um sistema baseado em comunicações satélite de operadores comerciais e que se destina a colmatar lacunas actualmente não cobertas pelos demais sistemas em utilização. Esta rede permite ao CMDT trocar informação de planeamento e operações nos modos de voz, dados e vídeo entre os COTs da brigada Stryker e plataformas chave de C2 que não estejam em linha de vista. Os sistemas satélite e BVTC baseados em equipamentos COTS são montados nos nós chave apresentados na tabela 3.

Os sistemas de comunicações que suportam a rede de informação da brigada Stryker estão ilustrados na figura 7 (FM-6.02.2, 2003: 3-5, 3-15): Incluem:

Terminais TACSAT Multicanal. A brigada Stryker utiliza o AN/TSC-154 SMART-T para ligações intra-brigada. Este terminal de comunicações TACSAT é montado num veículo HMMWV. Opera com a rede satélite MILSTAR na gama EHF, com ritmos de transmissão de dados baixo e médio (de 75 Bit/s a 1.544KBit/s, com uma largura de banda agregada máxima de 2.240KBit/s). Os equipamentos SMART-T providenciam conectividade militar e comercial para comunicações de dados, imagens, vídeo e áudio.

[54] NTDR - *Near Term Digital Radio*: Possui uma largura de banda para transmissão de dados de 300KBit/s.
[55] GBS - *Global Broadcast Service*

Encontra-se nos postos de comando da brigada e no escalão recuado. Serão utilizados meios não orgânicos (AN/TSC-85C, AN/TSC-93C, ou terminais satélite comerciais) para ligações a redes externas e ligações *reach-back* a um HICON. Terminais não orgânicos serão disponibilizados pelo HICON, ou por unidades de apoio sob controlo do HICON, e estarão presentes no PCPrinc e no EscRec.

JTRS/NTDR. O NTDR é um substituto temporário para o JTRS e será mantido até este último entrar em acção. O rádio NTDR está presente nos COT e veículos seleccionados de C2, apresentando interfaces LAN (Ethernet) and série. Possui um alcance de 10-20 km e tem incorporado um receptor GPS.

O **EPLRS** constitui a espinha dorsal da IT da brigada Stryker, a qual é utilizada para distribuir informação de SA e C2 por todo o espaço de batalha.

SINCGARS é uma família de rádios de combate (CNR) VHF-FM que constituem o principal meio de comunicações de C2 para as subunidades da Brigada Stryker. Os rádios SINCGARS podem transmitir e receber voz e dados (16KBit/s de largura de banda), sendo compatíveis com os formatos NATO, embora apenas em modo não seguro.

c. Enquadramento Conceptual e Estruturas Lógicas dos módulos SIC-T

O Sistema de Informação e Comunicações Táctico do Exército Português foi concebido para ser flexível perante a crescente complexidade dos sistemas e novas tecnologias de informação. Para além se ter pretendido garantir a ligação, sempre vital, entre os soldados no seu ambiente táctico e a sua estrutura de comando, pretendeu-se dotar a estrutura do comando de um acesso sem restrições à informação necessária ao exercício do C2. As preocupações técnicas focalizaram-se inevitavelmente no domínio da interoperabilidade em operações conjuntas e combinadas, e com os sistemas de comunicações fixos. Houve igualmente uma preocupação com a capacidade de transporte da informação num ambiente seguro (DCSI, 2006: 1).

O SIC-T baseia-se numa tecnologia de transferência de informação “Full IP” (Internet Protocol). Trata-se de uma estrutura modular, eficiente, segura, flexível e preparada para proporcionar ao comando, às informações, à logística e às unidades de combate, uma grande mobilidade e a necessária adaptabilidade às novas exigências do campo de batalha. Não considerando a componente de informação (SICCE) do SIC-T, o sistema tem por base uma arquitectura modular e funcional capaz de suportar um conjunto de teleserviços que percorrem de forma transparente os diversos módulos, subsistemas ou meios de transmissão, com o mínimo envolvimento do utilizador (DCSI, 2006: 2).

A arquitectura do SIC-T, na sua componente de comunicações (SITACO) subdivide-se num Subsistema de Área Estendida (SAE), num Subsistema de Área Local (SAL), num Subsistema de Utilizadores Móveis (SUM), num Subsistema de Gestão de Rede (SGR) e num Subsistema de Segurança de Rede (SSR), efectuando o SGR e o SSR a cobertura transversal a todo o sistema (ver figura 8). O SSR constitui-se como o garante da segurança da informação veiculada na rede e o SGR como o "cérebro da rede". Para a implementação da arquitectura funcional do SIC-T foram projectados sete módulos sistémicos, materializantes dos subsistemas: Nó de Trânsito (NT), Nó de Acesso (NA), Ponto de Acesso Rádio (PAR), Rear Link (RL), CCom de Batalhão (CCB), CCom de Companhia (CCC) e Centro de Gestão de Rede (CGR) (DCSI, 2006: 2).

(1) O Subsistema de Área Estendida

O SAE, constituindo a espinha dorsal (*backbone*) da rede, compõe-se por um conjunto de nós de comutação, interligados fundamentalmente por ligações rádio multicanal (feixes hertzianos). A partir de cada nó são sempre estabelecidos no mínimo duas (preferencialmente três) ligações, proporcionando-se caminhos alternativos para a informação e garantindo a estrutura em malha da rede. O SAE integra os módulos NT e RL (DCSI, 2006: 2-4), ilustrados nas figuras 9 e 10.

O NT poderá estabelecer até quatro ligações, com base em equipamentos de feixes hertzianos (FHz) de instalação fácil e rápida, a funcionar na banda "IV" a 8 Mbps com tecnologia *Forward Error Correction* (FEC) de raiz. Empenhado no seu contributo para a flexibilidade do sistema, este módulo disponibiliza igualmente outros suportes físicos para o estabelecimento da ligação, tais como, cabo óptico (nas distâncias de 300, 1.000, 5.000 e 10.000 metros) e par de cobre (WD1-TT) associado à tecnologia *Symetric High-Speed Subscriber Line* (SHDSL) (aproximadamente até uma distância de 4.000 m).

A segurança nos *links* de FHZ é garantida por um sistema de *bulk encryption* (BE), onde se realiza uma simulação de tráfego na ligação, com ritmos aleatórios independentemente de existir ou não tráfego real. Proporciona-se assim um mascaramento da informação transmitida, conseguido como resultado da injecção de tráfego pelo BE, o que induz o In em erro de análise, mesmo quando não existe tráfego na ligação.

É de notar um paralelismo interessante entre o conceito de NT e o do Centro Nodal (NC) do sistema MSE norte-americano. Com excepção de dois factores, a característica Full IP do SIC-T e as larguras de banda envolvidas nos *links* de FHz (1.5 Mbit/s para as ligações de FHz no MSE, 8 Mbit/s para as do SIC-T) a mesma filosofia de um dispositivo em malha está presente nos dois sistemas. No entanto, como se viu anteriormente, a

tendência no novo sistema americano LandWarNet (LWN) abandona o conceito de NC e substitui as ligações em FHz entre as UEB e superiores por *links* satélite de alto débito.

O módulo RL destina-se normalmente a ser projectado com uma Força a operar fora do território nacional e é instalado junto ao Posto de Comando (PC) dessa Força, para garantir a ligação à retaguarda (território nacional). Pode igualmente ser utilizado, embora com algumas limitações, para interligar via satélite dois NTs em operações convencionais. Este módulo faz parte do SAE, considerando-se como um nó do sistema, apesar de ser normalmente instalado junto ao PC da Força apoiada (SAL).

Destaca-se neste módulo a capacidade satélite, com terminais emissores/receptores de banda larga, com flexibilidade para utilização de satélites civis comerciais ou disponibilizados pela NATO a operar nas bandas "K_U" e "X" respectivamente[56]. Dispõe ainda de uma componente de High Frequency (HF), especialmente provida de duas vertentes: a primeira, para garantir multiplicidade de meios de modo a consolidar a ligação à retaguarda, e a segunda, para garantir as ligações, quando necessário, a grandes distâncias dentro da área de operações da Força a operar fora do território nacional.

Este módulo pode contemplar também o sistema TETRA, destinado a colmatar o défice de apoio de comunicações usualmente sentido em CROs quando ocorrem em áreas edificadas, uma vez que se trata de um sistema vocacionado para funcionar nesse tipo de ambiente. O seu modo de funcionamento assemelha-se aos telefones celulares, sendo contudo complementados com mecanismos de cifra, de chamadas de grupo, de chamadas emergência e prioritárias.

Efectuando novamente uma comparação com os sistemas norte-americanos, sobressai novamente a similaridade com o sistema MSE (uma única ligação TACSAT para o escalão superior ou para o Teatro Nacional). Ao contrário, na Brigada Stryker o conceito LWN permite já uma redundância substancial ao nível de ligações TACSAT ao escalão superior. Esta limitação foi já detectada pelo Exército e estão actualmente em estudo na DCSI propostas que visam solucionar essa vulnerabilidade (SILVA, 2008).

(2) O Subsistema de Área Local

O SAL destina-se intrinsecamente a proporcionar, a um determinado grupo de utilizadores normalmente localizados num PC, as diversas categorias de serviços (voz, dados, C2, mensagens, fax ou vídeo) disponíveis na rede, e extrinsecamente, garante o acesso à estrutura superior da rede (o SAE), através de um conjunto de nós de acesso. A

[56] Gama de frequências: Banda X- 7-12,5 GHz; Banda K_U: 12-18 GHz.

concepção modular do SAL, igualmente pensado para proporcionar flexibilidade ao sistema, permite a adopção de diferentes topologias compatíveis com o escalão táctico a apoiar, seja ele de Brigada, Batalhão ou Companhia. Assim, este subsistema é constituído pelos módulos SIC-T Nó de Acesso (NA), Centro de Comunicações de Batalhão (CCB) e Centro de Comunicações de Companhia (CCC). A filosofia presente no SAL com os seus módulos é bastante semelhante à das Extensões de Acesso (EA) do sistema MSE.

O CCB e o CCC, servindo respectivamente o PC do Batalhão e de Companhia, podem também, face à sua grande mobilidade, integrar o Subsistema de Utilizadores Móveis (SUM), quando não necessariamente arreigados ao serviço do PC, mas a fazerem uso da sua componente de Ponto de Acesso Rádio. (DCSI, 2006: 4-11)

A complexidade subjacente ao NA obrigou à sua concepção em dois *shelter*s, um de Transmissão e outro de C2 e Gestão (ver figuras 11, 12 e 13). Estando os meios radiantes colocados num único *shelter*, este pode ser afastado do PC, seleccionando-se para o efeito uma posição suficientemente elevada para permitir melhores condições de propagação. O NA sustenta a possibilidade de estabelecer três ligações de FHZ a 8 Mbps, uma ligação Satélite INMARSAT em ambiente IP (com limitada largura de banda) e em terminal analógico do tipo Mini M, quatro acessos HDSL (WD1-TT), cinco acessos ópticos (Expansão, *shelter* de C2 & Gestão, módulo RED, TINA e reserva), acesso IP/ Global System for Mobile Communications (GSM), multiconferência até oito utilizadores (em voz ou vídeo) extensível a toda a rede, central de Comutação para telefones analógicos e RDIS, comutação em ambiente IP (para telefones IP), rede local Wi- Fi (dados e voz) e ainda acesso dedicado à Internet, quando for possível a ligação a um ISP.

É neste *shelter* que reside a capacidade para disponibilizar os teleserviços aos utilizadores do PC, normalmente acantonados em tenda ou em contentores localizados nas imediações. No interior deste *shelter* poderá organicamente funcionar o G6, juntamente com os militares responsáveis pela gestão de rede e do subsistema de informação (SICCE). O mesmo *shelter* aloja para transporte um Módulo Red que é deslocado para o interior do PC (tenda ou contentor) e permite trabalhar, nesta área, informação classificada até ao grau de NATO SECRET/SECRETO (voz e dados), classificação de segurança garantida pelo equipamento de cifra IP - TCE 621.

O módulo CCB, não obstante estar ao serviço de um escalão inferior, Batalhão, possui uma concepção similar ao NA. Por esse motivo é composto pelo mesmo tipo de sub módulos (*shelter*s), "Transmissão" e "C2 & Gestão", ambos instalados em *shelter*s do tipo

T100. No entanto, atendendo às características do escalão apoiado, apresenta algumas diferenças conceptuais, tanto ao nível do *shelter* de "C2 & Gestão" como de "Transmissão". É todavia no *shelter* de "Transmissão", que residem as maiores discrepâncias pela exigência que lhe é atribuída em disponibilizar a interligação com o escalão superior e garantir a ligação ao escalão inferior, este último com grande mobilidade e com necessidades de comunicações específicas características das redes de combate rádio. Este *shelter*, normalmente instalado numa zona elevada e relativamente afastada do PC, apresenta as seguintes possibilidades: Rádio de Banda Larga (UHF), para ligação ao escalão inferior; *mini-link Line of Sight* (LOS) a 2 Mbps, para ligação ao escalão superior; quatro acessos SHDSL, para ligação ao escalão inferior e superior; satélite INMARSAT em ambiente IP; acessos ópticos; acesso IP/GSM; Rádio de Combate (PAR).

Existe assim, a partir do escalão Batalhão e junto ao seu PC, a capacidade para efectuar a integração rádio no ambiente IP da estrutura superior da rede. Esta integração das redes rádio de combate (P/525), em caso de necessidade, pode permitir a ligação ao PC das Companhias e garantir a integração de todos os utilizadores do subsistema móvel que apenas disponham do rádio P/525 como meio de comunicação, e que se localizem na área de cobertura do CCB (ver figuras 14, 15 e 16).

O Shelter de "C2 & Gestão", como se referiu anteriormente, é conceptualmente similar ao mesmo tipo de *shelter* existente no NA, apenas disponibilizando um número inferior de terminais de utilizador, sendo o escalão mais baixo onde ainda é possível veicular informação classificada com o grau de NATO SECRET/SECRETO.

Para o CCC, foi adoptada uma estrutura bastante mais ligeira, compatível com a mobilidade característica desta subunidade, e que é ilustrada na figura 17. Trata-se de um único *shelter* a ser instalado em viatura táctica ligeira de rodas (VTLR). Este tipo de *shelter*, para além de permitir a instalação dos equipamentos de comunicações, tem ainda integrado uma componente de energia (gerador) e mastros. Este módulo contempla: uma componente de gestão e controlo; os habituais interfaces ópticos, que permitem a interligação até às distâncias atrás referidas, de 300 a 10.000 m, dependendo dos cabos ópticos disponíveis; interfaces SHDSL; telefones analógicos (suportados por cabos WD1-TT); telefones IP; acesso Wi-Fi para voz e dados; Rádio de Banda Larga; *mini link* (LOS) de Feixes a 2 Mbps para ligação ao escalão superior; Capacidade de integração rádio de combate em ambiente IP, especialmente vocacionado para integrar os utilizadores no escalão inferior (igual ao módulo de batalhão).

(3) O Subsistema de Utilizadores Móveis

O SUM[57] destina-se basicamente ao apoio destes utilizadores profusamente disseminados pela área de operações, e consequentemente a sua concepção adapta-se às características de uma actuação mais independente, mas que pode ser simultaneamente integrado na rede táctica através dos Pontos de Acesso Rádio (PAR)[58]. As categorias de teleserviços previstos neste subsistema são as mesmas que existem no SAL, exceptuando as restrições de largura de banda, impostas pelos equipamentos utilizados neste subsistema. O SUM integra o módulo PAR (ver figura 18) e os utilizadores da rede rádio de combate, equipados com o P/525 (DCSI, 2006: 11-14).

O PAR detém a capacidade para implementar dois *links* de FHZ a 8 Mbps, os tradicionais interfaces ópticos, acessos SHDSL, a gestão local e disponibiliza ainda um número mínimo de terminais para utilização local (em voz e dados). A função principal do PAR é a integração do rádio P/525 em ambiente IP, através de chamadas de voz por marcação automática para a rede IP, de chamadas selectivas para o rádio e de um serviço de dados com implementação da internet táctica. Esta integração IP/Rádio no PAR é implementada de modo a flexibilizar o sistema, pois permite atribuir, de forma dinâmica, os rádios ao serviço de voz ou de dados (internet táctica) até ao máximo de seis rádios.

A utilização do PAR, e especialmente do SICCE, nos escalões mais baixos, irá introduzir alterações significativas na doutrina de utilização das redes rádio tradicionais (Pessoal, Operações, Informações, Logística, etc.). Inevitavelmente por imposição da arquitectura tecnológica adoptada, os dois tipos de redes passam a coexistir, e os utilizadores munidos deste meio de comunicação rádio passam a poder integrar-se, através do PAR, em pequenas redes rádio, normalmente a funcionar em modo de dados, onde terão acesso à situação operacional, permanentemente actualizada, disponibilizada pelo sistema de informação. Estes utilizadores formarão pequenas redes tácticas com elementos interligados entre si e à estrutura superior da rede através dos PARs, que como se viu, poderão para além deste módulo localizar-se igualmente nos CCB ou CCC.

[57] Todos os utilizadores de uma rede táctica de comunicações apresentam um grau de mobilidade relativa, uma vez que mudam de posição com maior ou menor frequência, contudo estes utilizadores, do SUM, caracterizam-se especialmente pela seu maior desprendimento à afixação a uma determinada área de operações, daí o termo "utilizadores móveis".

[58] Os conceitos de emprego dos PAR no SIC-T e no MSE são semelhantes. O que difere são os tipos de terminais que podem aceder a este serviço: no MSE limitam-se aos MSRT, no SIC-T para além do elemento base da CNR, o rádio p/525, qualquer terminal IP pode usufruir deste serviço.

Caso a situação táctica o permita, deixarão de existir redes de voz de carácter permanente, pois como atrás se mencionou, os utilizadores posicionam-se na rede de dados a actualizar a informação operacional (enviar e receber dados) sendo que, e aquando da existência de uma chamada de voz, são então avisados acusticamente ou através do ecrã do terminal de dados. Automaticamente ou à sua ordem, o rádio é retirado da frequência, dentro da rede de dados onde operava, passando automaticamente a dispor de uma frequência destinada a estabelecer a chamada de voz "dedicada" (ponto-a-ponto) com o seu interlocutor, que pode estar a utilizar outro meio rádio ou outro equipamento (p. ex. telefone IP) em qualquer ponto da rede táctica. Também pode o utilizador rádio, quando pretender iniciar uma chamada de voz, posicionar-se para o efeito numa frequência prevista pelo sistema para esta finalidade, efectuando a marcação automática para a rede IP, ou rádio, através de marcação telefónica disponibilizada pelo rádio.

No SIC-T o plano de numeração para as chamadas de voz têm também uma filosofia diferente da habitual, onde as tradicionais listas telefónicas estão exaustivamente impregnadas com informação de números de telefone que meramente respondiam por posições rígidas despersonalizadas. No novo sistema, perfeitamente conivente com a exigência da mobilidade de utilizadores e subsistemas, foi criado um conjunto de funcionalidades adicionais específicas para ambientes militares.

A cada utilizador validado do sistema será atribuído um número pessoal, o qual sempre que deseje os recursos de comunicações disponibilizados pelo sistema, procederá à sua afiliação na rede. Este serviço permite, a qualquer utilizador, o uso de qualquer terminal de rede, para fazer e receber chamadas automaticamente credenciadas através do próprio número pessoal que lhe foi previamente atribuído. Este facto anula o defeito tradicional da chamada poder ser só imputada a uma posição fixa responsável pela sua feitura ou recepção, sendo então encaminhada para o local e terminal da afiliação do utilizador. Estas chamadas serão condicionadas concordantemente com os seus privilégios de acesso (o perfil do utilizador passa a ser percepcionado pela gestão da própria rede), pois deixa de ser possível receber ou efectuar chamadas com equipamentos ligados à rede onde não existam afiliações de utilizadores. Num ambiente de trabalho de Estado-Maior, onde normalmente existem mais utilizadores do que propriamente terminais de voz disponíveis, é ainda acrescida a possibilidade de afiliação múltipla, onde diferentes utilizadores se podem afiliar no mesmo terminal.

É também implementado um serviço (de perfil compatível com o utente) de atribuição de prioridades de rede, que garante aos utentes com prioridade mais elevada

recursos para que possam efectuar as suas comunicações. O sistema gere a largura de banda dinamicamente, desligando ou recusando chamadas de utentes menos prioritários e redireccionando esses recursos para utentes com perfil de mais elevada prioridade.

(4) O Subsistema de Segurança de Rede

O SSR implementa diferentes níveis de segurança nas diferentes áreas de rede do SIC-T (*red* e *black*), sendo transversal a todos os módulos do SIC-T. No Nó de Acesso e no Centro de Comunicações de Batalhão, o sistema está preparado para veicular informação com a classificação de segurança até NATO SECRET/SECRETO. Deste modo, caso se pretenda classificar a informação disponível no SICCE com este nível de segurança, a base de dados real da componente operacional do Exército só estará disponível até ao PC de Batalhão.

Nos escalões inferiores, apesar de existirem mecanismos de segurança implementados, o sistema não utiliza equipamentos certificados pela NATO. É este o caso do rádio de combate P/525, certificado pela Autoridade de Segurança Alemã em CONFIDENCIAL[59]. As ligações de FHZ também dispõem de equipamento de cifra (*bulk encryption*), que reforça o mecanismo de segurança da rede.

Prevê-se numa primeira fase, que ao nível do escalão Batalhão poderá existir um *gateway* implementado com recursos humanos, que mantenha a base de dados operacional actualizada com informação relevante, proveniente das suas Companhias, a operar com um sistema de informação eventualmente adaptado do SICCE para baixos escalões - Sistema de Informação para os Baixos Escalões (SIBE) (DCSI, 2006: 14-15).

(5) O Subsistema de Gestão de Rede

O SGR ainda em fase embrionária, apresentará uma arquitectura modular assente no módulo Centro de Gestão de Rede (CGR), que se constituirá como o "cérebro" do sistema de comunicações. O CGR desempenha as funções de *System Executive and Plans* (SEP) e *Operational System Control* (OSC), requerido no modelo Eurocom para administração de redes. Os terminais de controlo (TC), instalados ao nível de cada módulo, são responsáveis por produzir a informação crítica sobre o módulo local, para apoio do administrador local e enviá-la automaticamente para o CGR. O TC desempenha a função de *Facility Control* (FC) do modelo Eurocom.

Em cada operação táctica aonde necessariamente se empenhem meios do SIC-T, devem existir no mínimo dois CGR: um activo, habitualmente no PC Principal da força

[59] A Autoridade Nacional de Segurança (ANS) ainda não certificou nenhum componente do SIC-T.

apoiada; e um de reserva (auxiliar), para assegurar a redundância e a sobrevivência do próprio sistema de comunicações como um todo. Esta redundância é comum também aos sistemas norte-americanos LWN e MSE.

A evolução das operações obriga a constantes mudanças dos PC, logo, dos "nós" do sistema, com eventuais perdas temporárias de ligações por parte desses nós. Assim, se o nó onde o CGR estiver a operar ficar temporariamente desligado, o sistema garantirá a sua total funcionalidade com a entrada em funcionamento do CGR auxiliar, garantindo desde logo a actualização automática da informação necessária à gestão da rede. (DCSI,2006: 15)

d. O SIC-T na manobra da brigada

Com a tecnologia actualmente disponível para o sistema C4ISR, o escalão Brigada pode ser empenhado em missões num Espaço de Batalha (EB) que anteriormente era atribuído ao escalão Divisão (EME, 2006: 2-33). A Força Operacional Permanente do Exército (FOPE) apresenta actualmente como componente principal três brigadas: a Brigada de Reacção Rápida (BrigRR), Brigada Mecanizada (BrigMec) e Brigada de Intervenção (BrigInt). Cada uma destas brigadas é apoiada por uma CTm, todas com a mesma constituição e possibilidades idênticas[60].

Á medida que ocorrer a movimentação das subunidades da Brigada, o SIC-T reorganizar-se-á para apoiar a manobra. A direcção da manobra e a localização das unidades de combate, apoio de combate e apoio de serviços irão ditar a localização das unidades de Transmissões. (FM-11.55, 1999: 2-1,2-10)

Em operações convencionais, os nós de trânsito (NT) deverão ser dispostos a partir da área da retaguarda da brigada até ao limite máximo avançado dos trens de batalhão, baseados em factores geográficos e de densidade de assinantes. Estes nós, módulos integrantes do SAE, constituem a base de toda a capacidade de *networking* intra-brigada. Os NT são independentes da estrutura de comando existente. No SIC-T, todos os NT deverão ser empregues de modo a garantir o máximo de redundância e flexibilidade de ligações. Cada NT dever-se-á ligar a pelo menos outros dois NT[61] para garantir uma capacidade de sobrevivência do encaminhamento de tráfego. Fica assim formada a grelha do *backbone* da rede. Os módulos RL podem ser utilizados, embora com algumas limitações, para interligar via satélite dois NT em operações convencionais, contornando assim eventuais limitações impostas pelo terreno (ver figura 21).

[60] As suas possibilidades são descritas no Apêndice 8.
[61] Da própria brigada ou da brigada adjacente.

(1) Relações de comando e apoio das unidades de Transmissões

No que diz respeito a relações de comando, as unidades de Tm podem ser dadas em reforço ou ser colocadas sobre controlo operacional. A CTmAp, pode por exemplo reforçar com a totalidade ou parte dos seus meios a Brigada de Reacção Rápida (BRR) quando esta se constituir no núcleo de um Battle Group[62] (QOP CTmAp, 2005: 1). O CMDT reforçado exerce um grau de C2 sobre a unidade em reforço igual ao exercido sobre a unidade orgânica sob o seu comando, normalmente comando completo. Quando NTs ou meios de comunicações estratégicas (ou seja, os componentes do SAE) são atribuídos da CTmAp às CTm das Brigadas, os comandantes das CTm das Brigadas são a autoridade responsável pelo seu emprego. Embora o reforço seja apenas temporário, deverá ser cuidadosamente planeada a cedência desses meios de Tm: uma vez empregues no campo de batalha e integrados na rede, uma posterior alteração da relação de comando, não se traduz no imediato, dado que se torna necessária a reconfiguração do *backbone* (ver figuras 19 e 20).

O controlo operacional (OPCON) é a autoridade conferida ou delegada num comandante para dirigir forças atribuídas, no desempenho de missões ou tarefas específicas, pormenorizando a execução se necessário. As missões ou tarefas são limitadas pela natureza, tempo e localização. Não inclui autoridade para utilizar separadamente os elementos que constituem as unidades envolvidas, nem tão pouco, comporta em si o controlo administrativo-logístico. (RC-OPERAÇÕES, 2007: II.2.5). As subunidades de TM deverão ser colocadas sob OPCON, durante movimentos, sempre que for necessário fazer avançar o dispositivo. De uma perspectiva de brigada, os meios de Tm[63] são colocados sob OPCON das UEB de manobra durante a execução de movimentos. Tal ocorre quando essas UEB são responsáveis pelos movimentos ao longo de eixos ou corredores designados e têm de controlar todas as unidades que se movimentam na sua área. Assim que as subunidades de Tm ocupam e se instalam na área que lhes foi atribuída, a relação de OPCON cessa. Normalmente, a relação de autoridade OPCON não é utilizada para outros fins (FM-11.55, 1999: 2-8).

Na doutrina dos EUA o grau de autoridade controlo técnico TECHCON é um grau de C2 exclusivo das Tm que confere a autoridade para controlar os aspectos técnicos da implementação e operação dos meios de Tm (FM-11.55, 1999: 2-9). No Exército

[62] A estrutura de um *Battle Group* da EU prevê duas CTm.
[63] Fundamentalmente nós de trânsito (NT) e pontos de acesso rádio (PAR).

Português, o grau de autoridade controlo técnico[64] é definido como a autoridade delegada por um Comandante a um elemento das forças armadas, normalmente pertencente ao seu Estado Maior para difundir instruções sobre procedimentos técnicos. (RC 130-1, 1987: 4.4). Os módulos do SAE deverão assim possuir controlo técnico sobre todas as ligações a equipamentos do SAL e do SUM. Por ex., uma ligação de feixes hertzianos entre um PAR ou um CCB e um NT está sob TECHCON do NT, e é este último que controla a ligação.

Por apoio entende-se a acção de uma força ou parte dela com o objectivo de auxiliar, proteger, complementar ou sustentar outra força (RC-OPERAÇÕES, 2007: III.2.33). Na gestão das redes de comunicações da brigada, são frequentemente estabelecidas relações de apoio directo (A/D). Os meios de Tm do SAL são colocados em A/D das unidades apoiadas. O apoio logístico dos meios dos SAL será normalmente da responsabilidade da unidade de origem (a não ser que seja especificado que a responsabilidade cabe à unidade apoiada), e os meios continuarão sob TECHCON da sua unidade de origem. Todos os NT e os meios do SUM, bem como os meios de transmissão a eles associados estarão em apoio geral (A/G) da brigada. As unidades de Tm que empenhem meios na malha de rede da brigada apoiarão a força como um todo.

(2) Operações de Combate Ofensivas

A finalidade das operações ofensivas é destruir o inimigo pela aplicação dos meios de forma violenta e localizada, não apenas nos seus elementos avançados mas em toda a sua profundidade. A manobra em profundidade constitui uma ameaça, a que o inimigo tem de fazer face. Deste modo, é obrigado a reagir ao invés de tomar a iniciativa. A sua destruição física é um meio para o sucesso e não um fim em si. A ideia é provocar a paralisia e a confusão destruindo a coerência da sua defesa, fragmentando e isolando o seu poder de combate. (RC-OPERAÇÕES, 2007: III.3.1). As operações podem ser faseadas, e o apoio de SIC para cada fase depende de muitas considerações. Diferentes tipos de operações ofensivas irão ditar diferentes tipos e níveis de apoio.

Ao prepararem-se para apoiar operações ofensivas, as CTm das Brigadas devem manter NT e PAR em reserva para movimentação rápida em seguimento do primeiro escalão de ataque. Quando for possível, NT e PAR serão posicionados atrás da linha de contacto, suficientemente longe para estarem protegidos da artilharia de campanha inimiga. Deverá ser feito um esforço ao nível ISTAR para minimizar a ameaça a estes meios. Alguns PAR serão pré-posicionados à frente de forma a estender o SUM até à área dos PC

[64] Presente no antigo RC-130.1 mas não no actual Regulamento de Campanha de Operações do Exército.

das UEC. A eventual utilização de NTs de outras Brigadas na sua área da retaguarda permite à brigada que efectua o ataque maximizar os seus meios do SAE para a operação ofensiva.

Durante o ataque, os NT seguem as UEB de manobra sabendo de antemão as localizações onde se irão posicionar. Deverão ser previamente identificadas várias localizações possíveis de modo a cobrir todas as contingências. As várias equipas PAR e NT que acompanharem o escalão de ataque deverão ter opções pré-planeadas de *links* alternativos para o caso de não conseguirem estabelecer contacto com a UEB sob a qual estarão em OPCON. A topologia do SAE alterar-se-á ao longo do tempo, proporcionando pontos de acesso para SAL e SUM, para apoio das necessidades do utilizador (ver fig. 24). Durante o movimento dos nós do SAE, estes não farão parte do SAE. Ligações ao SUM, podem naturalmente ser disponibilizadas pelo pessoal do nó SAE, durante o movimento. O SAE deverá adaptar-se às mudanças de topologia resultantes da mudança de nós SAE para as novas posições. As ligações através de um nó que deixe o SAE, deverão ser reencaminhadas. Durante o reencaminhamento, algumas ligações podem ser desligadas, devido a limitações de Largura de Banda (alguns parâmetros de Qualidade de Serviço (QoS) podem não ser satisfeitos). Se os nós do SAE são ligados por satélite e são capazes de manter as ligações internas da rede, enquanto em movimento, isto não é considerado como mobilidade da rede, pois não ocorre mudança da topologia (DST, 2003: 23-26).

A CNR constituirá o meio de comunicação primário durante a movimentação da força. A utilização do RL para aumentar o alcance operacional deverá igualmente ser planeada de modo a garantir a continuidade de ligação ao escalão superior. Normalmente o PCPrinc e o EscRec da brigada não se movimentarão durante a fase inicial do ataque e continuarão ligados ao SAL, e consequentemente ao SAE. A cobertura do SUM na área da retaguarda da brigada deverá ser preterida em detrimento das operações avançadas.

(3) Operações de Combate Defensivas

Normalmente, as operações defensivas são adoptadas quando o inimigo tem a iniciativa, para o impedir de conquistar terreno ou penetrar na área defendida. Estas procuram provocar o insucesso do ataque inimigo, destruir as suas forças e impedir que atinja os seus objectivos. Desta forma, a finalidade das operações defensivas é criar as condições para a acção ofensiva. Este aspecto é fundamental para a batalha defensiva, não devendo o defensor permitir uma situação em que apenas reage às iniciativas inimigas. Todas as oportunidades devem ser aproveitadas no sentido de recuperar a iniciativa, de

forma a, adoptando uma postura pró-activa, forçar o inimigo a reagir ao plano de defesa (RC-OPERAÇÕES, 2007: III.4.1).

As CTm deverão seguir esta postura pró-activa no emprego dos seus meios. Deste modo, os meios do SUM deverão garantir a cobertura pelo menos até aos PC das UEB ao contacto. São necessárias localizações alternativas para a instalação de meios do SUM e do SAE para efeitos de sobrevivência do sistema, bem como para deslocações rápidas em caso de penetração do dispositivo. Os elementos da CTm deverão estar familiarizados com os itinerários conducentes às localizações alternativas. Alguns meios do SUM deverão estar prontos a movimentar-se para a frente acompanhando o contra-ataque. É essencial a visualização da IOC, nomeadamente a ocorrência de penetrações, de modo a garantir a sobrevivência dos meios de Tm. Devem ser feitos planos para a sincronização do movimento de meios do SUM, SAE e SAL que estejam localizados nessas áreas.

Durante uma operação defensiva, os CMDTs de Unidades de Tm devem estar preparados para mudanças rápidas nos planos da brigada. Meios que estejam em perigo devem ser movimentados para outras localizações logo que possível. As emissões dos PAR podem ser desligadas em sequência para reduzir a assinatura electrónica que emana da sua cobertura de área. A manobra defensiva pode ditar lanços rápidos dos meios do SUM. Durante movimentos de saída de áreas de empenhamento, meios do SIC-T que tenham sido retirados da rede, não deverão ser logo instalados e reintegrados na rede, e sim estar preparados para apoiar o contra-ataque. De um modo geral, os meios de comunicações do SIC-T deverão estar geograficamente dispersos, afastados de alvos remuneradores, sob cobertura natural, desenfiados e evitar eixos de aproximação e corredores aéreos inimigos. No entanto, as ligações de feixes hertzianos deverão apoiar-se em pontos dominantes. A cobertura SUM deve ser maximizada ao longo de corredores de movimento, itinerários de reabastecimento e itinerários de evacuação e outras áreas críticas.

(4) Operações de Estabilização

As operações com forças destacadas apresentam requisitos únicos ao nível da rede de comunicações táctica. O planeamento do apoio de Tm deve ser feito cuidadosamente, pois o apoio de comunicações e logístico local poderá não ser o mais adequado no teatro. Os planeadores de SIC terão que analisar a missão de modo a garantir que todas as necessidades da força projectada sejam suportadas pelos meios SIC adequados. O módulo de apoio de comunicações deverá conter o seu próprio volante logístico para garantir a operação continuada do sistema. O módulo RL do SIC-T será o meio ideal para ser projectado com uma Força a operar fora do território nacional e instalado junto ao PC

dessa Força, para garantir a ligação à retaguarda (território nacional), sendo normalmente instalado junto ao PC da Força apoiada (SAL).

O apoio a FNDs irá frequentemente requerer extensões nos meios de comunicação de médio e longo alcance. Relativamente a FNDs a operar num TO fora de Portugal, deverão ser consideradas para além das ligações típicas doutrinárias, a utilização da infra-estrutura local de comunicações e eventualmente de SICs civis. Esta solução no entanto, só deverá ser admissível quando a referida infra-estrutura apresentar condições adequadas, nomeadamente sobre a segurança da informação. É igualmente necessária a conectividade aos sistemas NATO. Os destacamentos de Tm das FND ficarão sob comando completo do CMDT da força. Antes da projecção da força, a célula de G3 deverá coordenar os seguintes pontos: relações de comando (ao nível da interligação de meios), apoio logístico dos meios de Tm, endereçamento IP, planos de numeração telefónica e DNS[65]. Ao nível dos Sistemas de informação, a Força deverá estar apta a operar quatro domínios de segurança de rede em simultâneo, com as seguintes classificações: UE/NATO SECRET, MISSION SECRET, SECRETO e Rede Administrativa. Os serviços disponibilizados nos diferentes domínios de rede são descritos no Apêndice 10.

[65] DNS: *Domain Name System*, um serviço de resolução de nomes de máquinas em endereços IP.

4. Conclusões

A gestão da informação é a pedra angular das operações militares modernas. Constatou-se que a estrutura de transmissões tácticas do Exército, que o SIC-T veio substituir, não possuía a capacidade de efectuar essa gestão da informação de uma forma eficaz, estando duplamente desactualizada. Por um lado estava dimensionada e doutrinada para apoiar apenas operações em cenários convencionais, direccionadas contra um inimigo bem definido, o Pacto de Varsóvia, num espaço de batalha contíguo. Por outro lado, estava assente igualmente numa plataforma tecnológica ultrapassada, de comutação de circuitos, e redes rádio VHF e HF, com uma separação bem definida entre voz e dados. Com o final Guerra da Fria, o 11 de Setembro, a revolução mundial ao nível das tecnologias da informação, os novos conceitos de operações centradas em rede e guerra da informação, a não contiguidade do espaço de batalha, e em consequência destes factos, com as novas missões em que o Exército se vê actualmente envolvido (tendo em particular atenção o carácter conjunto e combinado das mesmas), o SIC-T constitui-se como um elemento potenciador da acção de C2 no Exército.

Para abordar esta problemática o método adoptado foi do tipo hipotético-dedutivo, que pela investigação conduzida permitiu, dar resposta às questões derivadas, confirmar as hipóteses levantadas e assim responder à questão central*: A doutrina das transmissões de campanha no Exército Português altera-se substancialmente com a adopção do SIC-T?*

Constatou-se ao longo da investigação que os princípios orientadores da actuação das Transmissões necessitam de ser revistos. Verificou-se a alteração do paradigma de apoio de comunicações para o de apoio SIC; pois o enfoque deixou de estar centrado apenas no transporte da informação, estendendo-se a um conjunto muito mais abrangente de actividades relacionadas com a mesma. É evidente a necessidade de uma abordagem mais abrangente, tendo em vista a nova realidade de operações conjuntas e combinadas, e de operações de novos tipos. O SIC-T constitui-se sem dúvida como um *enabler* chave para o estabelecimento das operações centradas em rede no Exército, mas não o pode fazer isoladamente. Terá sim de se integrar totalmente com o SIC-E e os sistemas congéneres da Defesa, contribuindo para a implementação de uma infoestrutura que permita a introdução do conceito NNEC a nível nacional. Só assim será possível a obtenção de uma IOC que facilite a acção de C2.

Considera-se deste modo a hipótese 1 comprovada: *Com a introdução de novos sistemas, novas tecnologias e de princípios como a NCW e a GI, e a participação em Operações Conjuntas e Combinadas (OCC), o apoio de SIC no Exército passa a ser encarado de forma diferente da realidade actual, constituindo-se o novo SIC-T do Exército Português como um componente fundamental mas não único.*

Contrariamente à antiga estrutura de CCom de Área e CCom de Cmd, onde a delimitação do apoio de comunicações era bastante inflexível, com o SIC-T passou-se para uma estrutura modular, esta última inspirada no projecto TACOMS 2000. Este projecto, porém, apresenta na sua génese um paralelismo com o sistema norte-americano MSE. O SAL, com os seus módulos de NA, CCB e CCC disponibiliza uma grande variedade de serviços aos vários escalões de comando da Brigada e das unidades subordinadas, ao passo que o SUM estende esse acesso indiferenciado a todos os utilizadores móveis autorizados. A conjugação dos vários subsistemas do SIC-T permite a introdução de conceitos como QOS, portabilidade, preempção, etc., para além do que o funcionamento do SIC-T em modo *full* IP com uma boa largura de banda contribui enormemente para a flexibilização do apoio, oferecendo uma gama integrada de serviços de voz, vídeo e dados. Considerou-se que na generalidade, e devido ao paralelismo existente entre os dois sistemas, o apoio da componente de comunicações pode ser efectuado segundo os moldes do sistema MSE.

Ao nível da componente conjunta, embora estejam a ser dados os primeiros passos, ainda existe um longo caminho a percorrer. Porém, dada a plataforma tecnológica em que assenta o SIC-T, este possui todas as condições para uma rápida integração ao nível combinado e conjunto, desde que exista vontade para tal. De igual modo, o grau de autoridade controlo técnico necessita de ser revisto para se poder flexibilizar o apoio SIC. Destaque-se ainda a incipiente capacidade de utilização do segmento espacial do SIC-T. Constatou-se que as ligações via feixes hertzianos tendem a ser substituídas por ligações satélite, tal como acontece nas novas Brigadas *Stryker* norte-americanas.

Considera-se assim igualmente comprovada a segunda hipótese colocada, *Os componentes do SIC-T reflectem uma organização modular, muito diferente da anterior estrutura de Tm que preconizava um apoio mais estático assente em CCom de Comando e CCom de Área. Esta organização modular irá alterar a forma como é prestado o apoio de SIC nas operações militares, permitindo uma maior flexibilidade, e facilitando a integração com outros sistemas (combinados e conjuntos).*

Notou-se que a nova arquitectura de segurança para o SIC-T ainda está numa fase incipiente. Seguindo a filosofia do projecto TACOMS, o enfoque foi feito nas

componentes de redes e sistemas, estabelecendo-se que a componente de segurança seria implementada apenas quando as referidas componentes estivessem operacionais. A inexistência de normas técnicas (com excepção dos RADs) e de doutrina condicionam igualmente que os únicos aspectos de segurança actualmente presentes no SIC-T sejam os equipamentos de cifra IP TCE-621 e os encriptadores *bulk* acoplados aos sistemas de feixes hertzianos. A esta situação também não é alheia a falta de uma cultura de segurança generalizada nos SICs do Exército. Considera-se que o caminho mais adequado será a transposição das directivas NATO na área da INFOSEC para o SSR, uma vez que todas as áreas da segurança dos SIC estão já cobertas por publicações doutrinárias NATO. Os equipamentos actuais (*routers*, *firewalls*, IDS) têm a possibilidade de suportar as mais recentes políticas de segurança, embora actualmente não estejam activadas no SIC-T. Um outro problema encontra-se na própria TCE 621, um equipamento de cifra IP não muito flexível e que pode por em questão a própria evolução do SIC-T.

Dado o actual estado de implementação do SIC-T, considera-se como não provada a terceira hipótese levantada, *A nova arquitectura de segurança para o SIC-T reflecte as últimas inovações na área de segurança de redes integradas de voz, vídeo e dados.*

Face ao anteriormente exposto, reconhece-se que ***a doutrina das transmissões de campanha no Exército Português se altera substancialmente com a adopção do SIC-T.***

5. Bibliografia

Livros, Monografias e Teses

ALBERTS, David, GARSTKA, John, STEIN, Frederick (2000). *Network Centric Warfare. Developing and Leveraging Information Superiority*. EUA: CCRP Publication Series.

BLAKER, James R (2007). *Transforming Military Force: The Legacy of Arthur Cebrowski and Network Centric Warfare*. EUA: Praeger Publishers Inc., ISBN: 978-0275994273

BRAUNLINGER, T. (2005). *Network Centric Warfare Implementation.* Fort Leavenworth, Kansas: Faculty of the U.S. Army Command and General Staff College.

CARES, Jeffrey (2006). *Distributed Networked Operations: The Foundations of Network Centric Warfare*. EUA: iUniverse.com, ISBN: 978-0595378005

CISCO. (2006). *The Theatre Independent Tactical Army and Air Force Network (TITAAN) Solution*. EUA, Cisco Press, San Francisco 2006

GONZALES, Daniel, et. al. (2005) *Network Centric Operations (NCO) Case Study: The Stryker Brigade Combat Team*,EUA, RAND, National Defense Research Institute

GOODE, Rog, HALLINGSTAD, Geir (2007). *NNEC NII IP network encryption (NINE): scenarios, characteristics, and requirements 2007*. Brussels.

NUNES, Paulo (2003) – *A conflitualidade da informação: da Guerra de Informação à Estratégia da informação*. IAEM. Curso de Estado Maior, TILD CEM 2002-2004.

SILVA, Rui (2002) – *Contributos para o Sistema Táctico de Comunicações, para apoio ao Sistema de Forças Nacional*, Lisboa: Instituto de Estudos Superiores Militares, TILD CEM 2000-2002.

VICENTE, Paulo (2007). *Guerra em Rede. Portugal e a Transformação da NATO*. Lisboa: Prefácio. ISBN: 978-989-8022-58-5

Publicações

DCSI. (2006). *Anexo B (Enquadramento Conceptual e Estruturas Lógicas dos Módulos SIC-T) ao Retatório Final do "Projecto Inicial de Implementação do Sistema de Informação e Comunicações Táctico (SIC-T)*. Lisboa.

DST. (2003). *Projecto SIC Táctico*. Lisboa.

DST (2006). *Relatório final do projecto inicial de implementação do sistema de informação e comunicações táctico (SIC-T)*, Lisboa.

EME (2003). *RAD 280-1 Segurança da informação armazenada, processada ou transmitida nos Sistemas de Informação e Comunicação do Exército*. Lisboa:EME, 2003

EME (2005). *RAD 280-2 Orientações gerais de segurança para os Sistemas de Informação e Comunicação do Exército*. Lisboa:EME, 2005

EME (2006) *Plano de Médio e Longo Prazo do Exército (2005 – 2023)*. Lisboa: EME, 2005

EME (2007). *Informação Nº 457/ 2007- DivCSInfo: Elemento de Guerra de Informação, Lisboa*, 5 de Dezembro de 2007

EPT (2003). *Manual de Comunicações de Campanha*, Porto: Tecnologias Criativas

FM-11.43. (1999). *The signal leader's guide.* Washington: Headquarters,Department of the Army.

FM-11.55. (1999). *Mobile Subscriber Equipment (MSE) Operations.* Washington: Headquarters, Department of the Army.

FM-6.02.2. (2003). *Command, Control,Communications, and Computer(C4) Operations: Stryker Brigade.* Washington: Headquarters, Department of the Army.

FMI-6.02.50. (2005). *LandWarNet Operations in the Division and Brigade Units (INITIAL DRAFT).* Washington: Headquarters Department of the Army.

FM 100-6 (1996). *Information Operations*, de 27Ago1996. Washington: Headquarters Department of the Army.

IAEM (1987). *Noções gerais de transmissões* – ME2552 Lisboa: IAEM.

JP 6-0 (2006). *Joint Publication 6-0 - Joint Communications System*, EUA, 20 de Março de 2006

JP 6.02 (1996). *Joint publication 6-02 - Joint doctrine for employment of operational/tactical command, control, communications, and computer systems*, EUA, 1 de Outubro de 1996

JP 3-13 (2006). *Joint Publication 3-13 - Information Operations*, EUA, 13 de Fevereiro de 2006

NATO (2007a). AJP-01(C), *Allied Joint Doctrine*

NATO (2007b). AJP-3.10 *NATO Military Doctrine for Information Operations*

NC3A (2005). *NATO Network Enabled Capability Feasibility Study Executive Summary: Version 2.0,* Bruxelas: NATO, Outubro de 2005

NC3B (2005). *INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms.* Bruxelas, 2005

NC3B (2006a). *INFOSEC Technical and Implementation Guidance in Support of Public Key Infrastructure Cryptographic Aspects.* Bruxelas, 2006

NC3B (2006b). *Primary Directive on INFOSEC.* Bruxelas, 2006

NC3B (2006c). *INFOSEC Technical & Implementation Directive for the Interconnection of CIS*. Bruxelas, 2006

NC3B (2006d). *INFOSEC Management Directive for CIS.* Bruxelas, 2006

QOP CTmAp. (2005). *QOP Companhia de Transmissões de Apoio.* Lisboa.

QOP CTm BrigRR. (2006). *QOP Companhia de Transmissões da Brigada de Reacção Rápida*. Lisboa.

RC 130-1. (1987). *RC 130-1 Operações.* Lisboa: EME, Departamento de Operações.

RC-INFORMAÇÕES (2005). *Regulamento Campanha Informações,* Lisboa: IESM.

RC-OPERAÇÕES (2007). *Regulamento Campanha Operações,* Lisboa: IESM

Artigos em publicações periódicas

CARREIRA, Dario. (2002). *O Sistema Integrado de Comando e Controlo do Exército SICCE*. Jornal do Exército nº 516. Lisboa, Março de 2002

FERREIRA, Edorindo (2005) . *O Conceito de Network Centric Warfare. Implicações para a Transformação da Força Operacional do Exército*. Boletim de Formação Investigação e Doutrina Nº 62. IESM, Lisboa, Setembro de 2005

Monografias electrónicas

FAST, William (2002). *Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age.* [Em linha] [Consultado em 10 de Março de 2008] Disponível na www em: http://www.ndu.edu/inss/siws/ch1.html

VIEIRA, José (2007). CEM Exército 2007, AEEE, Enquadramento Doutrinário, 3ª Sessão, SIC & GE. Lisboa.

Sítios da Internet

GLOBALSECURITY. (2008a). *MSE* [Em linha] [Consultado em 25 de Janeiro de 2008]. Disponível na www em: http://www.globalsecurity.org/military/systems/ground/mse.htm.

GLOBALSECURITY. (2008b). *WIN-T*[Em linha] [Consultado em 31 de Janeiro de 2008]. Disponível na www em: http://www.globalsecurity.org/military/systems/ground/win-t.htm

MDN (2008). *Ministério da Defesa Nacional* [Em linha] [Consultado em 31 de Janeiro de 2008].http://antigo.mdn.gov.pt/Defesa/Estrutura/Organigrama/DGAED/oportunidades_estrategicas.htm

NC3TA (2008) *NATO C3 Technical Architecture* [Em linha] [Consultado em 1 de Março de 2008]. Disponível na www em: http://194.7.80.153/website/book.asp?menuid=15&vs=0&page=vol2%2Dsup1%2Fch01%2Ehtml

SCEE. (2008). *Sistema de Certificação Electrónica do Estado*. [Em linha] [Consultado em12 de Abril de 2008]. Disponível na www em:http://www.scee.gov.pt/ECEE/pt/proj_pki

TACOMS 2000 (2008). *TACOMS – Standard Federated Networking* [Em linha] [Consultado em 27 de Novembro de 2007] Disponível na www em: http://www.tacomspost2000.org/cms/index.php?option=com_content&task=view&id=41&Itemid=75

Entrevistas

FERREIRA, MGen Edorindo, Director de Comunicações e Sistemas de Informação do Estado Maior General das Forças Armadas. Entrevista efectuada em 01 de Abril de 2008,

PALHA, TCor TInf Luís, Adjunto da Repartição de Tecnologias e Sistemas de Informação da Divisão de Comunicações e Sistemas de Informação do Estado Maior General das Forças Armadas. Entrevista efectuada em 01 de Abril de 2008,

PASTOR, MGen José Quesada, General Director de Comunicações e Sistemas de Informação do Exército. Entrevista efectuada em 22 de Fevereiro de 2008

SACRAMENTO, TCor Tm António, Chefe da Repartição de Segurança da Informação da Divisão de Comunicações e Sistemas de Informação. Entrevista efectuada em 22 de Fevereiro de 2008

SILVA, TCor Tm Rui Manuel Marques da, Chefe da Repartição de Sistemas de Comando e Controlo da Divisão de Comunicações e Sistemas de Informação. Entrevista efectuada em 4 de Abril de 2008.

APÊNDICE 1 – ENTREVISTAS REALIZADAS

Com o objectivo de complementar a investigação realizada para a elaboração deste trabalho, procedeu-se a um conjunto de entrevistas a entidades com responsabilidades na área das Comunicações e Sistemas de Informação.

Entrevista nº1

Realizada em 01 de Abril de 2008, ao Director de Comunicações e Sistemas de Informação do Estado Maior General das Forças Armadas, MGen Edorindo Ferreira.

Meu General,

Qual é a visão (se existe) das Forças Armadas relativamente à implementação do NNEC?

Ainda não há visão nenhuma. Presumo que irá haver… pelo menos julgo que seria bom que houvesse, mas a transformação por que passa neste momento a estrutura da defesa e das forças armadas não é propícia a que se defina já essa visão.

O meu general está assim a dizer que não existem directivas, orientações e objectivos…

Não, de facto não existem, pelo menos de uma forma sistematizada.

O modelo de transformação das Forças Armadas prevê esta capacidade?

Prevê-se a criação de uma divisão do EMGFA com um órgão que vá trabalhar todos os assuntos da transformação. Não está definido se esse órgão também vai tratar o assunto da transformação das comunicações, se bem que nós aqui na DICSI temos previsto uma «alineazinha», a qual diz que existirá uma repartição da DICSI que trabalhará assuntos da transformação exclusivamente no âmbito dos SIC. Mas nada disso é garantido: entretanto os estudos continuam, temos feito apresentações ao Gen CEMGFA, mas nada está decidido. E mesmo depois de nós decidirmos, nada nos diz que venha a ser assim,

porque se afigura que o Ministério da Defesa pretende criar uma estrutura definidora, orientadora de tudo o que é política de SIC para a defesa, nos âmbitos táctico, operacional e estratégico.

Eliminado: porque

Eliminado: quer

Quais os programas actuais e futuros que concorrem para esta capacidade?

Actualmente os que estão a decorrer incluem o MMHS (o qual está meio parado, como sabe), estamos a envidar grandes esforços no âmbito do *Information Exchange Gateway* (IEG) e estamos também a trabalhar no IPv6 e em projectos que têm a ver com a INFOSEC.

Quais as dificuldades e desafios que enfrenta (ramos e conjunto)?

A grande dificuldade é a ausência de espírito conjunto. O conceito de conjunto ainda não entrou na mente das pessoas. Para mim a grande dificuldade de implantação do conceito NNEC em Portugal tem mais a ver com mentalidades do que com tecnologia.

Qual o nível de ambição para a componente operacional?

Ainda não está nada definido.

Que participação Portugal tem ao nível do projecto NNEC? É uma participação activa? Existe um acompanhamento? E com que objectivos?

Tem. Neste momento quem está apenas a acompanhar esse projecto é a DICSI/EMGFA. A nível do Ministério, da DGAED e da DGIE, ninguém participa em nada. A DICSI participa nas reuniões. Há anualmente um simpósio sobre NNEC. Este ano vai ser na Turquia, em Maio, e vão estar presentes dois oficiais da DICSI, apesar de eu também ter sido convidado nominalmente. Houve um convite aos representantes do NC3 Board, do qual eu sou o representante nacional, mas devido a outros compromissos não posso estar presente. Estamos a tentar que vá também o NC3 Rep que está na DELNATO.

Eliminado: m

Eliminado: director

Eliminado: DelNATO

A participação nesse simpósio é apenas para ver qual é o estado da arte actual? Ou é já para começar a preparar o conceito nacional?

Antes de cada um desses seminários são-nos feitas perguntas para saber o ponto de situação em que estamos, ao nível de capacidades. Ao próprio nível de capacidades a NATO faz uma vez por ano uma visita aos países para ver o estado dessas capacidades. Já há uma resposta nacional relativamente a essas perguntas…genérica…Se quiser saber mais detalhes sobre essa resposta, fale com o TCor Palha, que desde há vários anos tem sido o coordenador deste assunto

As indústrias de defesa estão envolvidas? A que nível?

Não.

Existe documentação publicada ou em rascunho por parte da DICSI ou de outra entidade nacional?

Não.

Tem existido acompanhamento por parte do EMGFA nos projectos SIC-T e SICCE?

Não tem havido.

Não tem sido testada interoperabilidade?

O EMGFA tem participado unicamente na disponibilização de fundos para deslocação ao estrangeiro das equipas envolvidas em exercícios e workshops. Mais nada…No próximo exercício LUSÍADA em Novembro vamos procurar testar. Estamos a estudar nesse sentido, para aí sim fazer o teste desses sistemas.

Temos pessoal com experiência prática na área de operações centradas em rede?

Não temos em Portugal ninguém.

Qual o grau de interoperabilidade dos sistemas de C2 dos ramos? No caso do Exército temos o SICCE. Tem sido testado? Quero dizer, ao nível conjunto funcionamos minimamente?

Não. Não há conjunto, nem táctico nem operacional. Existe interligação básica ao nível das redes informáticas administrativas (intranets, SIG). Na NATO é curioso que enquanto ao nível naval o MCCIS está perfeitamente testado e é interoperável, no domínio terrestre, ainda não existe um STANAG, apesar de o SICCE e os outros sistemas nacionais NATO efectuarem estudos conjuntos. E se a NATO não tem, nós estamos mais atrasados ainda. Só prevejo que a interoperabilidade seja viável quando forem criadas condições com a nova estrutura organizativa das forças armadas

Eliminado: s

Ou seja, basicamente esvaziando os ramos de competências e concentrando no EMGFA?

Exactamente. Mas eu não sei se isso é possível.

A NNEC ainda não tem definido a nível NATO um modelo de aplicação, quem vai gerir, quem vai determinar o que é que se faz. Está em fase final de aprovação. O NC3 Board já o deveria ter aprovado na reunião anterior, não o aprovou. Espera-se que tal aconteça na reunião de Maio, que sejam definidas as linhas orientadoras, a doutrina para a NNEC. E aí serão dadas directivas específicas às nações. A partir daí é que nós temos que ver o que temos de fazer exactamente. Agora são coisas desgarradas. A partir de Maio espera-se que haja uma publicação com orientações concretas.

Para a elaboração deste trabalho, recorreu-se à consulta dos últimos FMs de comunicações Norte Americanos relativos às Brigadas Stryker, dado que a doutrina NATO está mais atrasada nesse aspecto. Nota-se que os EUA estão a apostar cada vez mais nas comunicações satélite tácticas. Portugal, especificamente o Exército tem a possibilidade de alguma vez, pelo menos através da NATO, utilizar o segmento

espacial? Ou vamos ficar condenados a ter apenas as ligações *rear-link*, como existem actualmente para as FND?

Neste momento estou à espera de uma resposta da NATO para a utilização da estação satélite da Fonte da Telha pelas FAs Portuguesas. Se a resposta for afirmativa temos a possibilidade de utilizar comunicações do sistema satélite da NATO. Não sei se a resposta vai ser afirmativa. Mas você está mais a falar ao nível táctico, correcto? Ao nível táctico é muito complicado. A própria NATO está a abandonar o seu sistema satélite que já tem alguns anos. A NATO está progressivamente a utilizar sistemas dos países membros: Um exemplo é o da empresa inglesa Paradigm, com capitais do Ministério da Defesa, que nós também estamos a utilizar.

Eliminado: yme

Eliminado: com capitais do Ministério da Defesa.

Mas nós pagamos para utilizar esses *links*?

Claro! E no caso dos satélites NATO possivelmente teremos de pagar também. Mas aqui estamos ao nível operacional. Ao nível táctico os EUA têm a Terra envolvida em redes satélite *Low Earth Orbit* (LEO)[66] e *Medium Earth Orbit* (MEO)[67]. Nós não temos nada disso. Outra coisa que eles têm com fartura e nós não, são UAVs. Toda a gente os tem, só nós não, e eu considero-os imprescindíveis ao nível táctico. Mas ainda ao nível dos satélites: a NATO utiliza também o sistema espanhol. O próprio CEMGFA espanhol esteve cá há pouco tempo e ofereceu o sistema deles para nossa utilização. Mas para tal, era necessária uma decisão política favorável, o que me parece difícil. E depois, a oferta foi feita, mas a utilização não seria grátis. Há países que estão a utilizar o sistema espanhol, mas pagam pela utilização. A Holanda, por outro lado, paga para utilizar o sistema francês. Mas não tenha dúvidas, o futuro está no satélite.

[66] Órbitas a altitudes compreendidas entre os 160 e os 2000 km.
[67] Órbitas a altitudes compreendidas entre os 2000 e os 35.786 km.

Entrevista nº2

Realizada em 22 de Fevereiro de 2008, ao Chefe da Repartição de Segurança da Informação da Divisão de Comunicações e Sistemas de Informação, TCor Tm António Sacramento.

Meu Tenente Coronel,

Qual é o estado actual das comunicações tácticas no Exército Português?

Temos que analisar essa situação conceptual e tecnologicamente. Ao nível do conceito estrutural penso que as companhias existentes respondem às necessidades operacionais do actual dispositivo. Ao nível dos equipamentos tirando os destacamentos existentes nas FNDs, o material está obsoleto, tendo em conta a realidade tecnológica actual. As comunicações de campanha CNR necessitam urgentemente da entrada em funcionamento do 525. É desejável que a sua distribuição ao Exército não demore muito mais tempo, pois os estudos deste projecto já começaram há cerca de doze anos…

Tem existido coordenação com o EMGFA/MDN ou com outros Ramos das FA no desenvolvimento de doutrina, procedimentos e técnicas comuns na área das comunicações aos níveis operacional e táctico?

Existe uma grande lacuna ao nível da doutrina de CSI no nosso Exército. Tem que haver naturalmente uma interoperabilidade conjunta. O que tem acontecido nos últimos anos durante a conduta dos exercícios conjuntos é uma notória falta de compatibilidade ao nível dos meios e procedimentos dos ramos. Ao nível da INFOSEC, a área de responsabilidade da minha repartição, foi criado o Grupo de Coordenação INFOSEC das FAs. A ideia por detrás deste grupo é justamente criar doutrina conjunta e estabelecer requisitos ao nível da INFOSEC. Actualmente estamos a trabalhar na estrutura CERT[68] das forças armadas, nomeadamente resposta a ataques informáticos, bem como a estrutura de segurança nas interligações entre redes dos ramos. Este grupo de trabalho funciona sob a direcção da DICSI/EMGFA. Outro projecto é o do MMHS que tem conhecido ultimamente uma maior implantação no Exército, embora tal tenha ocorrido muito depois da implementação deste sistema na Marinha e Força Aérea.

[68] Computer Emergency Response Team

No que diz respeito à doutrina, faço uma crítica. No Exército existem várias entidades que podem criar doutrina. De acordo com o quadro orgânico, missão e possibilidades, a DCSI não pode fazer doutrina, nem regulamentar doutrinariamente o funcionamento das comunicações. No entanto considero que é relativamente fácil defender que as directivas técnicas emanem desta Direcção. A questão é onde termina o âmbito de uma directiva técnica e começa o da doutrina. Pessoalmente, gostaria de "esticar", de alguma forma esse âmbito, pois na minha área de trabalho, a segurança da informação, está muita coisa por fazer.

No Programa de Médio e Longo Prazo do Exército, uma das capacidades em destaque é a Capacidade de Comando, Controlo e Comunicações. Citando O Objectivo Principal EC01/OC/001/05:

Dotar de forma gradual e numa perspectiva modular, até 2024, a Componente Operacional do SFN-Ex com um Sistema de Comando e Controlo Táctico adequado ao desempenho das suas missões específicas, em conformidade com os requisitos necessários no contexto NATO e em interligação com um Sistema de Comando e Controlo Estratégico que venha a ser desenvolvido. Para o efeito adoptar de forma progressiva, até final de 2024, na Componente Operacional do SFN-Ex, o conceito de Network Centric Warfare (NCW), através do incremento da interoperabilidade e da integração dos meios numa rede única sobre uma infra-estrutura tecnologicamente avançada.

Qual o estado actual da doutrina, procedimentos e técnicas existentes no Exército referentes a esta nova realidade?

Sobre a doutrina, desconheço. O actual Gen CEME promulgou a directiva 90/2007, onde apontou como sua preocupação o problema da Guerra da Informação. Foi feito um estudo pela DivCSinfo/EME, e sobre um draft desse estudo foi pedida opinião a esta direcção, que enviou os seus contributos. A NATO já evoluiu do conceito de segurança de informação para o de information assurance. Não o traduzo para "acreditação da informação" ou "certificação da informação" porque ainda não existe uma tradução oficial.

Essa é uma das dificuldades com que nos deparámos: a quantidade de conceitos doutrinários escritos em inglês e que não estão traduzidos para português…

Mesmo os que estão traduzidos, às vezes não o estão correctamente. Se lermos os RAD 180-1 e 180-2 (aprovados em 08Jan02 e 19Mai05, respectivamente, e elaborados pela então designada DCSI/EME), referem-se aos sistemas de informação e comunicação, mas também se referem algumas vezes aos sistemas de comunicação e sistemas de informação, embora depois tenhamos uma Divisão e uma Direcção de Comunicações e Sistemas de Informação.

No âmbito deste trabalho empregamos a sigla SIC, Sistemas de Informação e Comunicações.

Não concordo com essa designação (sistemas de informação e comunicação). Penso que o termo mais correcto seria CSI (comunicações e sistemas de informação), ou SIC (sistemas de informação e comunicações) na medida em que a sigla SIC tem origem na tradução da terminologia da língua inglesa *CIS (Communications and Information Systems).* Mas enfim, está feito. Por isso é que digo que deveriam ser frequentados cursos nesta área sob a égide da escola de comunicações NATO de Latina. Desapareceria da cabeça de muita gente as indefinições ligadas a estes conceitos. Isto porque a nossa referência deve ser a NATO e não os EUA.

A sua repartição foi envolvida na arquitectura de segurança para o SIC-T?

Não. O que o SIC-T e o SICCE têm solicitado de INFOSEC a esta repartição resume-se às TCEs.

O conceito de segurança para mim é transversal a todos os sistemas, seja o SIC-T ou o SIC-E. Se estamos a trabalhar para a constituição de uma rede de redes, uma falha de segurança num dos sistemas pode afectar o outro…

Vou-te responder baseado numa palestra a que assisti há algumas semanas, ~~e~~ em que o conferencista era o Prof. Paulo Veríssimo, um dos maiores especialistas nacionais em *information assurance*. Um dos temas que ele abordou foi o *security roadmap*: para as empresas que vendem segurança da informação, o melhor cliente que existe é aquele que paga a tempo, tem dinheiro e não sabe o que quer. São adquiridas *firewalls*, *software* antivírus, sistemas de detecção de intrusão, e no final possui-se um sistema topo de gama. Mas esquecemo-nos da componente humana e de todos os procedimentos que têm de ser implementados e regulamentados para instruir e controlar esse elemento, que é de longe o

mais importante. O que nos interessa ter um bom sistema se o pessoal que o opera não tem formação para tirar capacidade dele? A TCE não resolve tudo…

Está aprovada uma estrutura PKI comum à defesa?

Foi criada uma estrutura PKI para o Estado. A raiz central desse sistema vai ser instalada numa cave da Casa da Moeda, e a partir daí serão distribuídas chaves para todos os serviços e aplicações do Estado. O Grupo de Coordenação INFOSEC das FAs liderado pela DICSI/EMGFA avançou com o processo de criar a estrutura de chaves para as FAs. No entanto quem certifica essa estrutura é o Gabinete Nacional de Segurança (GNS), e como tal a proposta teve de passar pela Secretaria-geral do Ministério da Defesa. O ministério chamou então a si este processo e está a desenvolver novos estudos, para ser constituída uma estrutura de chaves para a Defesa e não só das FAs, mas penso que estamos no bom caminho.

Entrevista nº3

Realizada em 22 de Fevereiro de 2008, ao General Director de Comunicações e Sistemas de Informação do Exército, MGen José Quesada Pastor.

Meu General,

Qual é o estado actual das comunicações tácticas no Exército Português?

Essa pergunta se calhar acaba por resumir todas as outras. Vamos situar as coisas aos vários planos. O produto operacional do Exército são três brigadas, que conforme indicado no SFN podem ser empregues uma no seu todo, ou podem projectar uma UEB cada uma. As três brigadas têm cada uma uma companhia de Transmissões (CTm) que assegura a capacidade de C2 da Brigada. No caso do BrigInt, a CTm não é residente, estando localizada na EPT. No entanto, a obsolescência do material de Tm, nomeadamente o da BrigMec atinge proporções alarmantes. Por outro lado a BRR não dispõe de todos os meios que deveria ter. De uma forma geral há problemas de equipamentos em todas elas.

Mas o material existente em todas as CTm não está completamente ultrapassado?

Como sabe foi desenvolvido o projecto SIC-T. Este programa é uma arquitectura que está bem definida e bem estudada, e ao que me parece do que temos visto e comparado com outros exércitos, do mais moderno que existe. O que acontece é que os meios de comunicações são caros e são investimentos complexos. Porquê? Porque se por um lado não há verba para se comprarem todos de uma só vez, por outro lado eles tendem sempre a ficar desactualizados. Ou seja, isto corresponde a um investimento permanente, porque hoje compra-se um sistema topo de gama, mas o prazo de obsolescência dos materiais é hoje muito mais pequeno do que era antigamente. Apesar de tudo, o SIC-T baseia-se num rádio de combate do mais moderno que existe, cujo contrato está aparentemente a correr bem. Esse rádio está a ser fornecido por lotes que foram estendidos até 2017, data que eu pessoalmente considero comprida demais…receio que quando recebermos os últimos, eles já estejam desactualizados.

O SIC-T baseia-se igualmente em nós de comunicações adaptados ao nosso sistema de forças. É claro que as algumas das verbas da LPM destinadas ao C2 têm sido desviadas para a aquisição de outros meios como VBR. Bem, não bem desviadas, mas com as

cativações de 40% das verbas efectuadas pelo governo e a consequente redistribuição da verba remanescente, as verbas que aparentemente seriam razoáveis e boas demonstram ser exíguas. Neste momento estamos a fazer o mínimo para o projecto não morrer. Esse mínimo corresponde a números da ordem de grandeza de um, dois, no máximo três milhões de euros no triénio 2007-2009 e têm sido feitas aquisições que permitiram fazer viaturas protótipo de módulos de comunicações de combate: nó de companhia, nó de acesso, etc. O sistema é um sistema duplo que possui nós de comando e nós de acesso, gizando uma espécie de grandes correios, grandes sistemas de comunicações em campo de batalha. Já produzimos alguns protótipos, que têm sido testados a nível nacional (e pretendemos entrar num grande exercício nacional, tipo ORION). Têm sido testados na série de Exercícios Internacionais Combined Endeavor com sucesso. Temos pois a garantia de que o protótipo desenvolvido é bom e que funciona. Agora interessa adquiri-lo. É uma questão mais de quantidade do que de engenharia. Depois de feito, testado e aprovado um protótipo, a questão é apenas produzi-lo desde que haja verba para tal efeito.

Resumidamente, o estado das comunicações tácticas é adequado à estrutura de forças do Exército. É no entanto necessário modernizar os equipamentos e os procedimentos de Tm nas brigadas. O esforço do SIC-T está a ter um andamento mínimo para o projecto não morrer.

Tem existido coordenação com o EMGFA/MDN ou com outros Ramos das FA no desenvolvimento de doutrina, procedimentos e técnicas comuns na área das comunicações aos níveis operacional e táctico?

Pode-se dizer que sim. Juntaria aí ainda o nível estratégico, considerando aí as comunicações permanentes. Toda a cadeia de C2 do Exército está assente sobre a rede permanente e tem havido alguma cooperação. Hoje em dia é já muito difícil distinguir entre o SITEPE e o SICOM. A atitude desta direcção tem sido uma de grande colaboração com o EMGFA, nomeadamente na parte da rede estratégica. Existem actualmente vários *links* utilizados pelo SITEPE que pertencem ao SICOM. Eu pessoalmente não tenho dúvidas de que dentro de algum tempo todos os grandes sistemas de comunicações terão tendência a repousar em escalões cada vez mais altos. Mas até lá, até tal ser uniformizado e proporcional a cada um dos ramos, o Exército deve manter a sua autonomia nas redes de voz e de dados. Deve manter essa autonomia enquanto não houver um sistema da Defesa que dê garantias a todos os ramos. Dou-lhe o exemplo do *rear link* para o Líbano, que é da responsabilidade do EMGFA, mas que foi montado por pessoal do Exército. Existe uma

tentativa de racionalização de recursos. Também tenho de mencionar a extinção do CIE. Com a sua extinção foram mantidas no Exército as aplicações primárias que são do interesse exclusivo do Exército: pessoal, apoio aos utilizadores e serviços básicos de rede. Todas as outras grandes aplicações ficaram no Centro de Dados da Defesa. Da parte do Exército existe vontade de cooperar com um "super sistema", se bem que existem serviços do próprio ramo que por agora devem continuar a ser geridos pelo Exército.

Se o meu General me permite, derivou um pouco demais para a parte estratégica. Gostaria de saber o que acontece nas componentes táctica e operacional, nomeadamente cooperação em exercícios, como o *Linked Seas* ou o Lusíada? Tem havido cooperação? Existe documentação escrita?

Há alguma colaboração, muito pouca documentação.

Eu falo por experiência própria. Como o meu General sabe, estive nos últimos anos envolvido em muitos exercícios, bem como no estabelecimento de todas comunicações *rear link* com as FNDs. Na prática, a colaboração do EMGFA resumiu-se ao aluguer das ligações satélite. Todo o resto foi feito e configurado por nós… Mas o problema é que cada vez que é necessário montar um *rear link* ou apoiar um exercício começamos do zero.

Mas como sabe, no programa do SIC-T está proposto um módulo de *rear link*, em proposta na LPM já para 2008. No caso do Líbano, foi uma decisão que nos apanhou de surpresa. Necessitamos dessa capacidade, quando mais não seja, para que quando for necessário empenhar uma força no Darfur ou noutro teatro, não sejamos apanhados desprevenidos.

Ainda relativamente aos *rear link*, considero importante a reactivação da rede HF para servir de backup aos *rear links*, bem como de rede de último recurso no território nacional. O HF, quando tudo falha, quando falham satélites, quando falha o recurso a operadores civis, garante a ligação. Não têm de ser os rádio-amadores, tem que ser o Exército a garantir a componente de último recurso. Essa componente tem de funcionar mesmo em tempo de paz…com mensagens injectadas, com algum apoio aos sistemas mais modernos, que são naturalmente mais eficazes. É uma prioridade que não tem sido possível implementar dada a escassez de recursos. Ao nível táctico propriamente não creio que o problema se ponha, pois tirando pequenas operações, são de facto operações do ramo…raramente são operações conjuntas. Ao nível dos exercícios as coisas conseguem-se

resolver, mas uma doutrina nacional conjunta não existe. Talvez a criação do Comando Operacional Conjunto venha a contribuir para a resolução desse problema.

Do estudo que tenho feito da doutrina NATO e dos EUA, pese embora a escala das respectivas FAs em relação à realidade nacional, não difere muito do que pretende fazer o SIC-T. A grande diferença é o esforço relativo à integração das várias componentes (marítima, terrestre e aérea), o que não me parece que aconteça no caso nacional…

Esse esforço é feito sobretudo a nível dos exercícios… que é verdade são escassos e insuficientes para criar doutrina. As Zonas Militares são talvez as entidades que mais trabalham nesse sentido, pois estão ligadas aos Comandos Operacionais e pela própria defesa do triângulo estratégico. Aí há de facto uma necessidade maior de integração. Agora doutrina não há.

Se me permite uma pergunta politicamente incorrecta, porque não há capacidade ou porque não há vontade?

Só lhe posso responder por mim. Por mim há toda a vontade, mas isso tem que ser centralizado no EMGFA. Devo-lhe dizer que nós vamos e participamos como entidade responsável no Exército pelos SIC em todos os grupos de trabalho e em todas as reuniões que são feitas a nível do EMGFA. O COp de quem nós dependemos é autoridade técnica para todos os assuntos dos SIC e a respectiva segurança, que é algo que é importante referir também.

No Programa de Médio e Longo Prazo do Exército, uma das capacidades em destaque é a Capacidade de Comando, Controlo e Comunicações. Citando O Objectivo Principal EC01/OC/001/05:

Dotar de forma gradual e numa perspectiva modular, até 2024, a Componente Operacional do SFN-Ex com um Sistema de Comando e Controlo Táctico adequado ao desempenho das suas missões específicas, em conformidade com os requisitos necessários no contexto NATO e em interligação com um Sistema de Comando e Controlo Estratégico que venha a ser desenvolvido. Para o efeito adoptar de forma progressiva, até final de 2024, na Componente Operacional do SFN-Ex, o conceito de Network Centric Warfare (NCW), através do incremento da interoperabilidade e da

integração dos meios numa rede única sobre uma infra-estrutura tecnologicamente avançada.

Qual o estado actual da doutrina, procedimentos e técnicas existentes no Exército referentes a esta nova realidade? Se me permite desde já a minha opinião, eu tenho a impressão que existe muito pouco…

Começo por fazer uma afirmação de La Palisse: para existirem operações centradas em rede, tem de haver rede. Essa rede tem que existir, ter coerência lógica, e tem de ser sustentada e mantida. No momento em que nós estamos, o razoável é garantir o bom funcionamento da rede, porque sem rede não há operações centradas na rede. Quando se fala em NCW, que é de resto um esboço doutrinário ainda não consolidado mesmo por parte das nossas fontes de doutrina (NATO, EUA), também não se fala de operações avulsas. Uma das operações centradas na rede que me parece de primordial importância é a segurança da própria rede. Assim sendo a prioridade é a sustentação da rede, uma rede que permita voz e dados e o apoio ao C2 do Exército, e por extensão das FAs. A seguinte é a segurança da própria rede transversal aos patamares estratégicos, operacional e táctico. Sabemos as potenciais vulnerabilidades que uma rede introduz nas operações.

Depois de ter a rede segura, então começar a pensar em operações centradas na rede. Mas ainda estamos longe de criar essa rede. Temos uma rede que nós chamamos tradicionalmente permanente, e que está em funcionamento. Temos uma rede táctica desenhada para cada operação, a ser operada por destacamentos de Tm nos vários teatros de operações.

Se o meu General me permite uma pergunta mais incisiva, nós estamos à espera de indicações do EMGFA para nós começarmos a trabalhar, ou existe pelo contrário a intenção de nós fazermos alguma coisa e apresentarmos propostas ao EMGFA?

Não existe a intenção, não está na nossa missão e não temos capacidade para tal. Nós somos um órgão muito virado para a execução, muito virado para a resolução de problemas a curto prazo. A sustentação da rede, o apoio às FNDs, a manutenção dos sistemas preenchem grande parte quer das nossas tarefas de missão quer do nosso tempo: Não estamos muito vocacionados para o que você perguntou. Mas temos a abertura para colaborar.

Quais são os novos conceitos de apoio de Transmissões (SIC) introduzidos pelo SIC- T?

Primeiro um conceito integrado. Tradicionalmente existia um sistema de Tm de comando e um sistema de Tm de área, os quais eram disjuntos. No Exército Português, sempre pusemos a tónica no sistema de Tm de Comando. Agora esses sistemas estão integrados. Se estivesse a falar para um leigo, diria que existe uma *internet* no campo de batalha, onde todos os combatentes se ligam de acordo com as suas permissões de acesso.

Como deverá ser efectuado o emprego táctico das Tm (SIC) em operações militares convencionais? Antigamente tínhamos linhas de orientação bem definidas. Por exemplo, para uma operação defensiva utilizávamos meios filares, alinhávamos os *links* de feixes hertzianos paralelamente à OAZR, etc. Com os novos conceitos introduzidos pelo SIC-T faz ainda sentido estarmos a detalhar o tipo de apoio de procedimentos para os vários tipos de operações? Há conceitos que se mantêm? O apoio é basicamente o mesmo com algumas pequenas variantes?

A ideia que eu tenho acerca desse assunto também é pessoal. As operações convencionais são o farol, e o nosso apoio de SIC deve estar focado nesse tipo de operações. Se nos prepararmos para esse tipo de operações, também depressa estamos capacitados para actuar em operações do tipo CRO, que são normalmente muito menos exigentes em termos de capacidades e recursos.

Mas com esta nova arquitectura considera que a doutrina escrita para o apoio de Tm se mantém ou é alterado? O manual mais recente é o IAEM e tem a data de 1987, se não contarmos com algumas publicações da EPT mais vocacionadas para subalternos e capitães…

Sim mas os órgãos produtores de doutrina são o Comando de Instrução e Doutrina e o Instituto de Estudos Superiores Militares. Nós não temos doutrina nova, mas temos ideias, conceitos, que não estão porém sistematizados. Esta é a verdade. O que existe é em termos do SIC-T. Ou seja, na definição da arquitectura do sistema, que como pressuposto tem uma doutrina de emprego de meios.

Entrevista nº4

Realizada em 4 de Abril de 2008, ao Chefe da Repartição de Sistemas de Comando e Controlo da Divisão de Comunicações e Sistemas de Informação, TCor Tm Rui Manuel Marques da Silva.

Meu Tenente Coronel,

No estudo que fiz das brigadas Stryker do exército dos EUA, constatei que se substitui grandemente as ligações de feixes hertzianos por *links* TACSAT multicanal. A nível nacional, não temos obviamente possibilidade de enveredar por esse caminho. Mas na minha entrevista ao MGen Edorindo Ferreira, director da DCSI/EMGFA, ele falou-me na possibilidade de se utilizarem satélites NATO. Pode-me dizer se existe algo pensado ao nível do Exército neste campo?

Podemos dividir a tua questão em três! Relativamente à capacidade TACSAT, começamos a sentir esta necessidade há cerca de três anos com elementos das Operações Especiais. A participação desta força em operações de âmbito internacional, permitiu-lhes o contacto com camaradas de outras nações que trabalhavam justamente com esse tipo de equipamentos, os quais possuem capacidade de transmissão de dados e de voz sem dificuldades e sem interferências, por não estarem sujeitos às características do terreno.

A FND presente no Afeganistão começou igualmente a aperceber-se das vantagens deste tipo de capacidade que todos os outros contingentes já disponham, estando também a nossa força equipada com um ou dois equipamentos deste tipo cedidos pelo escalão superior. Esta força começou repetidamente, a mencionar nos seus relatórios administrativos a necessidade de ser equipada com mais equipamentos deste tipo. Foi nesta altura que foi proposto superiormente a aquisição de equipamentos com estas características, proposta que ainda aguarda decisão superior.

Mas essa solução é uma extensão ao conceito SIC-T? Eu tinha a ideia que a única capacidade satélite do SIC-T estava concentrada no módulo *rear-link*?

Tens razão, mas atenção: os módulos do SIC-T estão desenhados para fazer uma cobertura de área e apoiar os PC até ao escalão companhia e este tipo de equipamento é normalmente utilizado nos escalões mais baixos, portanto ao nível MS (*Mobile System*), ou seja, ao nível do CNR onde se insere o equipamento rádio GRC-525. Os relatórios da FND propõem a aquisição do PRC-117 igual ao que tem sido cedido pelo escalão superior, um

rádio da firma Harris. A FAP comprou dois ou três equipamentos deste tipo, que levou para o Afeganistão. Porém, quando chegaram ao Afeganistão não tinham licenças para poder utilizar o satélite TACSAT que foi disponibilizado. Ou seja, isto é sempre um pau de dois bicos. É necessário ter o equipamento, mas é igualmente necessária a devida autorização para, em cada operação podermos utilizar o satélite que disponibiliza esta capacidade.

Estamos a falar ao nível da CNR apenas?

Sim, mas o TACSAT no SIC-T é fundamentalmente a este nível que o podemos utilizar.

TACSAT multicanal como os EUA têm para interligar COTs é algo inexistente?

Completamente, pelo menos desconheço que os EUA disponibilizem essa capacidade satélite a países aliados. O que todas as outras nações têm é o que temos vindo a falar, com larguras de banda inferiores a 64 kBit/s. A nossa proposta para integrar esta capacidade, envolve também o GRC-525 que sendo o nosso CNR, faria todo o sentido que tivesse esta capacidade. Contactámos a firma Rohde & Schwarz para que disponibilizasse um módulo extra no 525, de comunicação satélite UHF. Foi-nos respondido que não era rentável dado o número de equipamentos que nós iríamos comprar com essas funcionalidades, e por nenhum outro país ter feito um pedido semelhante. Ficámos na contingência de ter de comprar outro rádio do mesmo tipo do 525! No entanto a nossa proposta assenta numa análise de mercado onde encontrámos outros rádios nomeadamente do tipo *hand-held*, semelhante ao nosso 501, e que possui esta capacidade TACSAT, podendo ser acoplado em montagens veiculares, o que lhe permite ter uma maior potência disponível. É um rádio que não tem a utilização táctica do 525, e que permite colmatar uma lacuna que temos, a falta de um rádio hand-held, pois o 501 não satisfaz minimamente, porque não tem capacidade de transmissão de dados.

A nossa proposta para aquisição deste tipo de equipamento contempla também o desenvolvimento de um *gateway* entre a família 525 e um rádio TACSAT. Ou seja posso ter uma rede de rádios 525, e aceder com este equipamento ao segmento espacial através de um outro rádio TACSAT. Se quisermos dispor de capacidade TACSAT com o 525 terá de ser através deste *gateway*.

Relativamente à capacidade satélite do tipo VSAT, aquela que está disponível no módulo *rear-link* do SIC-T, como tinhas falado a situação está longe de estar normalizada. Temos visto várias propostas, mas uma apresentada por uma firma israelita foi a mais interessante. Consiste na aquisição de uma única *ground-station* (a localizar no EMGFA) aonde todas as forças destacadas se ligam, sem haver necessidade de estabelecimento de *rear-links* ponto-a-ponto como temos actualmente com as nossas FNDs.

De qualquer forma, o módulo *rear-link* que se está a produzir no SIC-T tem sempre esta capacidade de interligação via satélite à qual chamamos SATCOM, com larguras de banda que podem ir até aos 2 Mbps, portanto trata-se de uma capacidade diferente da TACSAT que tínhamos vindo a falar anteriormente. Os equipamentos SATCOM do *rear-link* foram especificados para trabalhar na banda X e na banda K_U. Quando participarmos em operações com satélites disponibilizados pela NATO podermos usufruir da capacidade, SATCOM na banda X, quando isso não acontecer poderemos alugar um segmento espacial em satélites comerciais e utilizar a banda K_U. O módulo *rear-link* pode ter uma utilização bastante diversificada, e falando apenas da sua capacidade SATCOM, ela pode ser disponibilizada junto a PC de Brigada, Batalhão ou até mesmo num local onde ocorra uma situação de catástrofe ou calamidade.

Agora aquilo que estudaste dos EUA, de no espaço intra-brigada utilizarem *links* satélite de elevado débito, está completamente fora do nosso alcance, ou de qualquer outra nação, com a extensão apresentada pelos EUA. Os italianos, os alemães, os franceses e os espanhóis têm alguma capacidade própria do tipo SATCOM, mas normalmente não é utilizada no espaço intra-brigada.

Outra grande condicionante é obviamente o financiamento. Neste momento qual é o grau de implementação do SIC-T?

Protótipos prontos: módulos de batalhão, companhia e nó de acesso. Estamos a construir um *rear-link* e um módulo de companhia. Os três primeiros estão prontos e destinam-se à EPT, onde foram atribuídos à CTmApoio. O primeiro grande teste será feito no terreno a 11 de Maio, com o apoio ao exercício Dragão, da BrigInt. Têm sido realizadas várias demonstrações a última das quais em Março na DCSI a S. Ex.ª o Gen CEME. Aproveitou-se a oportunidade para elementos da EPT terem o primeiro contacto com os módulos. O processo de transferência dos módulos para a EPT será complementado com formação teórica/prática na segunda quinzena de Abril. Os módulos irão para a EPT no início de Maio, estando planeada uma fase de treino até 11 de Maio, início do exercício.

Neste exercício ainda é a equipa do SIC-T que ficará responsável pela parametrização e ajustes dos equipamentos. Findo o exercício os módulos regressarão à equipa de projecto SIC-T para integrar alguns equipamentos que ainda não será possível integrar antes de Maio deste ano. No dia 10 de Julho está previsto a entrega dos módulos oficialmente na EPT. Em Outubro irão participar em larga escala no exercício ORION, e provavelmente no LUSÍADA.

Conjugado com a componente de comunicações, estamos igualmente a implementar o SICCE na componente operacional.

O SICCE neste momento está operacional em que unidades?

O SICCE ainda não está a ser utilizado de forma regular no Exército. Tem sido utilizado esporadicamente em exercícios e demonstrações. Existe agora uma *task force* para por o SICCE a funcionar de uma vez por todas. Foram adquiridos cem computadores e vamos por o SICCE a funcionar até ao escalão companhia. Todas as UEC de manobra da FOPE foram contempladas. O SICCE vai funcionar a partir do escalão companhia de forma real, este escalão é o primeiro responsável por alimentar e actualizar a base de dados do sistema. Vamos ter p.ex., uma operação no Kosovo e o CmdtComp vai dispor no seu terminal SICCE a localização de cada viatura da sua unidade, e qual o seu estado. Vamos começar a ter capacidade em tempo real de visualizar o que se passa, vamos ter uma imagem operacional. Qual é a maior dificuldade que enfrentamos na operacionalização deste sistema? Sem duvida a capacidade de cifra. Vão ser adquiridos equipamentos de cifra -TCE 621, para resolver esse problema. Na fase inicial os terminais SICCE irão ser colocados numa rede virtual, e quando as TCEs estiverem disponíveis será feita a migração para a rede *red*. No mesmo computador do SICCE irá igualmente correr o MMHS, portal de informação, sistema de correio electrónico, serviço de *chat*, ou seja teremos uma rede de informação operacional segura com os serviços que foram solicitados pela componente operacional.

O SICCE sempre foi difícil de pôr a funcionar devido à base de dados que o sustenta. Se não temos uma base de dados actualizada, não é possível apresentar informação útil. Como referi anterior irá residir no Cmdt de Companhia a principal responsabilidade em actualizar a base de dados, para que as operações passem a ser planeadas e conduzidas com o apoio desta ferramenta de comando e controlo.

Uma das críticas de militares que trabalharam com o SICCE, foi o facto de que com o esquema de funcionamento do nosso exército, o trabalho de inserção tem de ser feito em duplicado. É feito em papel e é feito no SICCE, por o formato de saída do SICCE não ser o que está aprovado…

Os militares ainda não trabalharam com esta última versão da aplicação que está agora a ser instalada. Esta é a primeira versão que dispõe do formato da ordem de operações de raiz, já padronizada com a possibilidade de efectuar ordens parcelares etc. Se os militares ainda não estão habituados, é porque não fazem uma utilização diária desta ferramenta, a sua utilização diária permitirá uma familiarização com o interface gráfico do SICCE, por outro lado terão de se habituar a trabalhar neste ambiente, porque este é o modelo de dados que as outras nações NATO também estão a implementar. Esta versão está durante o presente ano a ser sujeita a testes de interoperabilidade a nível internacional. Somos um dos primeiros países que dispõe da versão validada internacionalmente (para validar a aplicação têm de ser realizados testes com sucesso pelo menos com três países) e no âmbito do MIP entra em vigor em 2009, estimando que o seu período de utilização se prolongue no mínimo até 2014. Porém, na componente territorial estamos já a instalar esta versão que internacionalmente só entra em vigor em 2009. O SICCE, juntamente com as restantes aplicações operacionais, vai ser suportado pela rede RIOS, a qual vai ter uma gestão centralizada a partir do RTm. Na região de Lisboa onde não temos restrições de largura de banda na rede SICOM, esta rede segura irá igualmente suportar VoIP, serviço que se estenderá à restante rede quando podermos implementar QoS.

RIOS significa?

Rede de Informação Operacional Segura.

Ao nível dos exercícios, a gestão desta rede será feita pela CTmApoio. Equacionou-se a ideia de os militares da CTmApoio estagiarem no RTm para irem mantendo o know-how de gestão da rede e não a praticarem apenas nos exercícios, e também garantir ao RTm o pessoal técnico necessário para manter os sistemas a funcionar.

Ao nível do SIC-T (componente de comunicações) existe uma proposta desta Direcção, com alguma abertura do Gen CEME, para reforçar o investimento no SIC-T. Aliás, não de reforçar, mas sim de concentrar as verbas. Não podemos ter a capacidade de C2 que necessita de um investimento de cerca 70.000.000 € dispersando este investimento até ao ano de 2017, correndo-se o risco de a tecnologia que estamos a utilizar agora nem sequer estar disponível em 2017. Vamos tentar concentrar este investimento em 4 anos,

entre 2009-2012. Mas não temos ainda a certeza se esta proposta vai ter um despacho favorável. Em termos concretos não sabemos ainda quando vai estar disponível uma capacidade real de Comando e Controlo no Exército.

Com a estrutura modular do SIC-T faz sentido estarmos a diferenciar o apoio CIS que temos de prestar nas operações militares convencionais? Como numa defensiva ou ofensiva? Com as actuais características dos equipamentos e sistemas, parece-me que se prestam serviços sempre da mesma maneira…

Como sabes, estamos algo atrasados na definição do conceito de emprego e doutrina do SIC-T, embora na generalidade concorde com essa perspectiva. Reconheço que com as contramedidas que é possível implementar com o rádio de combate através de salto em frequência, e sendo fundamentalmente todas as comunicações baseadas em transmissão de dados, não estamos tão expostos como estávamos do antecedente. Por exemplo os meios CIS das VBR foram implementados em conformidade com a arquitectura do SIC-T, e continuam a estar preparadas para se interligarem, numa posição defensiva, sem utilizarem meios rádio, podem interligar-se por WD1-TT ou cabo óptico permitindo a implementação de uma rede de dados local nessa posição defensiva. Todas as viaturas têm um interface óptico. É evidente que as ligações filares só se justificam em posições de natureza estática…

E a integração num esforço conjunto para obtenção de uma IOC?

Estás a falar ao nível dos sistemas de informação. O MIP, ao qual o SICCE pertence está a fazer um grande esforço para que o modelo de dados seja conjunto, o mesmo já está reflectido no STANAG 5525, já ratificado por Portugal. Ou seja, temos um modelo de dados conjunto. Agora uma coisa é estar ratificado, outra é estar implementado.

Surgiu a ideia de ao nível do EMGFA se realizar, com uma periodicidade bianual, um exercício focalizado apenas na interoperabilidade das comunicações e sistemas de informação. Porém não têm existido condições para a sua realização. Pretendia-se fazer um exercício do tipo *Combined Endeavor*, só que nacional. É caricato que tenhamos uma capacidade de interoperabilidade combinada terrestre superior à interoperabilidade conjunta nacional.

O primeiro trabalho conjunto, que conheço, esta a ser realizado no Centro de Operações Especiais Conjunto. Quer na componente de comunicações quer para o sistema de informação está a ser desenhado um modelo conjunto. Infelizmente, para todo o tipo de

exercícios o EMGFA tem vindo a utilizar, na componente de comunicações, uma *shelter* da FAP.

A filosofia do SIC-T é muito semelhante à que esteve por detrás do módulo CIS de Operações Especiais Conjuntas. Não quero dizer que o SIC-T influenciou essa arquitectura, mas sim que os módulos do SIC-T, que estão preparados para serem utilizados operacionalmente já têm inseridas as alterações que foram propostas no âmbito dessas reuniões conjuntas. Saliento especialmente a questão dos diferentes domínios de rede (*national secret, mission secret* e administrativo).

Tem sido dado ênfase à componente de segurança?

Confesso que nesta altura não estamos a dar muita ênfase à componente de segurança para além das TCEs. Porquê? Adoptámos a estratégia do TACOMS: primeiro pomos tudo a comunicar e a funcionar, e depois começamos a fechar vulnerabilidades. Se não actuarmos assim de início, o processo de *troubleshooting* torna-se infinitamente mais complexo. No âmbito do TACOMS foi agora criado muito recentemente o TSWG[69], no qual esperamos vir a participar.

Os EUA têm uma rede global integrada, a GIG. Ou seja, existe uma rede das redes, onde toda a gente fala com toda a gente desde que esteja autorizado para tal. Não é feita uma diferenciação muito demarcada entre os níveis táctico, estratégico e operacional, no modo de funcionamento da rede. No caso do Exército, sempre houve uma grande separação entre as comunicações tácticas e as permanentes (estratégicas). Neste momento, com o SIC-T, está-se a esbater mais essa diferença? Ou, pelo contrário, ainda continuamos com uma fronteira muito demarcada entre as duas redes?

Existe uma vontade muito forte de integração entre as duas. A separação não faz hoje qualquer sentido. A rede que vai ser projectada no terreno é a rede RIOS. O pessoal que está a trabalhar na rede RIOS quando ela não está projectada, ou não está em exercícios, é o pessoal da componente territorial. Mas quando ela é projectada, é o pessoal da componente operacional. Obviamente que tem de existir uma integração para as coisas funcionarem! Daí a proposta de os elementos da CTmApoio passarem a estagiar com alguma frequência no RTm.

[69] TACOMS Security Working Group.

E relativamente às CTm das Brigadas?

Ou existe a capacidade de investimento a curto prazo que eu mencionei anteriormente, três a quatro anos no máximo, para termos a capacidade de C2, ou estas CTm não vão ser constituídas nos tempos mais próximos. Estamos no SIC-T a dar prioridade ao reequipamento dos batalhões e das companhias operacionais de manobra em detrimento das CTm. Só a partir de 2011 surgem verbas para as CTm…

O Exército deve ter a capacidade de projectar uma brigada completa ou até três unidades de escalão batalhão (UEB). Mas neste caso estamos nitidamente a apostar apenas na projecção de UEBs?

Exactamente, UEB como primeira prioridade e Brigada como uma 2ª prioridade já algo distante.

Os QOM e QOP das CTm são adequados, ou são passíveis de ainda vir a sofrer alterações?

OS QOM e os QOP das CTm estão completamente desajustados uns dos outros. Na realidade estão com material do sistema antigo e com QOPs vocacionados para o SIC-T. Na minha opinião pessoal, face a este cenário de reequipamento CIS, faria o seguinte: concentraria todos os meios disponíveis num único local, talvez no Campo Militar de Santa Margarida (CMSM), e daí partiria o apoio CIS para todas as brigadas, nomeadamente para a realização de exercícios. Não vale a pena fazer de conta que temos três CTm quando na realidade não temos ainda uma. Não temos pessoal para as guarnecer (subalternos e capitães especialmente), e existem inúmeras faltas de material. Falo em Santa Margarida por ser a localização mais central a nível nacional. Somos poucos, quer sargentos quer oficiais, temos pouco material, não faz sentido estarmos a manter uma estrutura cujo produto operacional é reduzidíssimo.

Ao nível do SIC-T, concorda comigo que a arquitectura de rede do SIC-T é muito semelhante ao MSE do Exército Norte-Americano? Existem obviamente diferenças, como o facto de ser uma arquitectura full IP, utilizar cabos ópticos e se destinar a unidades de escalão brigada ou inferior, mas a filosofia apresenta muitas semelhanças. No entanto as funcionalidades e tipos de módulos são muito

semelhantes: tenho *links* de feixes hertzianos nos dois sistemas, tenho nós que se movimentam enquanto outros apoiam e garantem a redundância…

A arquitectura do SIC-T baseia-se no TACOMS. Indirectamente, reconheço que podemos, através do TACOMS, ter sido influenciados pelo MSE.

Entrevista nº5

Realizada em 01 de Abril de 2008, ao Adjunto da Repartição de Tecnologias e Sistemas de Informação da Divisão de Comunicações e Sistemas de Informação do Estado Maior General das Forças Armadas, TCor TInf Luís Palha.

Meu Tenente Coronel,

Na sua opinião, como representante do EMGFA no grupo de trabalho da NNEC da NATO, as FAs estão sensibilizadas para o conceito de operações centradas em rede?

Infelizmente, ainda não. Este conceito envolve uma mudança de mentalidades e alterações estruturais profundas nos organismos de modo a dar resposta às solicitações dos Comandos Superiores sem por em causa a cadeia de comando. Grande parte da hierarquia superior das FAs não tem ainda uma ideia clara do que são operações centradas em rede e vêem com certo receio o "partilhar" e "distribuir" Informação. Quem tem informação tem o poder. Existem uma série de ses e senãos que as nossas estruturas superiores de comando, não só em Portugal mas também noutros países, constataram ser esta uma questão problemática. Ao nível da componente da educação e treino deu-se um passo importante com a junção das academias, tentando-se sensibilizar nesta temática quem começa agora a ser formado, havendo necessidade de aparecerem programas de ensino muito concretos. É necessário começar a sensibilizar de raiz os futuros decisores. Isto é um problema que vai durar 5,10, 15 anos de reforma ao longo do tempo. A mentalização custa muito a avançar. Perante o cenário actual que temos a nível mundial, para cimentar um conceito destes, quanto mais agregador for o projecto, melhor. Foi por essa razão que NATO se virou para a componente infra-estrutural e tecnológica. É essa a área onde se consegue avançar rapidamente, tirando partido dos sistemas e tecnologias que estão disponíveis na componente civil. É nessa base que a NATO está a avançar. Há relativamente pouco tempo, esteve em Portugal uma delegação da NATO, com as *Force Proposals (FPs)*. Pela primeira vez apareceram *FPs* relativas ao NNEC, nomeadamente "*Information Assurance, Information Systems, Enabled Communications, Enabled Interoperability"*. Tudo isso é novo. Estive reunido com os elementos da NATO a discutir os assuntos relativos à componente técnica da DICSI, juntamente com o TCor Glicínio

Fernandes. Apresentámos a perspectiva nacional, para um horizonte temporal de médio e longo prazo, isto é até ao ano de 2020 inclusive.

Do que falamos em termos de *enabling* para a NNEC em termos nacionais?

Integração, partilha da informação, interoperabilidade, QOS, Cyber Defence, migração do protocolo IPv4 para IPv6, IEG (Information Exchange Gateway), entre outros programas.

Em conversa com o Sr. Major-general Edorindo Ferreira, Chefe da Divisão de Comunicações e Sistemas de Informação do EMGFA, ficámos com a sensação que a nível conjunto não existe praticamente nada?

Prevê-se que vá começar a haver. Temos que ter iniciativa. Estamos numa fase de não retorno. Portugal vai chegar a um ponto onde ou faz ou fica de fora. Existem compromissos que Portugal assumiu, nomeadamente ao nível das *Force Proposals*. Temos que ver o que fazem os outros países ao nível NATO e alinharmos por eles dentro da nossa realidade. Tudo isto tem custos elevados. Como exemplo a NATO pode estabelecer linhas de orientação para migrar definitivamente do protocolo IPv4 para IPv6 até 2010, e a Grã-Bretanha pode interpor dizendo que só o pode fazer em 2019. Deste modo, estamos perante uma situação de compromisso de meio-termo, que tem que ser coerente dentro das nossas capacidades e das dos outros países da Aliança para se chegar a esse objectivo. Há no entanto muita coisa por fazer, e é preciso um grande envolvimento e apoio dos ramos das FFAA, coisa que se verifica muito pouco. Existem alguns oficiais e departamentos que estão sensibilizados. No caso particular da Marinha através da 6ª Divisão, tem pessoal que está envolvido nestas matérias. A FAP encontra-se presentemente em transformação. Estão a decorrer reestruturações na FAP, as Direcções de Informática e de Electrotecnia fundiram-se na nova DICSI que ainda está na fase embrionária. É a transformação constante mas os anos vão passando e têm que ser tomadas decisões. Também é preciso pessoal qualificado para "agarrar" estas novas tecnologias, matérias que requerem tempo e estudo, que requerem metodologia, método de trabalho, equipas organizadas dos três ramos para estarem a trabalhar em todos os projectos desta área. Ou seja necessitamos de integração, de "remarmos" todos para o mesmo lado. Infelizmente não se vê isso. Daqui a alguns dias vou fazer uma convocatória acerca da migração do IPv4 para IPv6. A última vez que tu foste ao curso de IPv6 ao CET em Aveiro mais o Cap Manso (FAP) foi há 8 anos, não é verdade?

Não, eu não fui porque estava no CPOS nessa altura.

Sim, mas já foi há oito anos. O processo morreu no dia em que terminou o curso…E daqui a dias está a bater à porta, e não há nada feito. E o único Ramo que tomou a iniciativa de falar sobre esta questão com o EMGFA/DICSI foi a Marinha há relativamente pouco tempo. Vê bem as implicações que isso tem ao nível não das FFAAs, mas sim ao nível de toda a Defesa. É que *network centric* não são apenas as FFAAs, é o MDN, o MAI, etc. Nós tentamos acompanhar os projectos da NATO, mas há uma falta tremenda de pessoal com conhecimentos técnicos e de apoio dos ramos nesta área.

Da minha experiência pessoal, eu vinha a reuniões dos mais variados projectos na área das TIs e via sempre as mesmas caras…

E continua, mas com uma agravante. É que as pessoas são as mesmas, mas são cada vez menos. E o *outsourcing* não é alternativa para tudo. Não são os homens do *outsourcing* que vão ao terreno resolver os problemas quando as coisas correm mal…

Assusto-me com a falta de bases que existe na área de *networking* e sistemas nos ramos…

E o problema é que as chefias não estão sensibilizadas para isso…

APÊNDICE 2 – FIGURAS

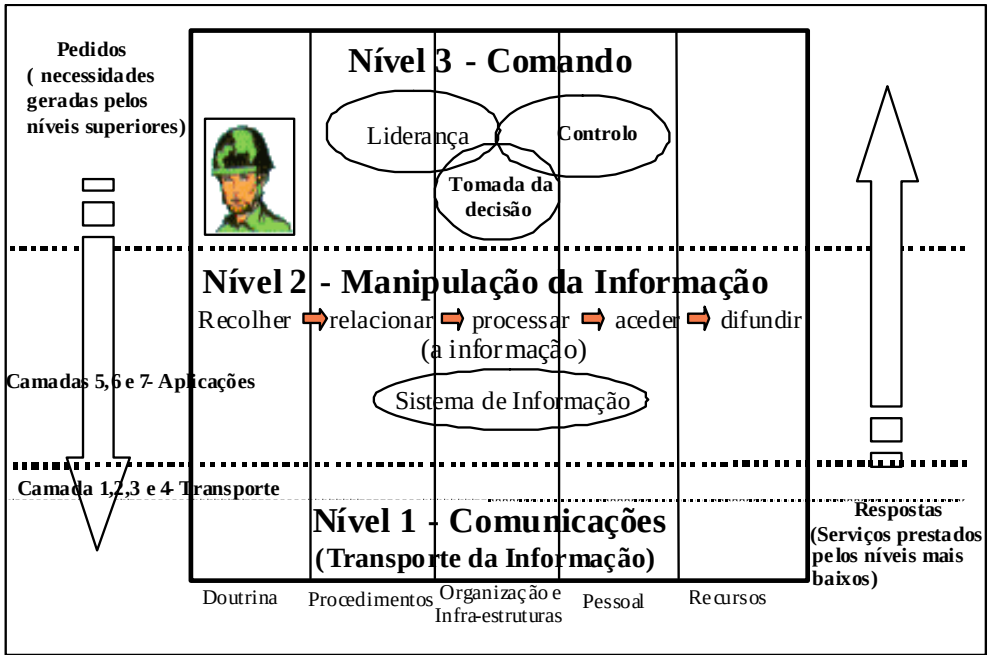

Figura 1- Organização de um Sistema de C2 em 3 níveis (DST, 2003: 4)

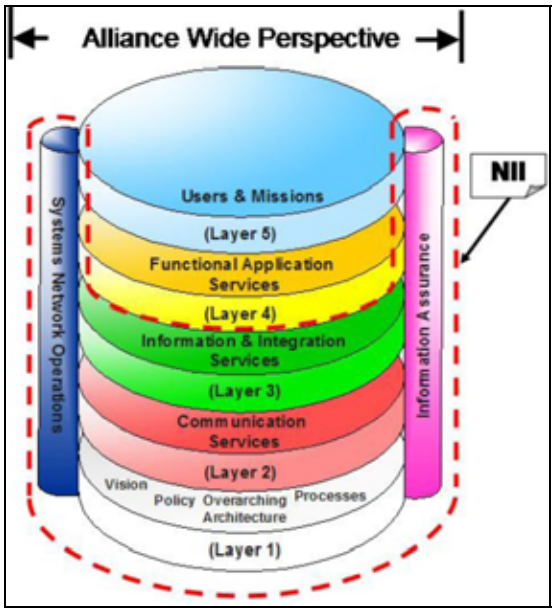

Figura 2 - Esquema Funcional do NII baseado no modelo OSI (NC3A, 2005: 6).

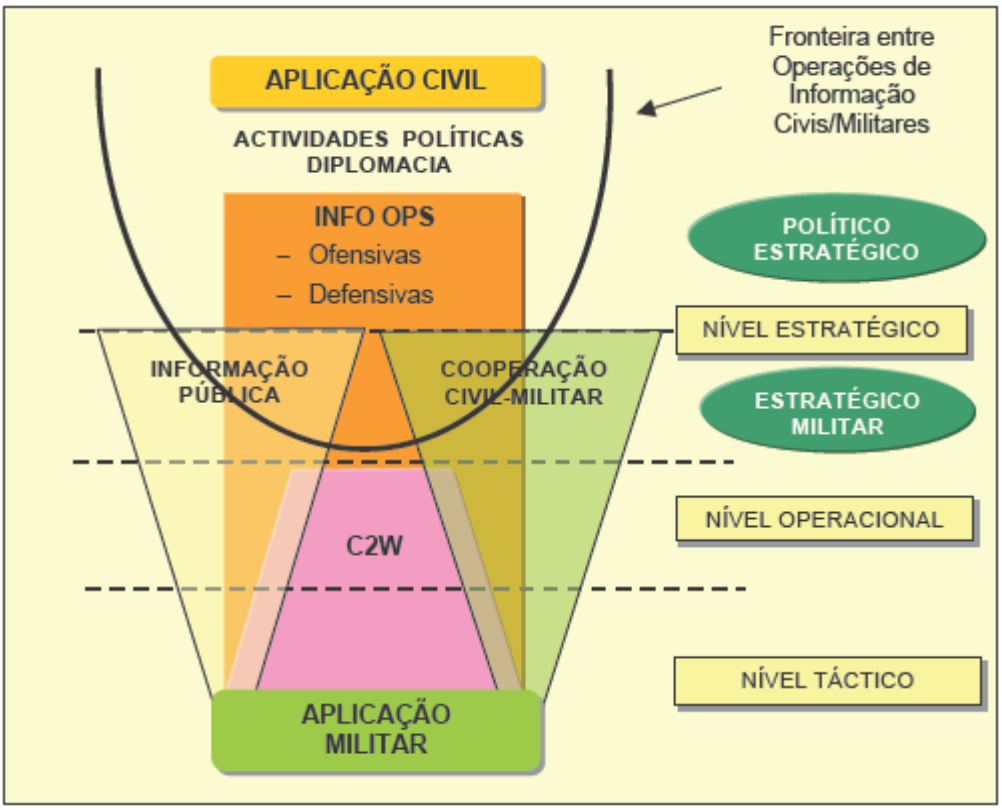

Figura 3 - Abrangência das Operações de Informação (DST, 2007:11)

Figura 4: Estrutura de um SIC (CARREIRA, 2002:13)

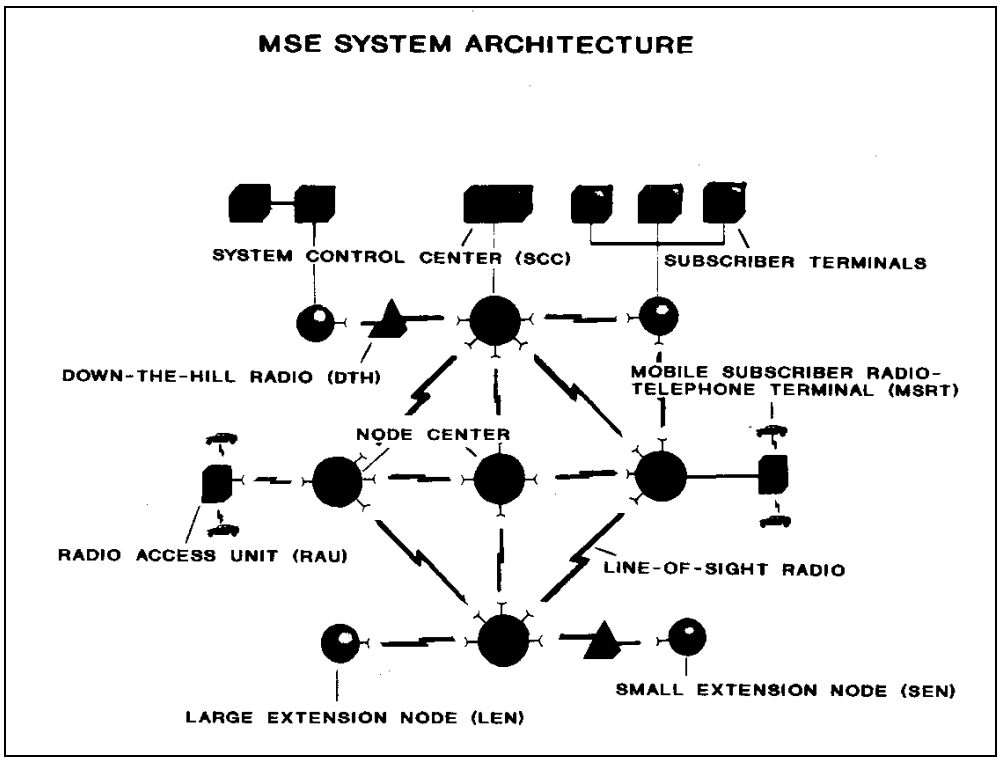

Figura 5 - Arquitectura do sistema MSE (GLOBALSECURITY,2008)

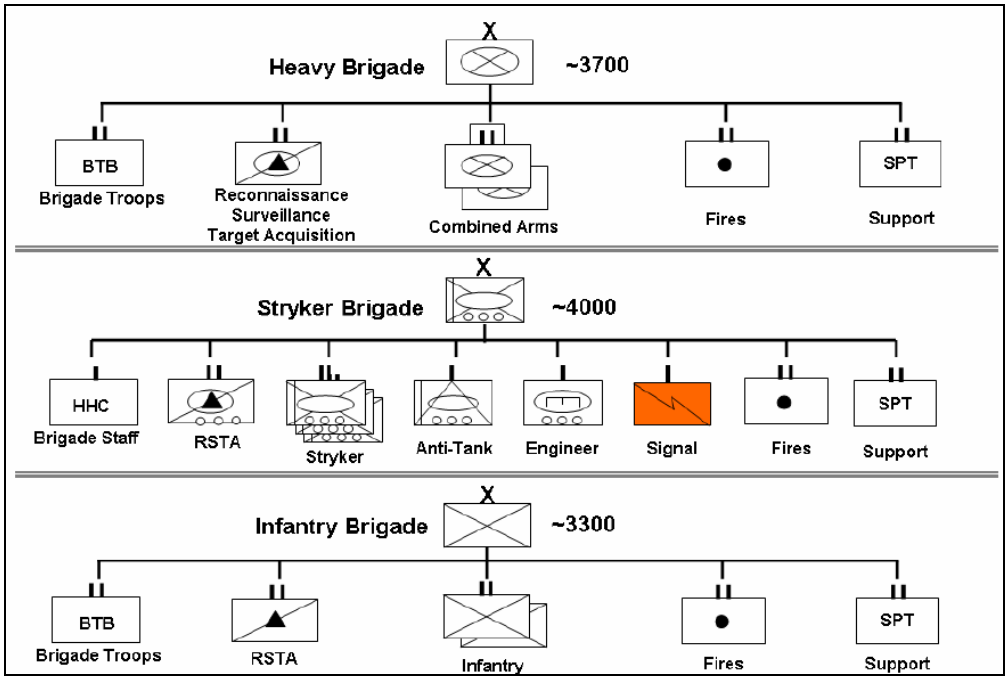

Figura 6 - Constituição das BCT (FMI 6.02-50, 2005: 10-2)

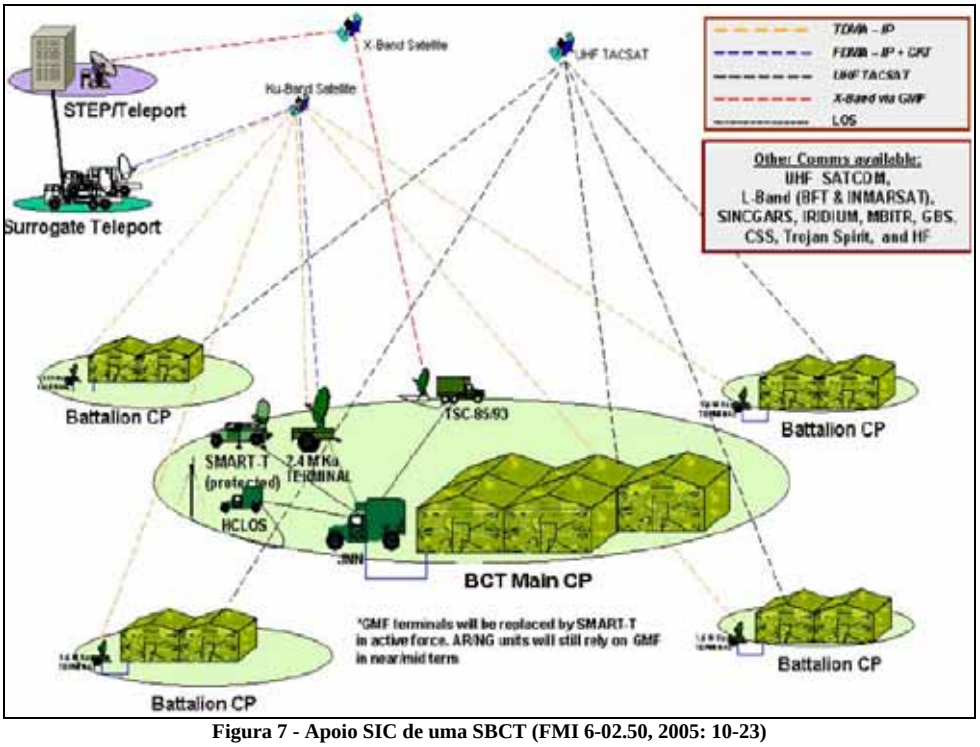

Figura 7 - Apoio SIC de uma SBCT (FMI 6-02.50, 2005: 10-23)

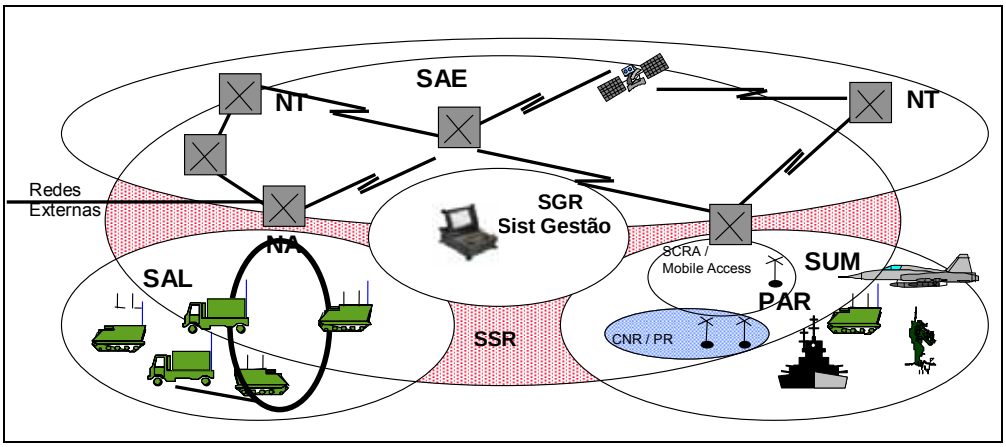

Figura 8 - O SIC-T e os seus subsistemas (DST, 2003: 21)

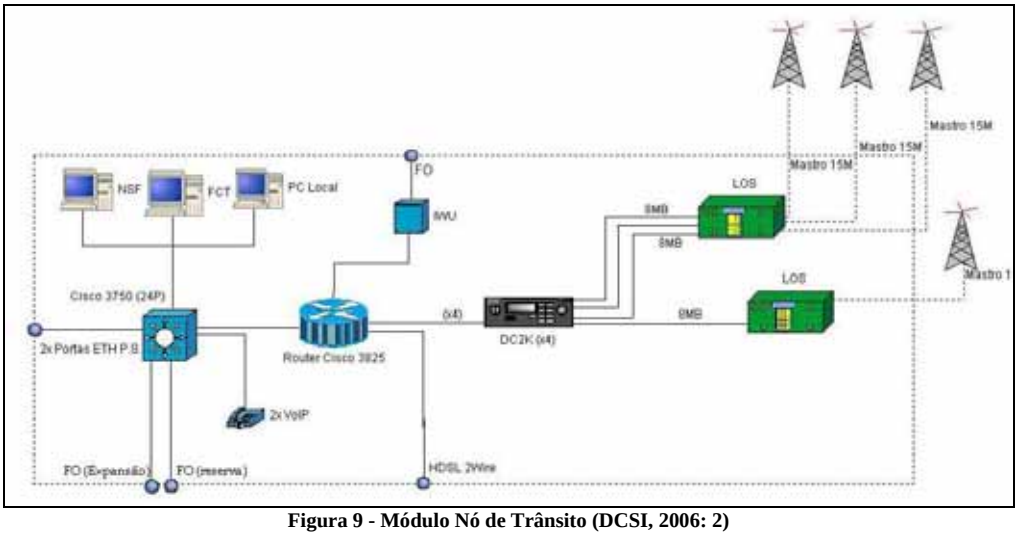

Figura 9 - Módulo Nó de Trânsito (DCSI, 2006: 2)

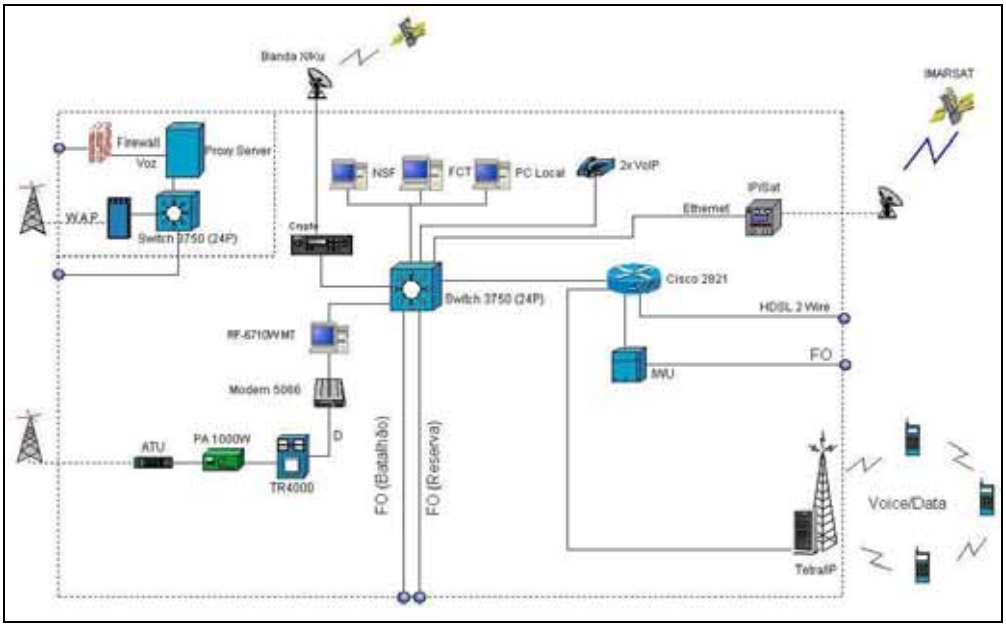

Figura 10 - Módulo *rear link* (DCSI, 2006: 3)

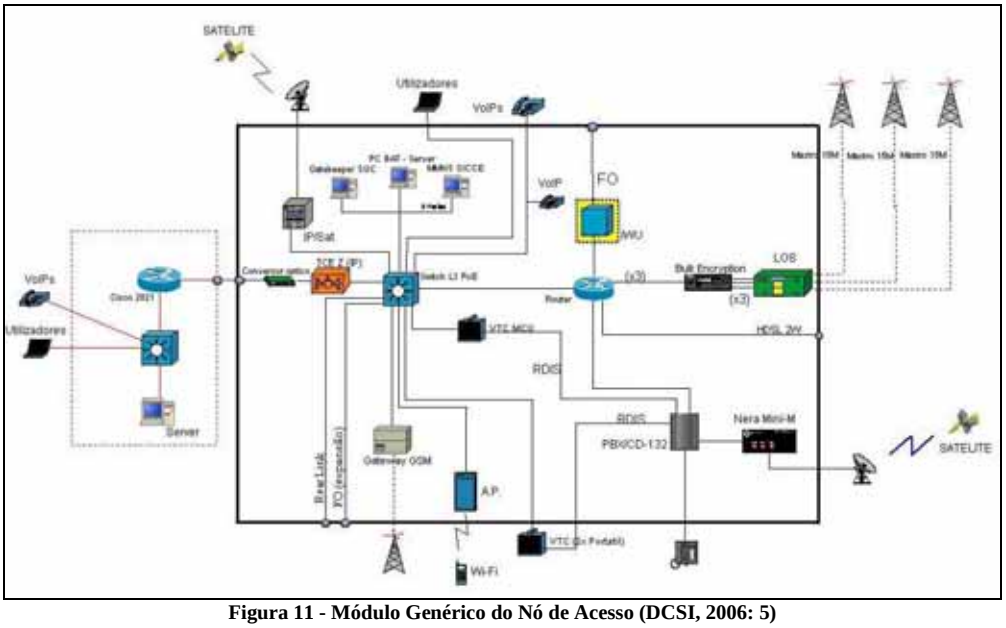

Figura 11 - Módulo Genérico do Nó de Acesso (DCSI, 2006: 5)

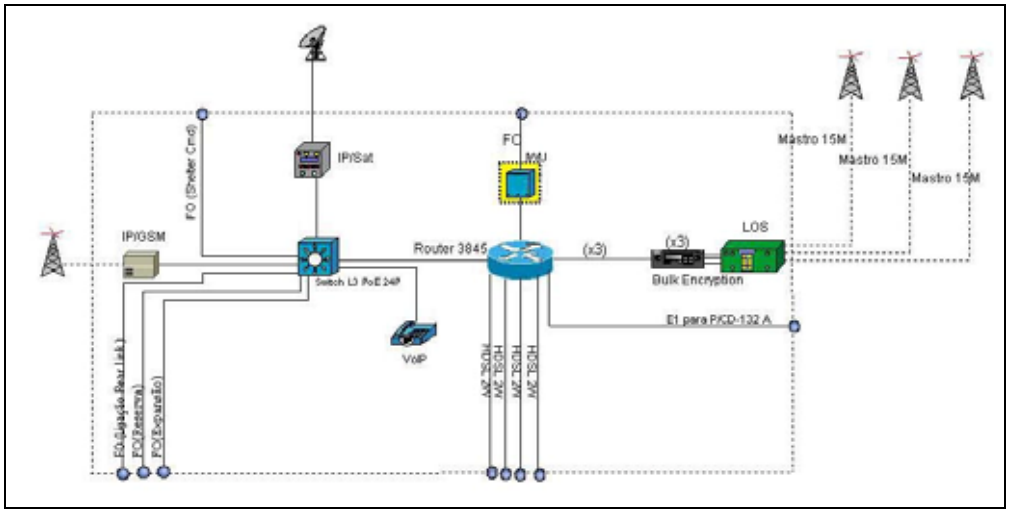

Figura 12 - Shelter de Transmissão do Nó de Acesso (DCSI, 2006: 6)

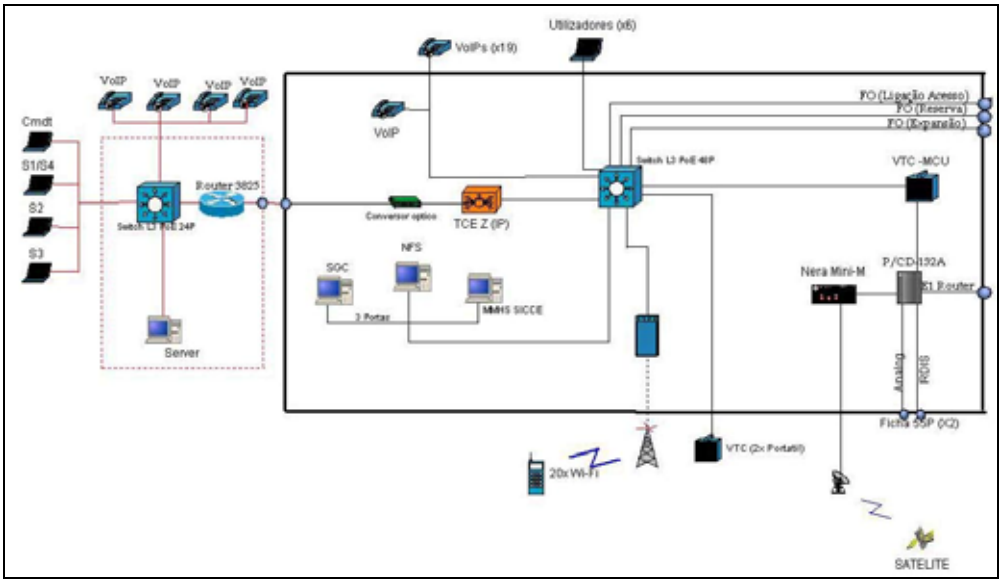

Figura 13 - Shelter de C2 e Gestão do Nó de Acesso (DCSI, 2006: 6)

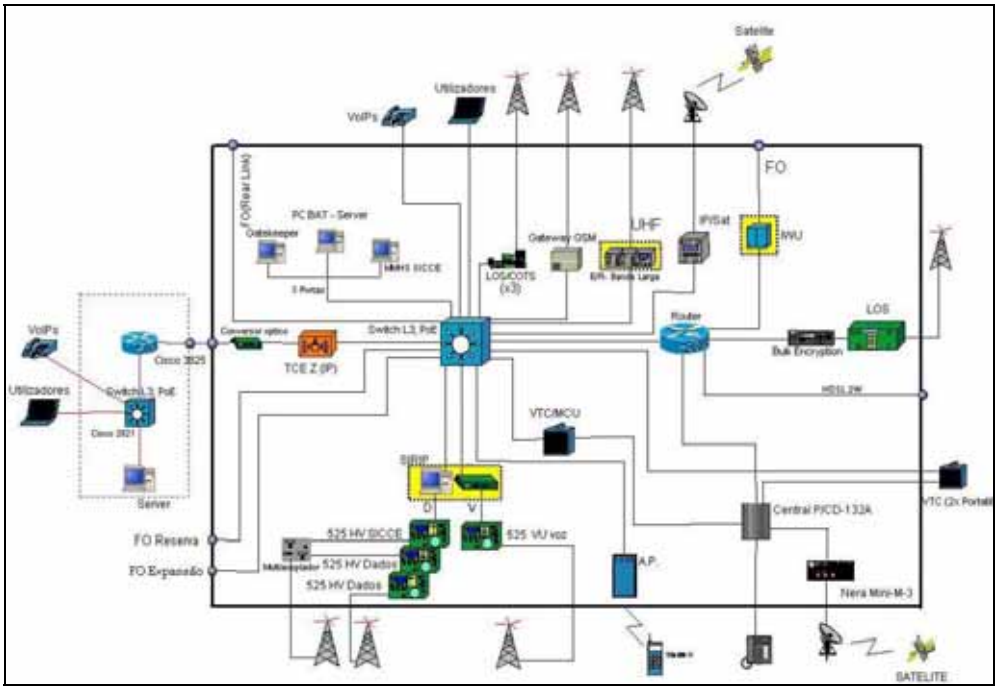

Figura 14 - Módulo do Centro de Comunicações do Batalhão (DCSI, 2006: 7)

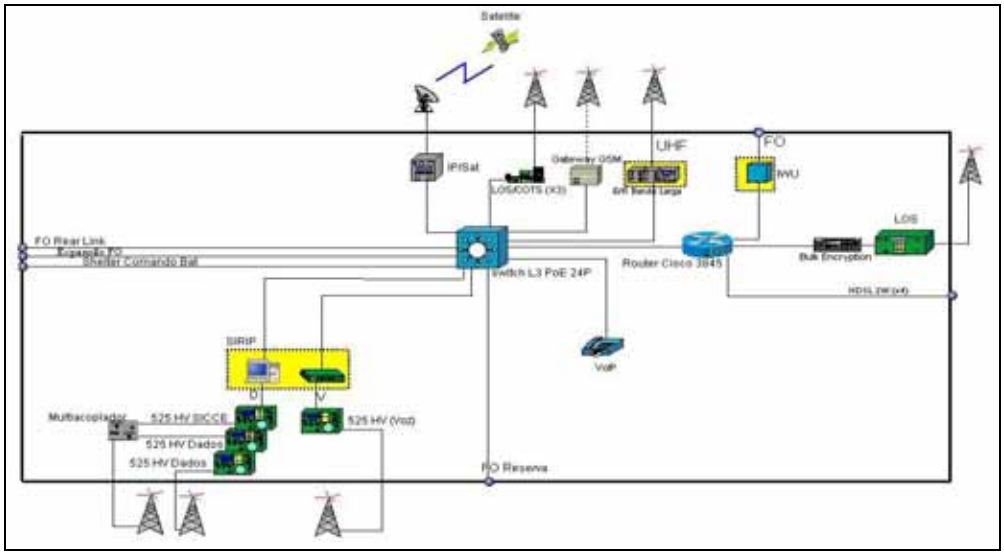

Figura 15 - Shelter de Transmissão do Centro de Comunicações de Batalhão (DCSI, 2006: 8)

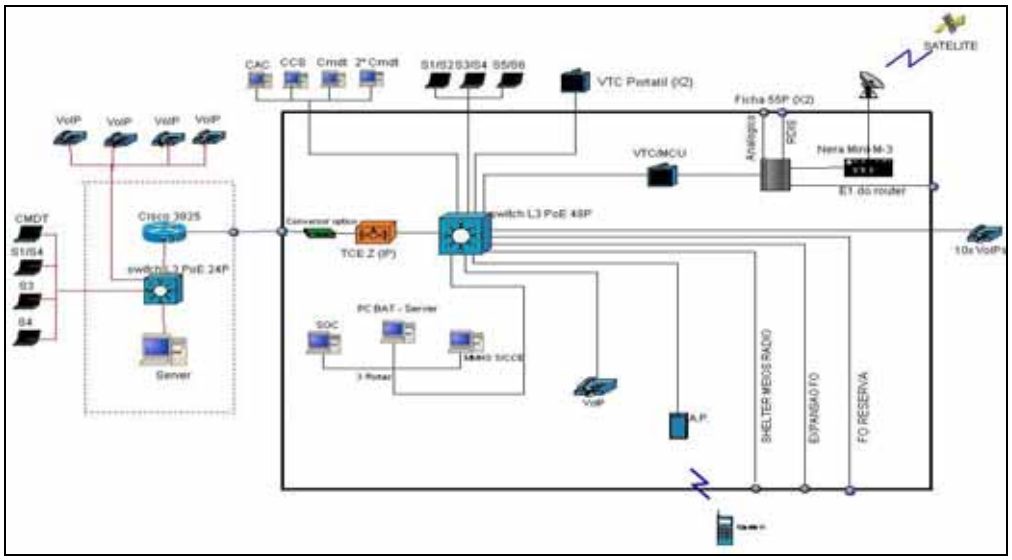

Figura 16 - Shelter de C2 & Gestão do Centro de Comunicações de Batalhão (DCSI, 2006: 9)

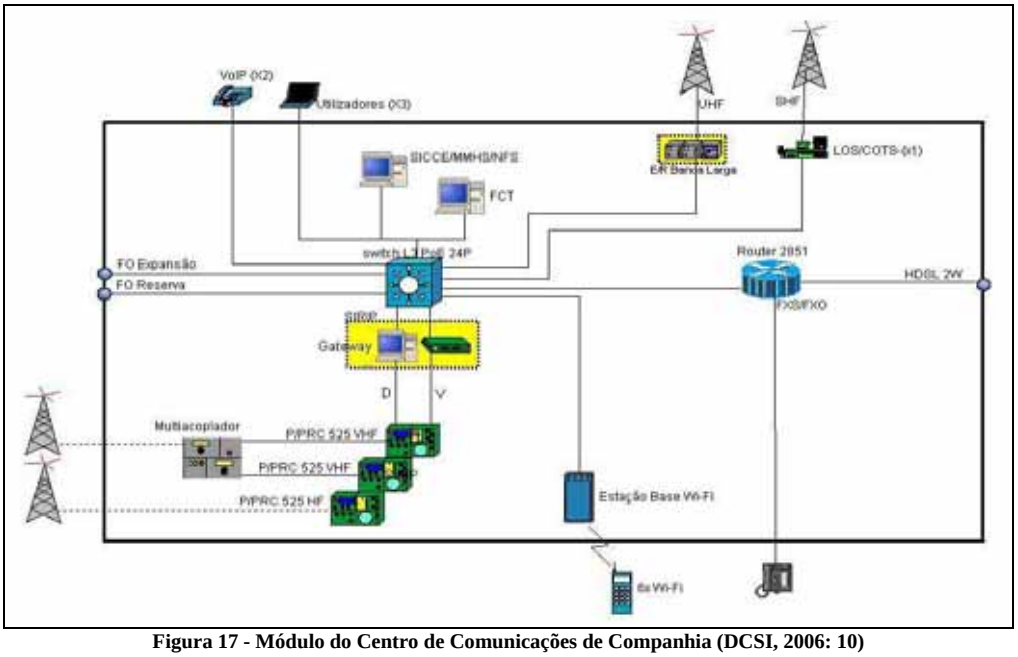

Figura 17 - Módulo do Centro de Comunicações de Companhia (DCSI, 2006: 10)

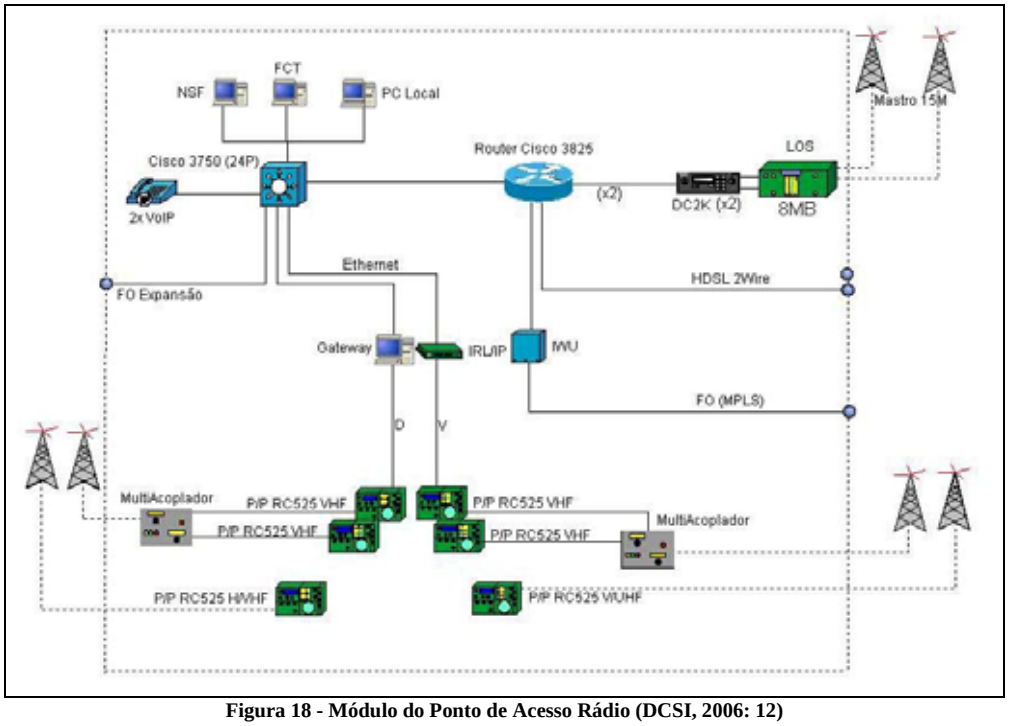

Figura 18 - Módulo do Ponto de Acesso Rádio (DCSI, 2006: 12)

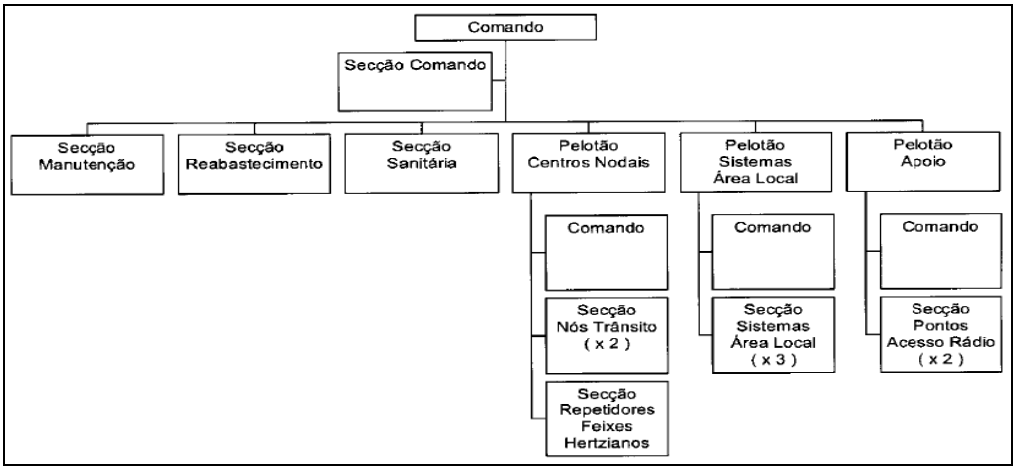

Figura 19 - Organigrama de CTm de Brigada (QOP CTm BrigRR, 2006: 1)

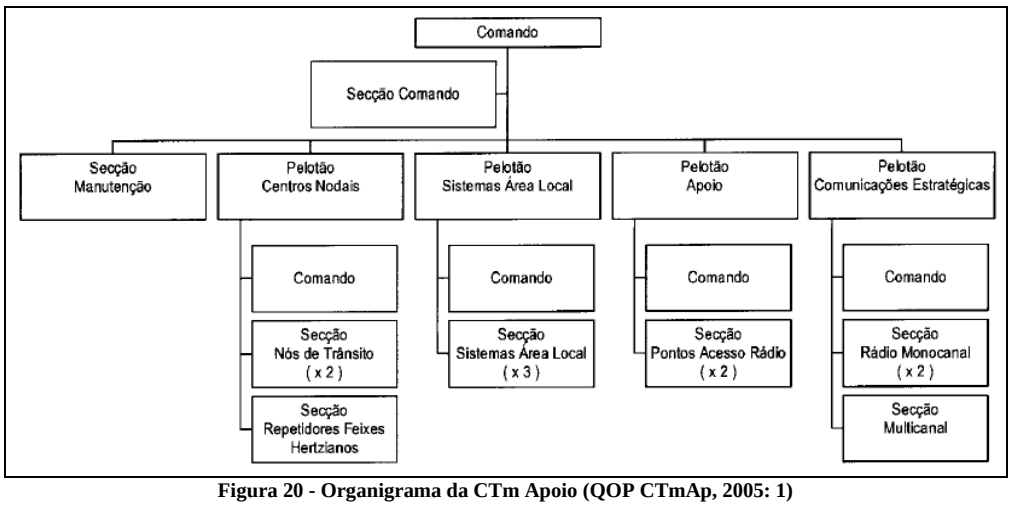

Figura 20 - Organigrama da CTm Apoio (QOP CTmAp, 2005: 1)

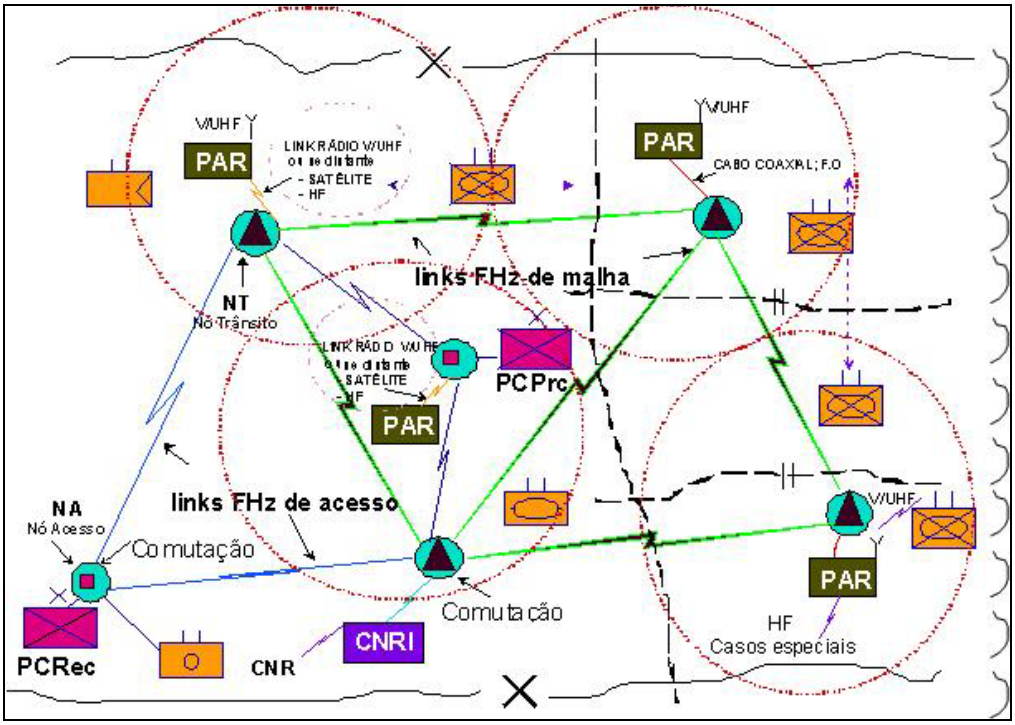

Figura 21 - Exemplo do apoio de comunicações a uma Brigada (DST, 2003: 27)

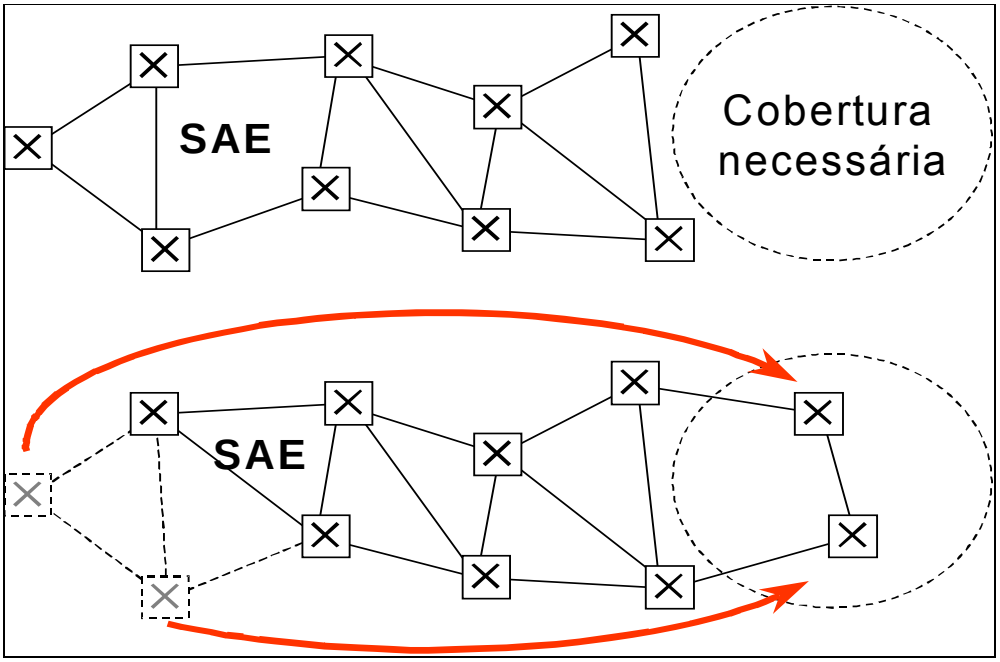

Figura 2 - Movimento de nós SAE (DST, 2003: 23)

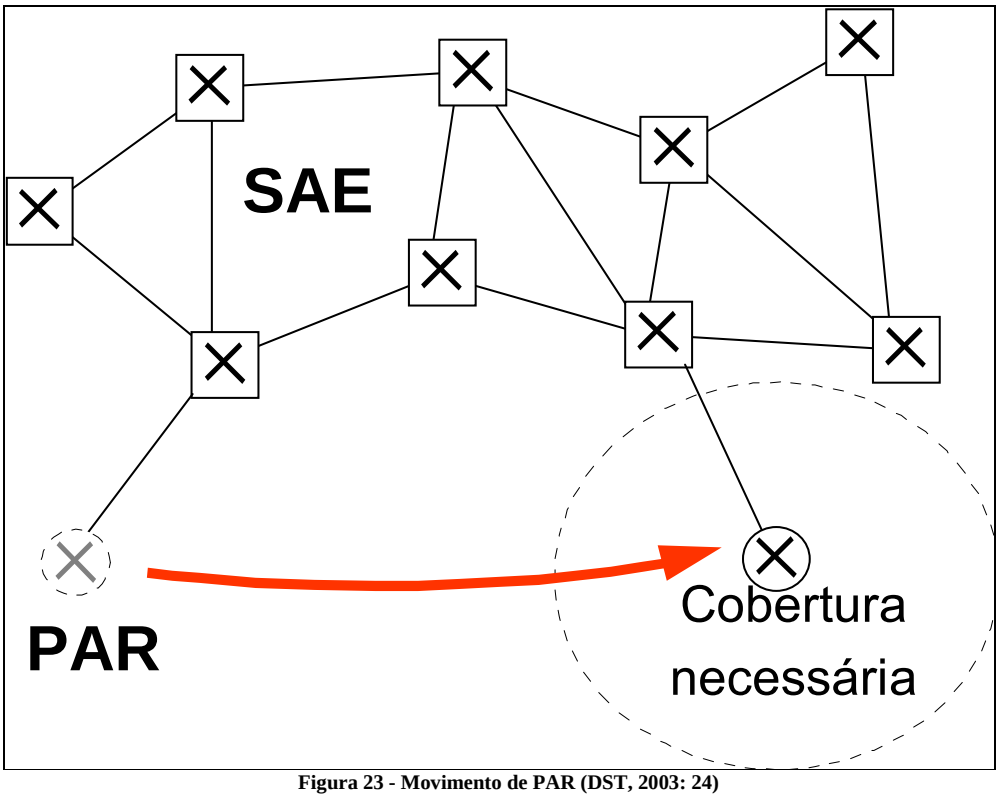

Figura 23 - Movimento de PAR (DST, 2003: 24)

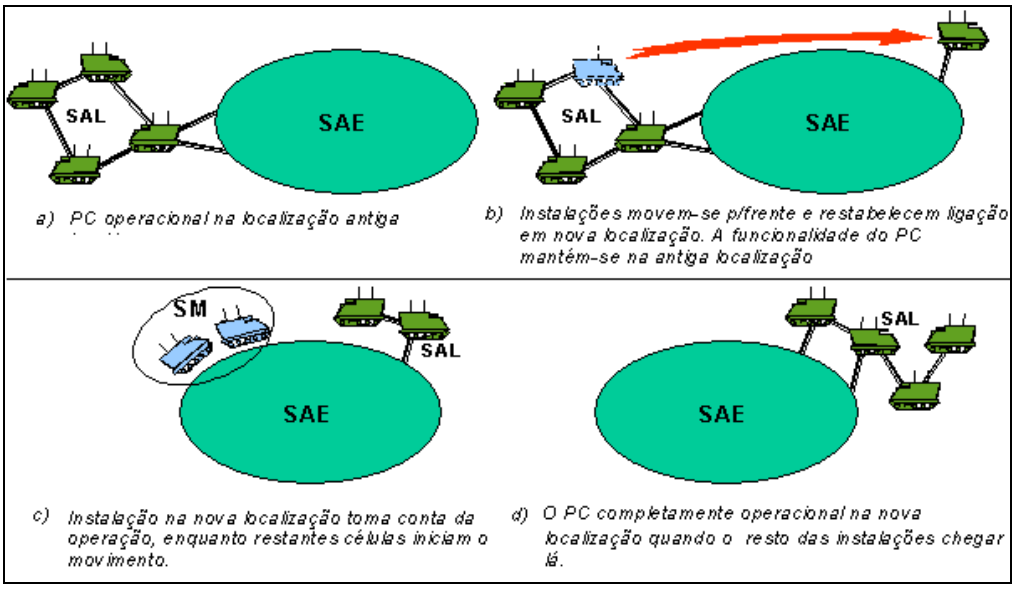

Figura 24 -Exemplo de movimento de um PC, sem duplicação de elementos (DST, 2003: 24)

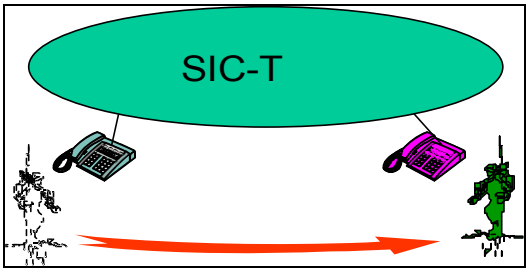

Figura 25 - O assinante restabelece a ligação (reafilia-se) noutro terminal (DST, 2003: 25)

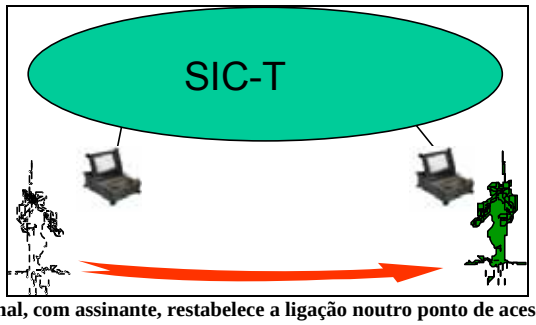

Figura 26 - Terminal, com assinante, restabelece a ligação noutro ponto de acesso (DST, 2003: 25)

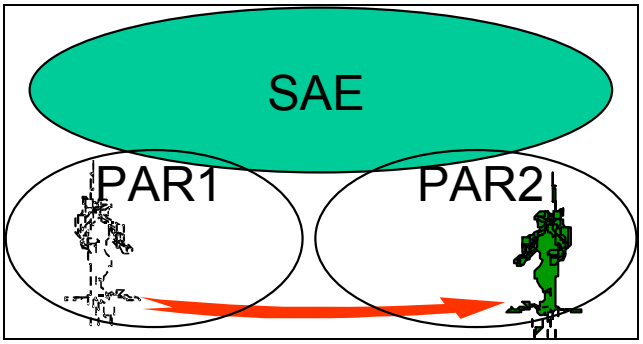

Figura 27 - Mover para outro PAR (DST, 2003: 26)

APÊNDICE 3 - SEGURANÇA DOS SISTEMAS DE COMUNICAÇÕES E INFORMAÇÃO

There is no security on this earth. Only opportunity.

Douglas MacArthur

a. Considerações de segurança de redes

O *NATO Network Enabled Capability (NNEC) Feasibility Study* (NNEC FS) delineou uma visão para a *Network and Information Infrastructure* (NII) necessária para suportar todo o espectro de operações militares previstas para o futuro. Foi identificada uma estratégia de desenvolvimento evolucionário para o NII, sendo que um dos aspectos críticos nesta abordagem é a disponibilidade de aparelhos de cifra de rede IP flexíveis e interoperáveis. Se não se dispuser de um equipamento com essas características, a evolução para a NEC será seriamente adiada. (GOODE, HALLINGSTAD, 2007: 3-5)

O NNEC FS inclui uma quantidade de requisitos estratégicos que têm de ser alcançados para que se possa alcançar a NNEC. O requisito estratégico Nº 7 consiste em "criar uma infra-estrutura de comunicações baseada em redes IP *black-core*[70], convergentes, e multinacionais, operada como uma Federação de Sistemas". O SIC-T possui todas as condições para poder ser inserido nesta realidade. Isto, porque a NII tem tendência a evoluir para uma arquitectura orientada por serviços, onde a confidencialidade da informação é aplicada junto do destinatário/utilizador e a rede providencia uma grande disponibilidade do serviço de transmissão/transporte, permitindo classes diferenciadas de tráfego, bem como a prioritização do mesmo. A componente de encriptação IP da rede[71]deverá estar em completa consonância com esta filosofia. Como tal, deverá ser capaz de suportar simultaneamente serviços de voz, vídeo e dados, e deverá estar disponível num formato interoperável para todos os membros da coligação.

A abordagem da segurança à NNEC inclui numa fase inicial a confidencialidade da informação residente na rede, mas ao nível aplicacional inclui também já a confidencialidade para capacidades específicas (p.ex. voz segura). A abordagem da segurança evoluirá eventualmente para um conceito baseado em objectos informacionais. O NINE aborda apenas a aproximação baseada em rede, mas deve ser implementado de modo a não ser condicionado por futuras evoluções de conceitos.

[70] Redes não classificadas e não diferenciadas, utilizáveis como rede de "transmissão" e roteamento para redes *red* (classificadas).´

[71] Designada oficiosamente na NATO como NNEC NII IP *network encryption* (NINE).

O objectivo principal do NINE é garantir, com elevado grau a confidencialidade da informação quando a mesma for transportada entre domínios de confiança[72]. Contudo, como componente integral do NII, dever-se-á garantir que equipamentos NINE suportem integralmente os fluxos de informação e os requisitos de gestão.

(1) Funções de segurança comuns de equipamentos de cifra IP

Os equipamentos de segurança utilizados actualmente nas organizações militares e civis para o estabelecimento de Virtual Private Networks (VPNs) assentam normalmente no standard IP Security (IPsec). As funções de segurança que podem ser encontradas nesses produtos incluem normalmente: confidencialidade e integridade dos dados, autenticação explícita e implícita da fonte, confidencialidade parcial do fluxo de dados e imposição de políticas, como se ilustra na figura 28.

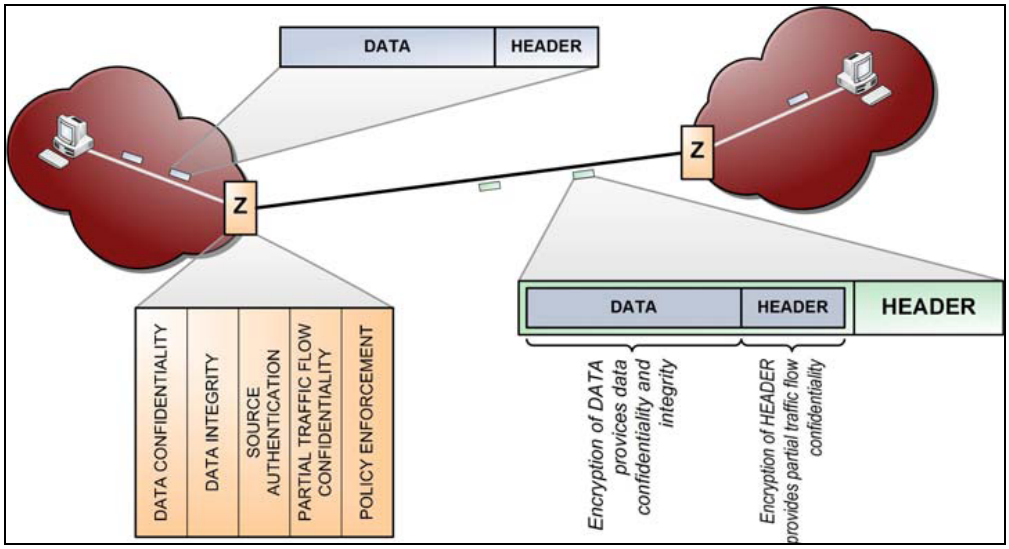

Figura 28 - Funções de segurança de equipamentos de cifra IP

A confidencialidade dos dados garante que o conteúdo dos dados não é divulgado a pessoal não autorizado. É alcançada pela encriptação do corpo dos pacotes IP. Os dados são encriptados no emissor ao entrar num equipamento IP cripto, e são posteriormente desencriptados num equipamento IP cripto do lado receptor. A confidencialidade dos dados sempre foi tradicionalmente o ponto focal da segurança da informação. A integridade dos dados é atingida de maneira semelhante, e garante que os dados não foram modificados durante a transmissão.

A autenticação da fonte (emissor) é conseguida explicitamente na especificação IPSec quando existe uma associação de segurança entre pares. Durante este

[72] Domínio de confiança: grupo de computadores em rede que partilham serviços de directoria comuns.

estabelecimento, é gerada uma chave que implicitamente autentica na fonte todos os pacotes pertencentes a essa associação de segurança durante uma dada transmissão.

A autenticação é limitada ao equipamento IP cripto originante ou mesmo a um grupo de equipamentos IP cripto no caso da utilização de chaves de grupo partilhadas. Na maioria dos casos, isto significa que pode ser identificada a rede de origem, mas não o utilizador ou máquina originante.

Com a utilização destes aparelhos, consegue-se igualmente obter um grau limitado de confidencialidade do fluxo de tráfego. Devido ao facto de o cabeçalho IP ser encriptado, o originador e o destinatário não serão revelados no caso de uma análise da informação cifrada. Contudo, esta capacidade de confidencialidade do fluxo de tráfego é apenas parcial, dado que as comunicações entre redes podem ser monitorizadas, bem como o volume de tráfego e os ritmos de transmissão de pacotes.

Muitas vezes, os aparelhos IP cripto também efectuam imposição de políticas, encaminhando selectivamente tráfego de uma rede para outra. Para a maioria dos actuais equipamentos de cifra IP[73], a política aplicada é muito simples: apenas o tráfego que tem a sua origem noutro equipamento de cifra IP autenticado é encaminhado para a rede classificada. Todo o restante tráfego é rejeitado. Para equipamentos que separem redes classificadas e não classificadas, o nível de garantia desta imposição tem de ser elevado de modo a isolar as redes de forma correcta.

(2) Conceito de Protecção do Núcleo da Rede (PNR)

Protecção do Núcleo da Rede (PNR) é um conceito que se pretende utilizar para implementar uma infra-estrutura de rede que seja capaz de ir ao alcance de futuras operações militares num ambiente NEC. O principal enfoque da PNR está no fornecimento de um serviço de transmissão/transporte que apresente o maior grau de disponibilidade possível. Deixa-se assim para atrás o tradicional enfoque na garantia da confidencialidade da rede, centrando-se cada vez mais a atenção na disponibilidade da rede em apoio de ambientes dinâmicos, conjuntos e combinados, e onde o factor tempo é de importância crucial. A NATO definiu três conceitos que auxiliam a compreensão da PNR:

(a) **Protecção do Núcleo da Rede (PNR) -** Consiste na disponibilização de serviços de transporte em ambientes dinâmicos, focado particularmente na obtenção da maior disponibilidade de serviço possível. É alcançado através da

[73] Tais como a TCE 621 da empresa THALES, que é empregue pelas Forças Armadas Portuguesas e se prevê que venha igualmente a equipar os módulos do SIC-T.

utilização de múltiplas classes de serviços de rede, tanto para desempenho como para segurança, combinadas com a protecção de todos os componentes da rede e com superior conhecimento, gestão e controlo.

(b) **Segmento de Núcleo Protegido (SNP) –** Rede implementada segundo os princípios da PNR, e que foi desenhada para trabalhar de forma consistente com outros SNP na base de uma Federação de Sistemas.

(c) **Núcleo Protegido (NP)** – Conjunto de SNPs trabalhando em conjunto no âmbito de uma Federação de Sistemas, com vista a atingir as características da PNR.

Ao passo que a PNR é um conceito, os SNPs e o NP são ambos redes, sendo o NP a culminação de uma abordagem tipo federação de sistemas. Num NP não existe uma autoridade central e os SNPs colaboram e cooperam em apoio de objectivos comuns. Mostra-se um exemplo de um NP na figura 29 (as cores indicam domínios de segurança diferentes).

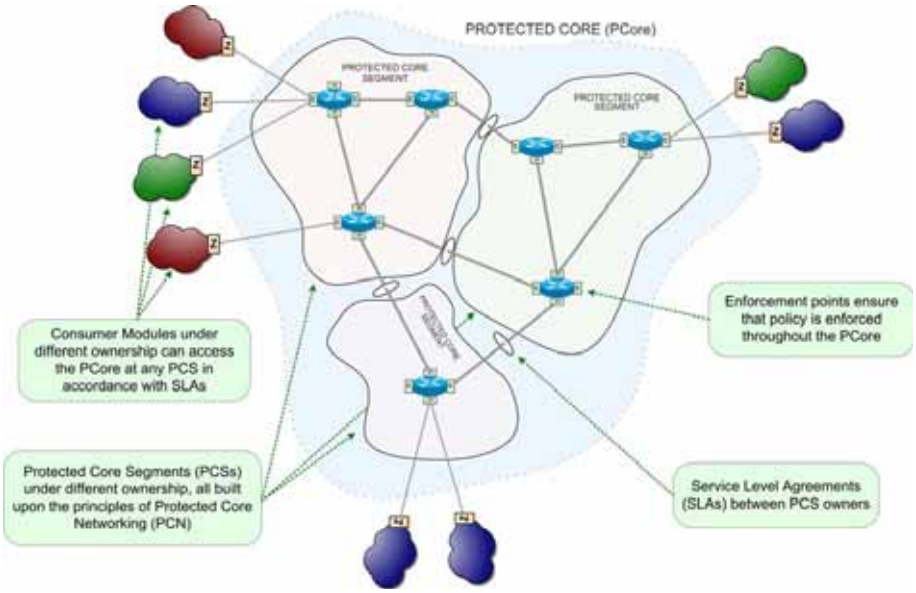

Figura 29 - Núcleo Protegido constituído a partir de múltiplos segmentos

Estas definições formam a base para providenciar uma infra-estrutura de rede que seja capaz de suportar as operações militares futuras, caracterizadas pela elevada velocidade da acção de comando, rápida adaptação e auto sincronização. De modo a permitir esta dinâmica, a PNR aborda várias áreas onde um conjunto de robustas capacidades de rede deve providenciar de uma forma eficiente o nível de disponibilidade da rede requerido. As características fundamentais da PNR serão:

Serviços Diferenciados: Elevada disponibilidade na PNR inclui o suporte de múltiplas classes de tráfego, tais como voz interactiva, vídeo e dados. Dado que a largura de banda pode ter limitações, múltiplos níveis de prioridade e também de preempção têm igualmente de ser suportados. Com o conceito de PNR, *best effort* não é suficiente para a implementação destas funções.

Gestão e Controlo Superiores: A disponibilização de alta disponibilidade requer *shared awareness* entre as áreas de rede, aplicação e gestão da segurança. Apenas com uma visão holística será o sistema de gestão capaz de suportar as operações, uma tarefa exigente da federação de sistemas.

Conhecimento Superior: As melhores decisões de gestão só poderão ser tomadas se estiver disponível o conhecimento adequado acerca da infra-estrutura. Esse conhecimento deve incluir informação acerca de todas as partes da infra-estrutura, tais como capacidade dos *links*, taxas de erro, propriedades da segurança, bem como informação acerca da carga de tráfego e padrões de ataques informáticos tentados.

Protecção Superior: Os mecanismos de protecção devem ser permeantes na PNR, impondo políticas que assegurem a remoção imediata de tráfego não autorizado.

Suporte de ambientes dinâmicos e federados: Uma conectividade consistente é necessária tanto para os utilizadores como para os segmentos da infra-estrutura de rede. De modo a aumentar a flexibilidade, aplica-se o conceito de um núcleo em expansão, com o crescimento da infra-estrutura de rede, ao passo que os domínios de utilizador aumentam em número, mas diminuem em tamanho.

b. Requisitos para capacidades

O propósito por detrás da criação de uma NII é permitir à organização militar executar operações militares com maior eficácia. De modo a apoiar melhor a evolução das operações militares, as funcionalidades do NINE deveriam ser baseadas nos requisitos das operações. No cenário de exequibilidade da NNEC foram estudados vários cenários respeitantes aos seus requisitos operacionais. Estes requisitos operacionais foram posteriormente decompostos em requisitos NII. Alguns destes requisitos podem ser utilizados para derivar pelo menos alguns dos requisitos do NINE.

Garantir a confidencialidade da informação em coligações

A função principal do NINE é garantir a confidencialidade da informação. No entanto, devido ao requisito operacional de ser capaz de partilhar informação com diferentes parceiros em operações combinadas, o NINE tem de ser capaz de providenciar a confidencialidade da informação em múltiplas situações. Um equipamento NINE deverá

deste modo ser capaz de garantir a confidencialidade da informação, não apenas entre domínios pertencentes à mesma entidade, mas também entre domínios heterogéneos pertencentes a entidades diferentes. Tal facto requer que o equipamento suporte múltiplos algoritmos de encriptação e tem outras implicações.

Suporte à convergência das redes

Através do requisito "suporte a operações expedicionárias" surge o requisito NII de suporte à convergência das redes, ou seja, suporte de múltiplas classes de tráfego, como voz, vídeo e dados, sobre a rede. O NINE também será afectado, pois os equipamentos serão componentes da rede que terão de lidar de forma correcta com a diferenciação do tráfego e de facilitar o fluir de serviços extremo-a-extremo geridos de modo a cumprir este requisito.

Uso eficaz da largura de banda

O NII deverá suportar operações militares de diferentes tipos, incluindo CROs. Dado que a largura de banda nesses cenários será normalmente limitada, o NII deverá ser capaz de utilizar eficazmente a largura de banda disponível. Isto inclui providenciar múltiplos níveis de precedência e preempção de modo a efectuar uma correcta prioritização de tráfego.

Suporte de ambientes federados dinâmicos

De modo a suportar ambientes dinâmicos a conectividade tem de ser não apenas pervasiva, mas também flexível. O suporte de ambientes dinâmicos tem de suportar a mobilidade dos utilizadores. Este apoio está ligado aos requisitos dos utilizadores, e pode ir da configuração automática dos sistemas quando estes se movimentam para outra localização e se voltam a ligar, até ao apoio de comunicações em movimento. De modo a atingir uma grande flexibilidade, os módulos individuais deveriam ser baseados num desenho modular. Por ex., uma rede classificada que inclua um equipamento NINE para garantir a confidencialidade da informação, seria um módulo individual. Desde que este módulo se mantenha o mesmo enquanto o utilizador de desloca, não importará onde este se irá ligar na rede de transporte. Para se ganhar flexibilidade adicional, o tamanho do módulo do utilizador deveria aumentar e a rede de transporte expandir-se. Esta é a ideia que está por detrás do princípio do "núcleo em expansão" presente no NNEC FS.

A razão por detrás do núcleo em expansão é que os domínios classificados são limitados na sua flexibilidade devido ao requisito da confidencialidade. No entanto, desde que todo o domínio seja tratado como uma única entidade, este deverá ser capaz de se movimentar consistentemente por toda a rede de transporte. Se a rede de transporte crescer

em direcção aos utilizadores, mais e menores domínios classificados irão aparecer, cada um deles capaz de se movimentar consistentemente na rede. Este facto aumenta a flexibilidade por intermédio de menores domínios de utilizadores e de um núcleo mais extenso. A Figura 30 demonstra o princípio de expansão do núcleo. Os módulos de utilizador multiplicam-se mas diminuem em tamanho à medida que o núcleo se expande. A protecção do núcleo é garantida com pontos de imposição de políticas no próprio núcleo. Esta expansão do núcleo deveria idealmente continuar até o domínio de utilizador ser um único equipamento, dando ao utilizador a máxima flexibilidade.

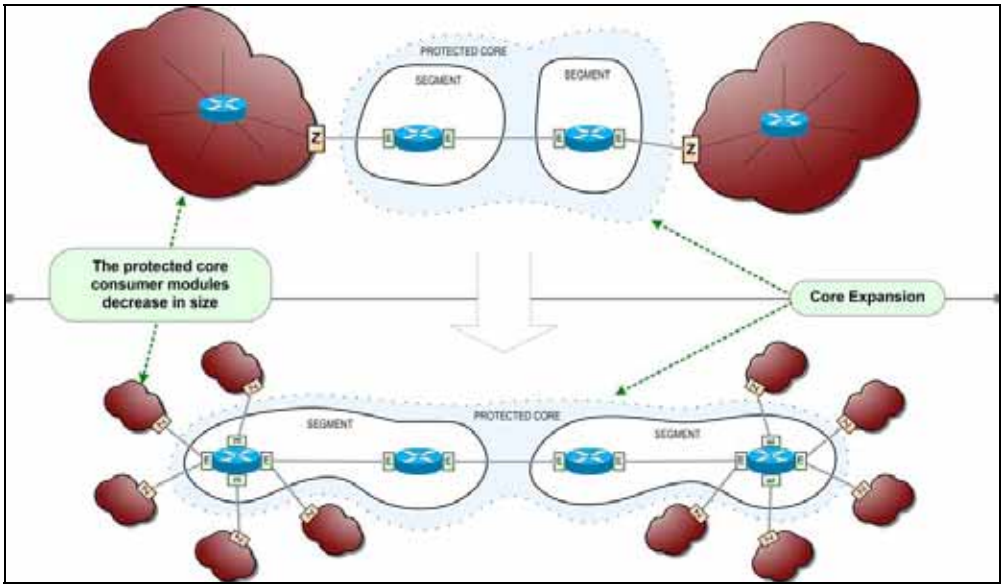

Figura 30- Expansão do núcleo

Para além do apoio a utilizadores móveis, a rede de transporte deve suportar mudanças dinâmicas e mesmo a mobilidade da própria rede, isto é, dos diferentes segmentos da rede de transporte. Tal deve-se à natureza das redes em ambiente combinado, onde cada nação participante é capaz de contribuir com parte da rede de transporte para o estabelecimento de uma infra-estrutura completamente funcional. A rede de transporte não deverá requerer mudanças de configuração manuais, pois tal facto vai contra o carácter dinâmico de operações onde existem mudanças nas nações participantes (e também dentro dos seus próprios sistemas nacionais).

Dado que a rede de transporte num ambiente NEC será constituída pelas contribuições das diferentes nações, a construção da mesma a rede tem ter presente a filosofia da federação de sistemas. Tal assegurará que a operação não depende de uma nação em particular, e que quaisquer nações que decidam participar numa coligação serão capazes de rapidamente estabelecer a rede de transporte. As nações serão depois capazes

de utilizar as redes umas das outras para aumentar ainda mais a flexibilidade, de acordo com os acordos apropriados estabelecidos entre elas. Todavia, de modo a garantir que os diferentes segmentos são interoperáveis, deverão ser utilizados interfaces comuns e não-proprietários.

Suportar PNR

O NINE tem de suportar as características fundamentais da PNR: Serviços diferenciados, gestão e controlo superiores, conhecimento superior, protecção superior e suporte de ambientes dinâmicos e federados.

c. Cenários

Podem ocorrer diferentes cenários para a implementação do NINE, os quais no fundo correspondem mais ou menos a diferentes níveis de maturidade.

Nível de maturidade 1 – Situação actual

A presente situação do SIC-T, com a utilização das TCE 621 pode ser encarada nível de maturidade 1. Este nível de maturidade é caracterizado por sistemas independentes desenhados e construídos em isolamento, não sendo por isso capazes de comunicar com outros sistemas. As soluções de segurança são efectuadas para um único sistema, o que não permite qualquer flexibilidade. A aplicação de cifra IP nesta situação é mostrada na fig. 31. Surgem desde logo vários problemas:

Em primeiro lugar, o encriptador IP (Z) apenas se liga a encriptadores IP exactamente iguais[74]. Ou seja, é pertença da mesma entidade de rede, suporta apenas um mesmo conjunto de algoritmos e não permite a passagem de qualquer outro tráfego. Esta realidade permite interconectividade entre redes homogéneas sob gestão comum e nada mais.

Em segundo lugar, o equipamento de cifra IP está rigidamente ligado ao lado classificado (*red* ou colorido) e não classificado (*black*) da rede. Mudanças à configuração em qualquer lado do encriptador IP requerem reconfigurações manuais do equipamento cripto

Em terceiro lugar, a WAN *black* é utilizada ou em *links* ponto-a-ponto ou numa rede nacional de pequena dimensão. Raramente consiste numa rede abrangente conjunta e combinada. Finalmente, a gestão da segurança e a gestão da rede estão separadas, e a gestão da rede dos próprios encriptadores IP é muito limitada. A própria gestão da rede é

[74] No caso das TCE 621, equipamentos com versões de *software* pertencentes a *major releases* diferentes não comunicam uns com os outros.

para além disso dificultada pelas diferentes classificações de segurança das redes *black* e *red*.

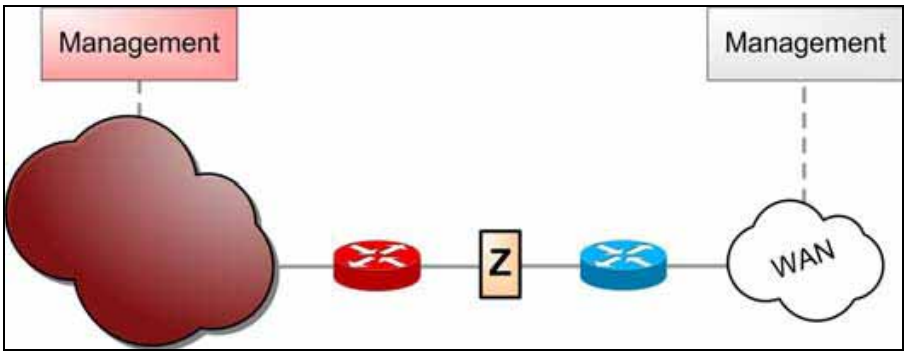

Figura 31 – Nível de Maturidade 1

Nível de maturidade 2 – Objectivo NINE

No nível de maturidade 2, o nível alvo para o NINE, pretende-se a interconexão entre redes heterogéneas com graus de classificação similares, p.ex. Nacional Secreto, NATO Secret e Mission Secret. A partilha de informação neste ponto é mais caracterizada pela coordenação e partilha de bases de dados do que pela introdução de serviços realmente integrados. A situação para o NINE neste nível de maturidade é diferente do nível de maturidade 1. Tal como é ilustrado na fig. 32, a estreita ligação entre o equipamento NINE e a nuvem colorida (classificada) foi reforçada e o NINE deverá idealmente deslocar-se sempre com a nuvem classificada. O ponto de ligação entre o equipamento NINE e a rede *black* (neste caso um NP) foi eliminado. A nuvem colorida, incluindo o equipamento NINE, pode movimentar-se livremente para qualquer localização ao longo do NP. À medida que o NP se expande e as redes coloridas diminuem de tamanhão, a flexibilidade do sistema como um todo aumenta, tal como foi previsto no NNEC FS. O NP será uma construção conjunta e combinada e os serviços prestados à rede colorida serão regulados por *Service Level Agreements* (SLAs).

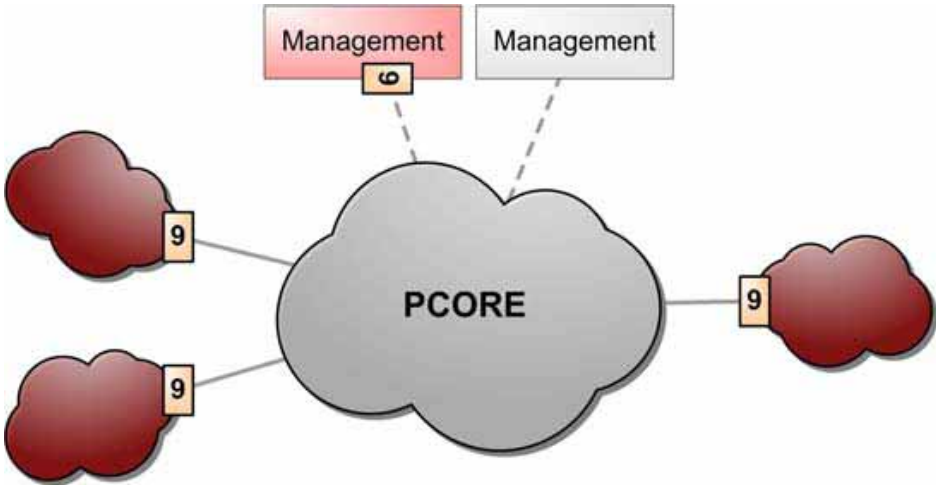

Figura 32 – Nível de maturidade 2

Para além disto, a gestão foi colocalizada e os equipamentos NINE providenciam funções de gestão de rede aos gestores do segmento NP e funções de gestão de segurança aos gestores do segmento colorido. A gestão de segurança e de rede dos equipamentos NINE será efectuada primariamente pelos proprietários do sistema, independentemente da localização do equipamento. Porém, os equipamentos NINE podem igualmente partilhar informação com o NP, para além da informação partilhada através dos próprios centros de gestão nacionais.

Nível de Maturidade 3 – Ambientes de Serviços

A característica principal no nível de maturidade 3 é a integração. Através de uma orientação baseada em serviços, as aplicações podem ser melhor integradas. Pretende-se integrar serviços existentes e não desenhar soluções específicas para cada operação. O nível de maturidade 3 é ilustrado na figura 33. Dos equipamentos NINE espera-se que garantam a confidencialidade da informação nesta situação; todavia, a partilha de informação é baseada primariamente em serviços. Tal facto tem implicações na forma em que o NINE filtra o tráfego de rede, pelo que este cenário ainda se afigura algo distante.

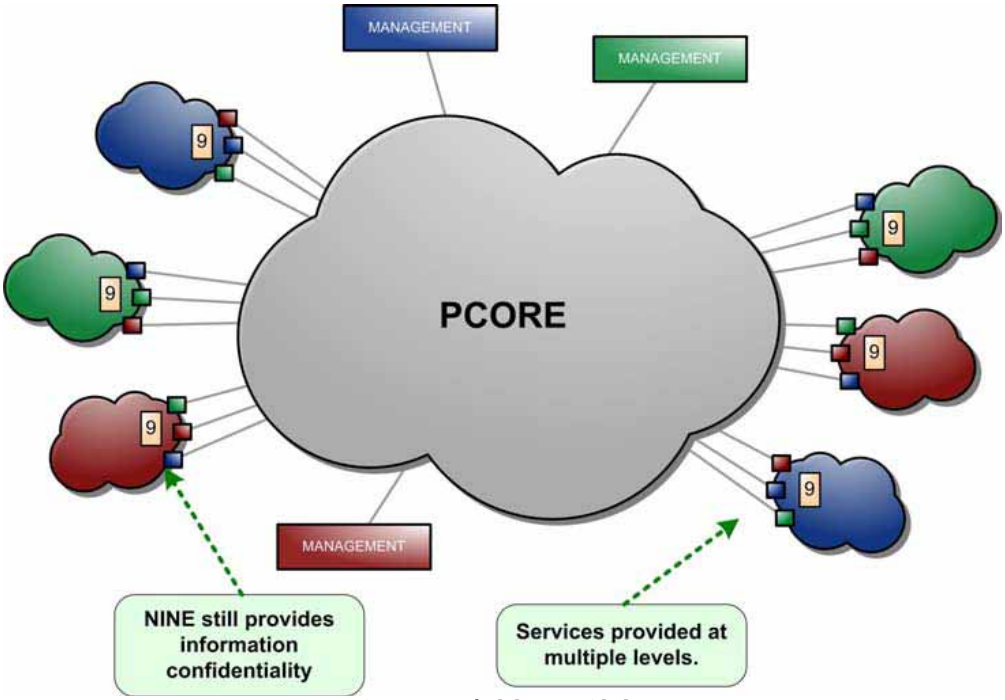

Figura 33 – Nível de maturidade 3

d. Modos de operação do NINE

Os equipamentos de cifra IP tradicionais foram desenhados para interoperar apenas com aparelhos iguais. Tanto o suporte de algoritmos como o de chaves é estático. Num ambiente conjunto e combinado, é importante ser capaz de partilhar informação com parceiros, mesmo se estes estão num grau de segurança superior. Um equipamento NINE pode ter de se ligar a diversos parceiros e deverá como tal ter de ser capaz de se ligar a esses mesmos parceiros. P.ex., um equipamento NINE poderá ser utilizado para garantir confidencialidade da informação entre dois domínios nacionais com grau de classificação semelhante[75].

Pode igualmente ser utilizado para garantir a confidencialidade da informação entre um domínio de uma nação e um domínio de outra nação, numa situação em que os parceiros confiem um no outro. Um exemplo é apresentado na figura 35. Relembre-se que os equipamentos NINE apenas garantem a confidencialidade da informação. O mecanismo de partilha da informação aplicado aos diferentes cenários depende da forma como as nações decidirem implementar a sua solução de partilha de informação.

[75] Tal como acontece actualmente na rede MMHS nacional.

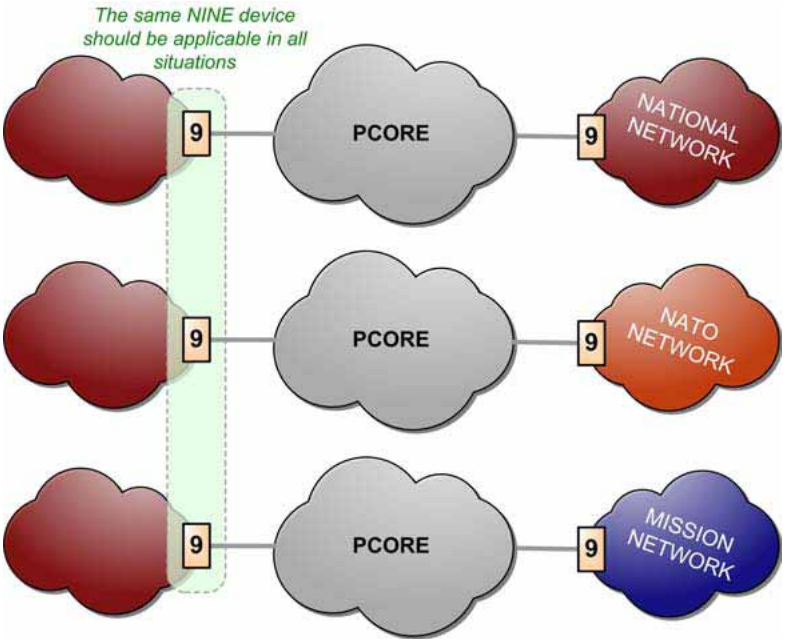

Figura 34 - Equipamento NINE utilizado para conexões em múltiplos cenários

APÊNDICE 4 - ARQUITECTURA DE SEGURANÇA EM REDES IP NATO

Ao nível da NATO, existe um número significativo de sistemas que armazenam, processam ou transmitem informação NATO, e que vão desde computadores *stand-alone*, passando por pequenas redes locais (LANs) e terminando em grandes e complexas redes do tipo WAN. (NC3B, 2006b:16)

A informação NATO, disponível num formato designado a permitir a sua rápida recolha, transmissão e utilização, pode ser vulnerável ao acesso por parte de utilizadores não identificados, à negação do acesso a utilizadores autorizados, e à corrupção, alteração e eliminação não autorizados. Para além disso, os complexos e por vezes não tão robustos equipamentos constituintes dos sistemas são caros e muitas vezes difíceis de reparar ou substituir rapidamente.

Os sistemas são alvos preferenciais para operações de recolha de informações, especialmente se as medidas de segurança forem consideradas ineficazes. Tais operações podem permitir a obtenção rápida e não detectada de grandes quantidades de informação. Qualquer operação executada por serviços de informações (ou organizações subversivas ou grupos terroristas), que tenha por alvo a NATO ou alguma das nações que dela fazem parte, será provavelmente bem planeada e bem executada. A perda de acesso aos sistemas por parte de utilizadores autorizados, ou a corrupção dos dados residentes nos sistemas pode igualmente ser um alvo atractivo, e não menos pernicioso à eficácia da NATO no cumprimento das suas missões, independentemente da classificação de segurança da informação em questão.

Os sistemas NATO que armazenem, processem ou transmitam informação classificada NATO CONFIDENCIAL e superior, ou informação de categoria especial, deverão operar num dos seguintes modos de operação de segurança[76]:

(1) Dedicado – Modo de operação no qual todos os indivíduos com acesso ao sistema possuem credenciação de segurança equivalente à mais elevada classificação de segurança da informação armazenada, processada ou transmitida pelo sistema, e em que todos necessitam de ter acesso a toda a informação armazenada, processada ou guardada pelo sistema;

[76] Em casos específicos, e durante períodos de tempo diferenciados, alguns sistemas podem funcionar em mais do que um modo de operação.

(2) *System high* - Modo de operação no qual todos os indivíduos com acesso ao sistema possuem credenciação de segurança equivalente à mais elevada classificação de segurança da informação armazenada, processada ou transmitida pelo sistema, mas onde nem todos os indivíduos com acesso ao sistema necessitam de ter acesso a toda a informação armazenada, processada ou guardada pelo sistema; a autorização para acesso à informação poderá ser concedida a um nível formal ou informal;

(3) Compartimentada – Modo de operação no qual todos os indivíduos com acesso ao sistema possuem credenciação de segurança equivalente à mais elevada classificação de segurança da informação armazenada, processada ou transmitida pelo sistema, mas onde nem todos os indivíduos com acesso ao sistema possuem uma autorização formal[77] para aceder a toda a informação armazenada, processada ou transmitida pelo sistema.

(4) Multi-nível - Modo de operação no qual nem todos os indivíduos com acesso ao sistema possuem credenciação de segurança equivalente à mais elevada classificação de segurança da informação armazenada, processada ou transmitida pelo sistema, e onde nem todos os indivíduos necessitam de ter acesso a toda a informação armazenada, processada ou guardada pelo sistema.

Sistemas NATO que armazenem, processem ou transmitam apenas informação NATO RESERVADO e/ou não-classificada deverão operar num dos seguintes modos de operação:

(1) Dedicado – Modo de operação no qual todos os indivíduos com acesso ao sistema necessitam de ter acesso a toda a informação armazenada, processada ou guardada pelo sistema;

(2) *System high* - Modo de operação no qual nem todos os indivíduos com acesso ao sistema necessitam de ter acesso a toda a informação armazenada, processada ou guardada pelo sistema[78].

A política de segurança da NATO define como objectivos de segurança a confidencialidade, a integridade e a disponibilidade. Para se atingir estes objectivos, deverão ser seguidos os seguintes princípios da segurança:

[77] A autorização formal indica a existência de uma gestão de controlo de acessos, por contraponto à discrição individual de um responsável em conceder acesso (autorização informal).

[78] Estas interpretações dos modos de operação demonstram que não é necessária uma credenciação de segurança para aceder a informação não classificada ou NATO reservado.

(1) Gestão do risco de segurança – para sistemas NATO, processos de gestão do risco de segurança serão aplicados para monitorizar, reduzir, eliminar, evitar e aceitar riscos;

(2) Minimalidade – apenas as funções, protocolos e serviços necessários ao cumprimento operacional da missão serão instalados e utilizados,

(3) Menor Privilégio – aos utilizadores do sistema serão apenas concedidos os privilégios e as autorizações necessárias para a execução das suas tarefas;

(4) Nó auto-protegido – um sistema não confiará noutros sistemas e implementará medidas de protecção para controlar a troca de informação com outros sistemas;

(5) Defesa em profundidade – medidas de protecção serão implementadas em vários componentes até onde for possível, de modo que não exista uma única linha de defesa;

(6) Verificação da Implementação de segurança – a aplicação destes princípios e a subsequente implantação de medidas de protecção será inicial e periodicamente verificada pelas autoridades de aprovação e acreditação da política de segurança.

No manuseamento de informação classificada NATO existem padrões mínimos de segurança que devem ser implementados de modo a que os princípios de segurança acima identificados sejam implementados. Estes padrões mínimos vêm expressos nas últimas versões da directiva de gestão INFO SEC para SIC e nas directivas técnicas e de implementação INFOSEC da NC3B (p.ex., a directiva de segurança para Computadores e LANs, a directiva para a interligação de SICs, e a directiva de ferramentas de segurança).

Educação e consciencialização acerca da segurança

Um factor primordial no alcançar de uma postura INFOSEC adequada consiste num programa activo de consciencialização e educação acerca da segurança para todo o pessoal técnico e utilizadores do sistema. Para garantir que as responsabilidades de segurança são correctamente compreendidas, deverão ser educados e sensibilizados para a problemática da INFOSEC toda a gestão de topo, os planeadores do sistema, o pessoal envolvido na gestão do sistema, e os utilizadores. O pessoal afecto ao sistema e os utilizadores deverão cumprir as Security Operating Procedures (SecOPs) adequadas.

Interligação de SICs

A política de segurança da NATO requer medidas que controlem a ligação de SICs que processem informação classificada NATO. A directiva de gestão de INFOSEC define os requisitos de aprovação ou acreditação e as directivas técnicas e de implementação INFOSEC definem as medidas a serem implementadas.

Ligação de SICs NATO à Internet ou a redes similares do domínio público

Os SICs NATO podem utilizar a Internet ou redes similares do domínio público numa perspectiva de rede de transporte (e não na perspectiva normal de utilização das mesmas), desde que seja implementada protecção criptográfica apropriada. A utilização da Internet deverá ser seriamente considerada tendo em vista o objectivo de segurança "disponibilidade".

O requisito de medidas protectoras para SICs NATO ligados à Internet ou a redes similares no domínio público advém dos extraordinários riscos de segurança levantados por este tipo de redes públicas devido à sua acessibilidade à escala global, e à possibilidade de exploração por partes terceiras das inerentes vulnerabilidades do conjunto de protocolos IPv4 e da generalidade dos sistemas operativos dos terminais. Neste caso, é assim mandatório que os SICs NATO, bem como os dados neles guardados e processados, sejam especificamente protegidos para não ficarem numa situação de risco inaceitável.

A ligação de SICs NATO que armazenem, processem ou transmitam informação NATO UNCLASSIFIED/NATO RESTRICTED, à Internet ou redes similares no domínio público será controlada para proteger o SIC NATO de acessos externos ou modificações não autorizadas, e para prevenir que informação transmitida seja ilicitamente lida ou modificada. Este controlo deverá ser feito respeitando os requisitos espelhados na última versão da "*NC3B INFOSEC Technical & Implementation Directive for the Interconnection of CIS*" (AC/322-D/0030).

Quando um SIC NATO que armazene, processe ou transmita informação NATO UNCLASSIFIED, e que esteja ligado à Internet ou redes similares no domínio público, se ligar a um SIC NATO que armazene, processe ou transmita informação NATO RESTRICTED, então a conectividade entre ambos deverá estar de acordo com os requisitos de interligação necessários para transmissão de informação NATO RESTRICTED para a Internet.

Quando um SIC NATO que armazene, processe ou transmita informação NATO UNCLASSIFIED/NATO RESTRICTED, e que esteja ligado à Internet ou redes similares no domínio público, se ligar a um SIC NATO que armazene, processe ou transmita informação NATO CONFIDENTIAL/NATO SECRET, então a conectividade a este último será estritamente controlada, será sujeita aos requisitos da aprovação de segurança apropriada, será sujeita a avaliação e certificação por uma agência/autoridade nacional ou NATO, e será sujeita a avaliações de vulnerabilidades periódicas (*Section VII, INFOSEC Management Directive for CIS*).

A ligação de um SIC NATO que armazene, processe ou transmita informação NATO CONFIDENTIAL/NATO SECRET à Internet ou redes similares no domínio público, será sujeita aos requisitos da aprovação de segurança apropriada, será sujeita a avaliação e certificação por uma agência/autoridade nacional ou NATO, e será sujeita a avaliações de vulnerabilidades periódicas (*Section VII, INFOSEC Management Directive for CIS*).

É proibida ligação directa ou em cascata de SICs NATO que armazenem, processem ou transmitam informação com a classificação COSMIC TOP SECRET, à Internet ou redes similares no domínio público.

Os princípios de gestão do risco de segurança, minimalismo, nós auto-protegidos e defesa em profundidade serão aplicados nas ligações dos SICs NATO à Internet ou redes similares no domínio público.

A ligação de SICs nacionais que armazenem, processem ou transmitam informação NATO à Internet ou redes similares no domínio público está sujeita aos regulamentos e regras de segurança nacionais apropriados.

A única informação que pode ser transmitida em claro é a seguinte:

(a) Informação pública e *open source*, ou informação NATO especificamente aprovada para divulgação pública;

(b) Informação NATO UNCLASSIFIED não-sensível.

Apenas informação pública e *open source* ou informação NATO especificamente aprovada para divulgação pública, poderá ser colocada em sítios ou páginas Web, sendo no entanto sujeita aos requisitos de integridade do(s) originador(es) da informação.

Para todas as ligações de SICs NATO ao domínio da Internet ou redes semelhantes no domínio público, os seguintes pontos serão sujeitos à aprovação da autoridade de segurança ou acreditação:

(a) Método de ligação e serviços disponibilizados;

(b) Análise do risco de segurança e metodologia de gestão do risco a ser utilizada, e os resultados da análise do risco de segurança;

(c) Procedimentos e mecanismos para assegurar que a informação classificada NATO, ou NATO UNCLASSIFIED de disseminação limitada, não é transmitida sobre meios de comunicação não protegidos;

(d) Procedimentos e/ou mecanismos para assegurar a confidencialidade, integridade e/ou disponibilidade da informação, bem como dos serviços/recursos da estrutura de apoio;

(e) Procedimentos e/ou mecanismos para ir de encontro aos requisitos de pretação de contas;

(f) Documentação relacionada com a segurança, incluindo o plano de testes de segurança e os resultados dos testes de segurança.

A autoridade de acreditação será responsável pela implementação inicial de segurança e por verificações periódicas posteriores.

APÊNDICE 5 - FUNCIONAMENTO DE UMA INFRA-ESTRUTURA PKI

As Infra-estruturas de Chaves Públicas, ou Public Key Infrastructures (PKI) na terminologia anglo-saxónica, constituem sistemas de certificação electrónica que conjugam um conjunto de procedimentos e normas, legislação e infra-estrutura tecnológica, recorrendo a técnicas de criptografia assimétrica, com o objectivo de proporcionar ambientes de segurança electrónica. As Infra-estruturas de Chaves Públicas proporcionam mecanismos de autenticação digital forte de identidades e assinaturas, bem como a confidencialidade e o não repúdio nas transacções e comunicações electrónicas. A implementação de PKI tem sido extensiva a projectos alargados no domínio da segurança electrónica de redes distribuídas, com aplicações diversas no domínio dos serviços do Governo electrónico e da Sociedade da Informação (SCEE, 2008).

Uma PKI é um órgão ou iniciativa que tem como objectivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de acreditação e confiança em transacções entre partes que utilizam certificados digitais. A principal função da PKI é definir um conjunto de técnicas, práticas e procedimentos a serem adoptados pelas entidades a fim de estabelecer um sistema de certificação digital baseado em chaves públicas. Para assegurar que uma determinada chave pertence a um dado utilizador é necessário que uma Autoridade Certificadora (AC) confira a sua identidade e os seus respectivos dados. Ela será a entidade responsável pela emissão, suspensão, renovação ou revogação de seu certificado digital, além de ser obrigada a manter sempre disponível a Lista de Certificados Revogados (CRL).

O pessoal, programas e sistemas que executam ou apoiam as missões da NATO necessitam de um largo espectro de serviços de segurança para uma grande quantidade de aplicações. Estas últimas incluem o *messaging*, encriptação de ficheiros, transferência de ficheiros, transacções de bases de dados, acessos a servidores Web e quaisquer outras aplicações que requeiram certificados ou chaves (na modalidade chave pública/chave privada). Os serviços de segurança para essas aplicações baseiam-se num conjunto de componentes de segurança que incluem computadores, guardas, *firewalls*, *routers*, *software* aplicacional e servidores de bases de dados acreditados. Tal como é definido na *NPKI Reference Architecture*, uma infra-estrutura de chaves pública deverá providenciar no mínimo as seguintes funções (NC3B, 2006a:1-6):

(1) Gestão de certificados de identidade e chaves privadas, utilizadas para assinatura digital e para providenciar identificação e autenticação;

(2) Para utilizadores que necessitem, gestão de certificados de estabelecimento de certificados e chaves privadas, incluindo a recuperação de chaves privadas de entidades chave.

(3) As correspondentes funções de gestão de chaves públicas, tal como a re-emissão, validação, revogação, e manutenção da pretação de contas das chaves.

A PKI deverá suportar algoritmos criptográficos de chaves públicas para a criação e certificação de pares de chaves públicas/privadas, para a aplicação de assinaturas digitais para certificados ou para executar o estabelecimento de sessões autenticadas. Dado o actual ritmo de progressão da capacidade de análise criptográfica, o tamanho das chaves deverá aumentar e algoritmos menos complexos deverão ser substituídos por outros mais robustos.

É recomendado pela NATO o uso de algoritmos do domínio público em apoio de serviços de segurança seleccionados. Esta utilização de algoritmos padrão simplifica significativamente o desenvolvimento e implementação da PKI, contribuindo para o objectivo de interoperabilidade entre parceiros de comunicação. A utilização de um dado algoritmo depende de vários factores. Estes factores incluem os atributos do SIC bem como as funções geradoras de um qualquer algoritmo de cifra. Considera-se que quando se aborda a infra-estrutura criptográfica, deverá ser seguida a *INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms*, a qual basicamente estipula a proporcionalidade entre a força do algoritmo de cifra necessário e a avaliação do risco. Esta avaliação do risco deverá fazer uma distinção entre redes não-confiáveis (como a Internet) e redes confiáveis (como a Rede de Dados do Exército, a intranet da Defesa, a NATO Secret WAN, etc.). Assume-se igualmente que onde uma PKI suporte um SIC NATO CONFIDENTIAL ou de classificação de segurança superior, exista uma capacidade de encriptação das comunicações aprovada que providencie os serviços de confidencialidade necessários.

APÊNDICE 6 – O CONCEITO LANDWARNET DO EXÉRCITO DOS EUA

No final de 2003, o Comando Superior do Exército dos EUA debruçou-se sobre as lições aprendidas nas operações *Enduring Freedom* e *Iraqi Freedom* e convocou um comité para decidir quais seriam os facilitadores conjuntos (*enabler*s) de C2, informações e apoio de combate e serviços necessários para fortalecer o novo exército modular e a que nível o Exército poderia atribuir meios a esses facilitadores. Foi assim aprovado o conceito *Barebones (+)*[79], o qual designa a articulação, constituição e grau de profundidade das capacidades de comunicações e comando de batalha. As melhorias sobre sistemas de C2 actuais incluem:

(1) **Maior largura de banda**. Graças a uma maior largura de banda para as comunicações, serão disponibilizados serviços previamente não disponíveis aos centros de operações tácticos das BCT Estes incluem telefonia IP, vídeo teleconferência e ferramentas colaborativas gráficas de planeamento.

(1) **Conectividade conjunta**. O CMDT da BCT ganha igualmente ferramentas essenciais para a operação no ambiente conjunto: correio electrónico classificado e não-classificado, bem como acesso à informação disponível nas redes classificadas e não classificadas do DoD.

(2) **Comando da batalha em movimento (BCOTM – *Battle Command on the Move*)**. Esta capacidade baseada no segmento espacial (rede de satélites) fornece ao CMDT os sistemas de comunicações e comando da batalha necessários para o C2 da BCT em movimento, permitindo-lhe aceder a toda a informação residente no seu PC a partir de qualquer ponto do campo de batalha. O sistema BCOTM inclui um subsistema ABCS montado num veículo e ligado a sistemas de comunicações satélites móveis e estacionários.

(3) ***Force XXI Battle Command Brigade and Below* (FBCB2)**. O FBCB2 garante *situational awareness* quase em tempo real e capacidade C2 aos escalões tácticos mais baixos. Facilita o fluxo de informação de comando de batalha através do espaço de batalha, e interopera com sistemas de informação do escalão superior, tais como o sistema de controlo de manobra (MCS).[80] O resultado é uma integração

[79] Que se traduz por esqueleto+
[80] *Maneuver Control System.*

horizontal e vertical da informação de comando da batalha por todo o espaço de batalha digital e dentro dos escalões tácticos BCTs e inferiores.

(4) ***Blue Force Tracker* (BFT)**. O BFT é um sistema de informação táctica que liga via satélite combatentes, veículos, aeronaves e sensores de modo a formar uma imagem digital da localização das unidades amigas no campo de batalha. Unidades e veículos equipados com o BFT podem acompanhar a sua própria localização e das outras forças amigas, bem como ver a topografia do campo de batalha. O BFT consiste num sistema de comunicações satélite móvel ligado a uma plataforma FBCB2. (FMI-6.02.50, 2005, p. 10.6)

A actual doutrina SIC do Exército Norte-Americano está centrada no conceito LandWarNet (LWN). LWN é basicamente o nome atribuído ao conjunto de **todas** as redes do Exército, englobando quer as redes da componente "territorial" quer as das unidades projectadas ou envolvidas em operações. É a contribuição do Exército para a *Global Information Grid* (GIG), e que consiste no conjunto interligado extremo-a-extremo das capacidades informacionais, processos associados e pessoal, necessárias à aquisição, processamento, armazenagem, transporte, controlo, protecção, disseminação e apresentação da informação, para apoiar os combatentes, os decisores e o pessoal de apoio. Engloba todos os serviços e sistemas de comunicações e informáticos proprietários ou alugados, o *software* (incluindo aplicações), serviços de COMSEC e outros serviços associados. A LWN compreende igualmente o conjunto de capacidades informacionais extremo-a-extremo que permite ao Exército dos EUA participar em ambientes conjuntos e combinados. (FMI-6.02.50, 2005, p. 1.2)

A LWN é essencialmente a combinação do conjunto de aplicações funcionais (destinadas ao C2, Informações, Apoio Logístico, etc.), transmitidas sobre uma rede de transporte integrada (compreendendo os segmentos espacial, aéreo e terrestre, as infra-estruturas fixas, e os terminais de rede), que utilizam um conjunto comum de serviços de rede (voz, dados, vídeo, colaboração, armazenamento, descoberta, *messaging*, velocidade de serviço, qualidade de serviço, *hosting*, segurança da informação, NETOPS, garantia da informação, gestão da disseminação da informação e gestão de redes).

Existem cinco imperativos LWN que têm de ser realizados para serem atingidas as novas capacidades conjuntas e expedicionárias do exército Americano "modular". Estes imperativos representam os fundamentos da LandWarNet e abordam a linha base de equipamentos e tecnologia, o modo de emprego dessa linha base, o modo como ela será

organizada e inserida em rede, os recursos que lhe serão atribuídos e a maneira como ela será controlada. Estes imperativos LandWarNet irão concretizar a visão do Exército Americano de organizar rapidamente unidades tarefa modulares, de projectar e empregar simultaneamente essas forças a partir de múltiplas plataformas de projecção, todas com a capacidade de combater à chegada, e com a capacidade de conjugar todas as capacidades conjuntas para combater e ganhar. Resumindo cada um dos imperativos:

(1) **Interoperabilidade Técnica Conjunta (JTI)**: Configurações técnicas de equipamentos, opções de *hardware*, padrões e protocolos conjuntos implementadas numa arquitectura conjunta, associada ao desenvolvimento, instalação, operação, manutenção e defesa dos sistemas de comunicações LandWarNet que dotarão o Exército dos EUA de capacidades expedicionárias e conjuntas.

(2) **Interoperabilidade Operacional Conjunta (JOI)**: Tácticas, técnicas e procedimentos (TTP), conceitos e processos conjuntos associados ao desenvolvimento, instalação, operação, manutenção, defesa e NETOPS dos sistemas de comunicações LandWarNet que dotarão o Exército dos EUA de capacidades expedicionárias e conjuntas.

(3) **Arquitectura LandWarNet e *Director of Combat Development* (DCD) Construct**: Uma estrutura única que congrega várias organizações numa Empresa de DCD e de desenvolvimento arquitectural unificada.

(4) **Estratégia de investimento LandWarNet**: Sincronização de requisitos e prioritização para investimentos LandWarNet, de acordo com a JTI.

(5) **LandWarNet NETOPS**: Uma estrutura abrangendo todo o Exército dos EUA e que faz parte das operações de rede (NETOPS) conjuntas, e que exerce o controlo da LandWarNet, respondendo ao *Regional Component Command* (RCC).

O potencial da estrutura modular não será alcançado se não se alcançarem estes imperativos. A modularidade é dependente da interoperabilidade. A interoperabilidade é dependente da LandWarNet e a LandWarNet depende destes imperativos.

A realização da LWN tem como resultado um Exército mais integrado digitalmente. Melhora a conectividade entre sensores, decisores e atiradores e sistemas de armas, contribuindo cabalmente para o conceito da NCW. Apoia a sincronização entre CMDTs, Estados-Maiores e órgãos de apoio de modo a agilizar os ciclos de decisão e melhorar a eficácia do comando em situações de combate. Fornece ligação ao território nacional e reduz o apoio logístico projectado necessário ao Soldado, aumentando a

mobilidade, agilidade e capacidade de sustentação. Fornece adicionalmente uma capacidade de terminal de rede robusto e protegido, permite o treino descentralizado a partir da *home station*, planeamento colaborativo e treino da missão, apoio à projecção e apoio operacional ao combatente projectado a partir do território nacional. (FMI-6.02.50, 2005, p. 1.3)

APÊNDICE 7 – RESPONSABILIDADE PARA ESTABELECIMENTO DE COMUNICAÇÕES

A responsabilidade para estabelecimento de comunicações é definida da seguinte maneira: (RC-OPERAÇÕES, 2007: III.2.45):

(a) Do escalão superior para o inferior;

(b) Da esquerda para a direita;

(c) Da unidade que apoia para a unidade apoiada.

A ligação deve, quando possível, ser recíproca entre o escalão superior, subordinado e adjacentes. A ligação é **recíproca** quando:

(a) Uma força é colocada sob o comando ou controlo de um quartel-general de nacionalidade diferente;

(b) Entre unidades de escalão brigada e superior de nacionalidades diferentes quando são adjacentes.

Quando a ligação **não é recíproca**, a responsabilidade para o seu estabelecimento respeita os seguintes princípios:

(a) Da esquerda para a direita;

(b) Da retaguarda para a frente, entre unidades do mesmo escalão;

(c) Do escalão mais elevado para o escalão mais baixo;

(d) Da unidade que apoia para a unidade apoiada;

(e) Da força que efectua a entrada em posição para a força que retira durante a substituição de tropas de combate; da força que retira (passa para a retaguarda) para a força que está em posição (estática) durante a passagem de linha para a retaguarda.

APÊNDICE 8 – POSSIBILIDADES DAS CTM DA FOPE

As CTm das Brigadas da FOPE têm como missão "instalar e manter o sistema de informação e comunicações táctico, necessário ao exercício do comando e controlo da Brigada" (QOP CTm BrigRR, 2006:1). As suas possibilidades são as seguintes:

(1) Assegurar o funcionamento do sistema de informação e comunicações táctico, necessário ao exercício do comando e controlo da Brigada;

(2) Garantir o apoio a todas as Unidades que transitem pela Área de Apoio da Companhia;

(3) Montar quatro Nós de Trânsito como principal elemento de transporte;

(4) Apoiar em comunicações três postos de comando, instalando três sistemas de área local;

(5) Montar seis Pontos de Acesso Rádio para apoio e cobertura da sua Área de Responsabilidade (AOR).

A CTmApoio, que integra o lote Unidades de Apoio Geral, tem como missão "garantir a ligação às Forças Nacionais Destacadas e o Apoio Adicional em comunicações a uma Brigada". (QOP CTmAp, 2005: 1) Tem as seguintes possibilidades:

(1) Garantir a ligação a todas as forças do Sistema de Forças Nacional que não disponham de Unidade de apoio de comunicações;

(2) Garantir apoio adicional em comunicações quando a sua AOR for superior ao normal;

(3) Reforçar com a totalidade ou parte dos seus meios a Brigada de Reacção Rápida (BrigRR) quando esta se constitua no núcleo de um Battle Group;

(4) Apoiar em comunicações o Sistema Nacional de Protecção Civil (SNPC), em situações de catástrofe;

(5) Fornecer Módulos de Apoio de Comunicações a Forças Nacionais Destacadas, quando necessário, garantindo ainda o *rear link*.

APÊNDICE 9 – POSSÍVEIS CENÁRIOS DE INTEROPERABILIDADE E MOBILIDADE NO SIC-T

Várias circunstâncias podem obrigar à mudança da topologia da estrutura de comunicações durante a operação. Os PCs das brigadas e das suas subunidades necessitam de mudar a sua localização periodicamente e, nessa altura, as suas ligações ao SAE mudarão também, de um nó para outro numa localização diferente (ver fig. 24). O movimento do PC pode acontecer de vários modos, implicando diferentes conexões, e problemas de interoperabilidade para cada um dos cenários: (DST, 2003: 23-26)

(a) Mover o PC por fases. Um grupo mantém a funcionalidade do PC no antigo lugar, enquanto outro se move para a nova localização;

(b) Mover todo o PC, sem reter qualquer funcionalidade na antiga localização;

(c) Mover o PC por duplicação de algumas ou de todas as células, de forma a manter a operacionalidade em permanência;

Com a introdução do SIC-T, garante-se igualmente uma muito maior mobilidade e interoperabilidade dos utilizadores do SIC-T. Nos casos onde um utilizador altera a sua ligação á rede, o que inclui sobretudo a situação de um terminal de utilizador do Sistema de Utilizadores Móvel, através da CNR, todos os serviços disponibilizados (voz, mensagens, dados, etc.) continuam a ser garantidos depois da mudança.

A **mobilidade do assinante** refere-se ao movimento de um assinante para um terminal diferente, que pode estar localizado em qualquer dos subsistemas SAL, SAE ou SUM. Um assinante deverá poder reafiliar-se a um novo ponto de acesso dentro do sistema, e utilizar o terminal que aí estiver disponível, independentemente da localização do anterior terminal, mantendo o seu perfil de acesso (ver fig. 25). Se não for possível satisfazer este requisito, ao nível do SGR será resolvido o problema da afiliação deste utilizador na rede, inclusive da possibilidade ou não da sua realização. Ou seja, cada assinante possui um número telefónico, um endereço de e-mail, um nome de utilizador e um perfil de acesso únicos que transporta consigo, e que são válidos em qualquer localização do espaço de batalha. Esta caracterização é feita com base na função orgânica de cada assinante (p. ex. CMDT, G1, G2, etc.).

A **mobilidade do terminal**, refere-se ao movimento de um utilizador juntamente com o seu terminal, de um ponto de acesso da rede para outro. No SIC-T, um assinante deve ser capaz de ligar o seu terminal a um novo ponto de acesso em qualquer circunstância, e em consequência, deverá ser capaz de se reafiliar de novo e manter o seu perfil de acesso (ver fig. 26).

Em ambos os casos, mesmo que o utilizador se mova entre sub-redes SAL, pertencente ao SIC-T, poderão ocorrer problemas de interoperabilidade se as sub-redes do SAL estiverem ligadas a um SAE de outra nação.

Outra possibilidade é a movimentação de um utilizador móvel do SIC-T através do TO, com interligação pelo SUM. Quando este se movimenta de uma área coberta por um PAR, para a área de cobertura de outro PAR, não deverá ocorrer nenhuma redução na qualidade do serviço proporcionada. Esta transferência de ligação poder-se-á processar de várias maneiras: de uma forma automática quando a ligação se degrada abaixo de um determinado nível (como acontece nas operadoras móveis civis); de uma forma manual iniciada pelo SGR; ou de uma forma manual iniciada pelo operador do terminal móvel (ver fig. 27).

APÊNDICE 10 – SERVIÇOS DISPONIBILIZADOS NOS DIFERENTES DOMÍNIOS DE REDE

Domínio **NATO SECRET** – É disponibilizado o acesso aos serviços e aplicações que correm sobre a NSWAN. Designadamente, aos ICC, MCCIS, BICES, ADAMS, LOCE, VTC, JCOP[81], ACCS1, Mensagens Militares da NATO e outros a considerar;

Domínio **Nacional Secreto** - É disponibilizado o acesso aos seguintes serviços e sistemas: serviço de mensagens militares formais (ex: MMHS), mensagens não formais – e-mail seguro (ex: Outlook), WISE, VoIP, SICCOC (baseado num modelo de dados JC3IEDM - STANAG 5525), GEOMETOC, VTC (incluindo Mensagens Instantâneas), *chat*; poderão ser adicionados outros serviços e sistemas considerados convenientes.

Domínio **Mission Secret** - É disponibilizado o acesso aos serviços e sistemas que forem considerados necessários para cada missão específica, dentro do leque de serviços referidos nos dois domínios anteriores.

Domínio **Rede Administrativa** - Disponibiliza os serviços e funcionalidades actualmente existentes na Intranet da Defesa.

[81] Quando disponível

APÊNDICE 11 - PROPOSTA DE ARQUITECTURA DE SEGURANÇA DE REDE PARA O SIC-T

A proposta para a infra-estrutura de segurança de rede para o SIC-T baseia-se nos princípios da defesa em profundidade e de nó auto-protegido. O princípio de nó auto-protegido baseia-se no conceito de que um nó de rede (ou seja um módulo) é responsável por se proteger a si próprio de ameaças externas utilizando um *boundary protection service* (BPS) como mostrado na figura 35. No mínimo, o BPS para um módulo de rede do SIC-T deveria consistir numa *firewall* e num sensor IDS[82] como mostrado na figura 35. Deveria igualmente ser colocado um sensor IDS adicional atrás da *firewall* sempre que possível.

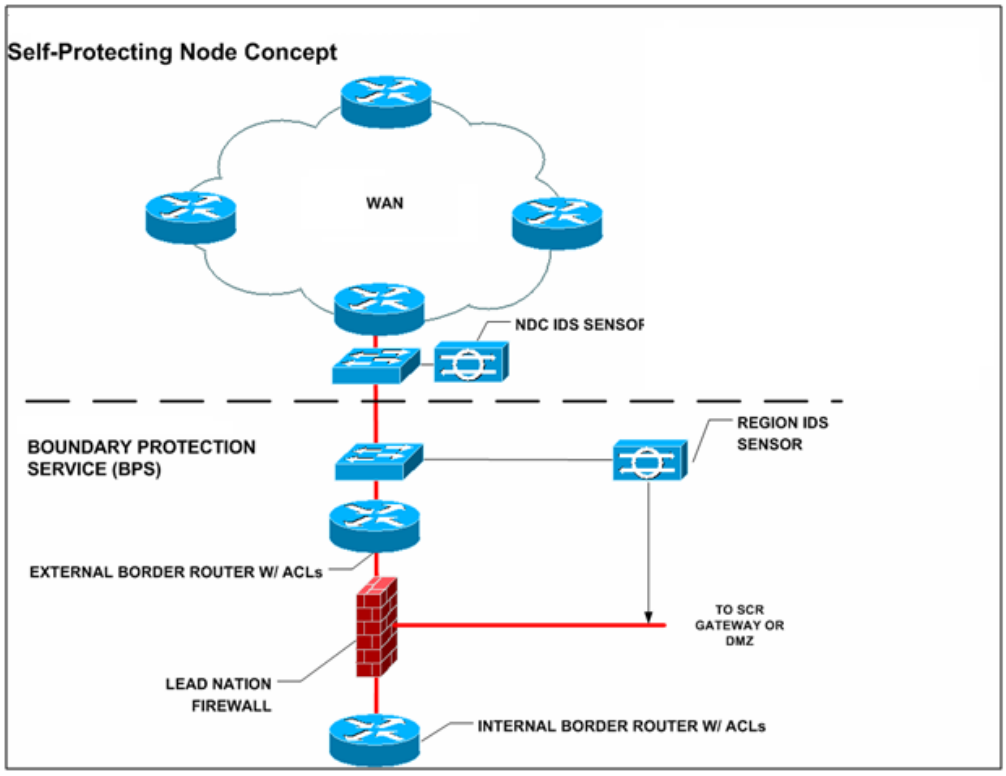

Figura 35 - Princípio de nó auto-protegido

A ameaça às redes do SIC-T é complexa e cobre um largo espectro de potenciais fontes: a interligação com outros sistemas similares (nacionais ou aliados) e a consequente

[82] IDS: *Intrusion and Detection System*

interacção com os mesmos, *malware*[83] introduzido por utilizadores do sistema ou sistemas infectados e acções de CNA inimigas, entre outras. Tendo em vista que as vulnerabilidades podem ocorrer a diferentes níveis no SIC, o princípio da defesa em profundidade pretende estabelecer uma postura de IA adequada, num ambiente de risco partilhado através da integração do pessoal, tecnologia e operações. Torna-se assim óbvio que o acesso físico a equipamentos IP (tais como portáteis, telefones VoIP, *routers*, etc.) deverá ser restringido e controlado.

Esta aproximação de segurança é uma combinação balanceada de medidas físicas, procedimentais, organizacionais e técnicas. Apesar de se considerar desejável a existência de uma estrutura segurança multinível, tudo parece apontar que se avance para uma implementação do tipo *system high*. Isto acontece, porque a gestão de segurança multinível se configura ainda como sendo demasiado complexa. (CISCO, 2006). Acresce ainda que actualmente não existem sistemas cripto certificados pela NATO que suportem segurança multinível.

[83] Software destinado a infiltrar-se em sistemas de computadores alheios de forma ilícita, com o intuito de causar algum dano ou roubo de informação.

- **TOP LEVEL ARCHITECTURE**

- **TACOMS Subsystems**

1. The architecture comprises four subsystems:

    a. The Local Area Subsystem (LAS)

    b. The Wide Area Subsystem (WAS)

    c. The Mobile Subsystem (MS)

    d. The System Management and Control Subsystem (SMCS).

1. The LAS provides access to communication services to users in Headquarters and Command Posts (CPs). These range from the main multinational HQ Land Component Command (LCC) of a Combined Joint Task Force (CJTF) or High Readiness Force HRF-HQ to a national Battle Group (BG) or Battalion Command Posts (CP). The LAS will support both narrowband and wideband user access and services. The LAS access, which may serve individual vehicles or small groups of vehicles, will be connected together within the Headquarters by a high capacity LAS backbone. The LAS Backbone will provide connections out of the Headquarters to the WAS and the MS.
2. The WAS serves to interconnect LAS nodes serving HQs and Command Posts, MS nodes and external networks such as public, private and military strategic and legacy (non-TACOMS) tactical networks. The WAS consists of WAS nodes interconnected by transmission links. The WAS will have different error and propagation characteristics dependent of the technology being used (SATCOM, UHF/ microwave radio relay etc.). While LAS nodes are co-located with the command posts, WAS nodes are deployed in locations most suitable for the purpose of the interconnection.
3. The MS offers communication services to the mobile users using wireless access. The MS user groups are not homogeneous and will comprise manoeuvre units, combat support units (fire support, air defence) and combat service support units (logistics, medical, military police and personnel). The Mobile Subsystem is made up entirely of radio networks that are characterised by bandwidth and error rate limitations due to typical operating frequencies in the HF, VHF and UHF bands. The MS may consist of different types of national radio networks used to connect mobile users such as Single Channel Radio Access (SCRA), Combat Net Radio (CNR), Narrow-Band Packet Radio (NBPR) and Broad-Band Radio (BBR).
4. The SMCS provides the planning, monitoring and control functions to the other three TACOMS subsystems (LAS, WAS, MS). It is distributed across the network and therefore relies on the other subsystems to provide a reliable data communications service for the transfer of management information between the SMCS entities. The SMCS is required to operate effectively in a tactical environment and so must be designed to adapt effectively to the high mobility of a tactical network and to unplanned changes in network topology. It has a modular structure in order to be adaptable to the size of the managed network.

- **TACOMS Network Elements**

2. The Network Elements (NE) are the building blocks of the TACOMS subsystems, as shown in Figure 2-3. Each NE is provided by a single nation. The following types of NEs are defined and standardised for each subsystem.

5. The NEs belonging to the LAS subsystem are:

    LAS backbone NE: This element provides access to local users and connects to other LAS elements and to the WAS or MS. It is typically used to connect a multinational HQ to the WAS, or a national HQ to another national HQ.

LAS access NE: This element provides access to local users and connects to a LAS backbone NE. It will typically serve a national part of a multinational HQ.

6. The NE belonging to the WAS subsystem is:

   WAS NE: The WAS NE is a set (or subnet) of interconnected WAS switching and transmission equipment deployed by one nation. All equipment necessary for the WAS to provide the defined services in terms of QoS and capacity, are included in the WAS NE. A number of WAS NEs, each covering a typical geographical area, are interconnected to form a WAS subsystem.

7. The NEs belonging to the MS subsystem are:

   Radio Access Point Network (RAPNET) NE is a MS element with connections to the WAS/LAS subsystems and to other MS NEs. A RAPNET NE is made of a common radio equipment called Radio Access Point (RAP), and remote radio-equipment linked to it by over-the-air (not standardised by TACOMS) connections. A RAPNET NE may be composed of various types of radio sub-networks, either SCRA, CNR, NBPR or BBR and provides access to wireless users.

   Packet Radio Network (PNET) NE is a MS element composed of packet radios interconnected by nationally defined over-the-air interface. A PNET is connected to a RAPNET or another PNET. A PNET NE may be composed of various types of radio sub-networks, either CNR (in packet mode), NBPR or BBR (in packet mode) and provides access to wireless users.

   Circuit Radio Network (CNET) NE is a MS element composed of radios working in circuit mode interconnected by nationally defined over-the-air interface. A CNET is connected to a RAPNET or another CNET. A CNET NE may be composed of various types of radio sub-networks, either CNR or BBR (in circuit mode) and provides access to wireless users.

- **TACOMS Interfaces**

3. TACOMS NEs provide interfaces that are standardised with complete physical, link and network layer protocols, to ensure multinational interoperability, in STANAG 4639. The following groups of TACOMS interfaces are defined:

   Interoperability Points (IOP) between TACOMS network elements.

   User Terminal Access Points (UTAP) for connection to user and operator terminals.

   External Network Access Points (ENAP) to connect to non-TACOMS networks.

8. Figure 2-3 shows the TACOMS network elements and their interfaces.

9. At each TACOMS interface each national element must include the necessary inter-working functions to translate between the protocols of the interface and those used internally in the national element.

10. Translation between different voice encoding schemes, or any other application level translations, may be necessary due to different technologies using TACOMS interfaces and in the national elements but TACOMS has specified a codec negotiation process to reduce the transcoding to a minimum.

11. The Interfaces are based on physical/electrical features in such a way to guarantee bandwidth over-provisioning (with the exception of L3).

12. All interfaces are defined as a cable interface with complete and unambiguous protocol stacks. The lower layers of the protocol stack are defined in STANAG 4640.

13. A complete definition of each of the following interfaces is provided in STANAG 4639.

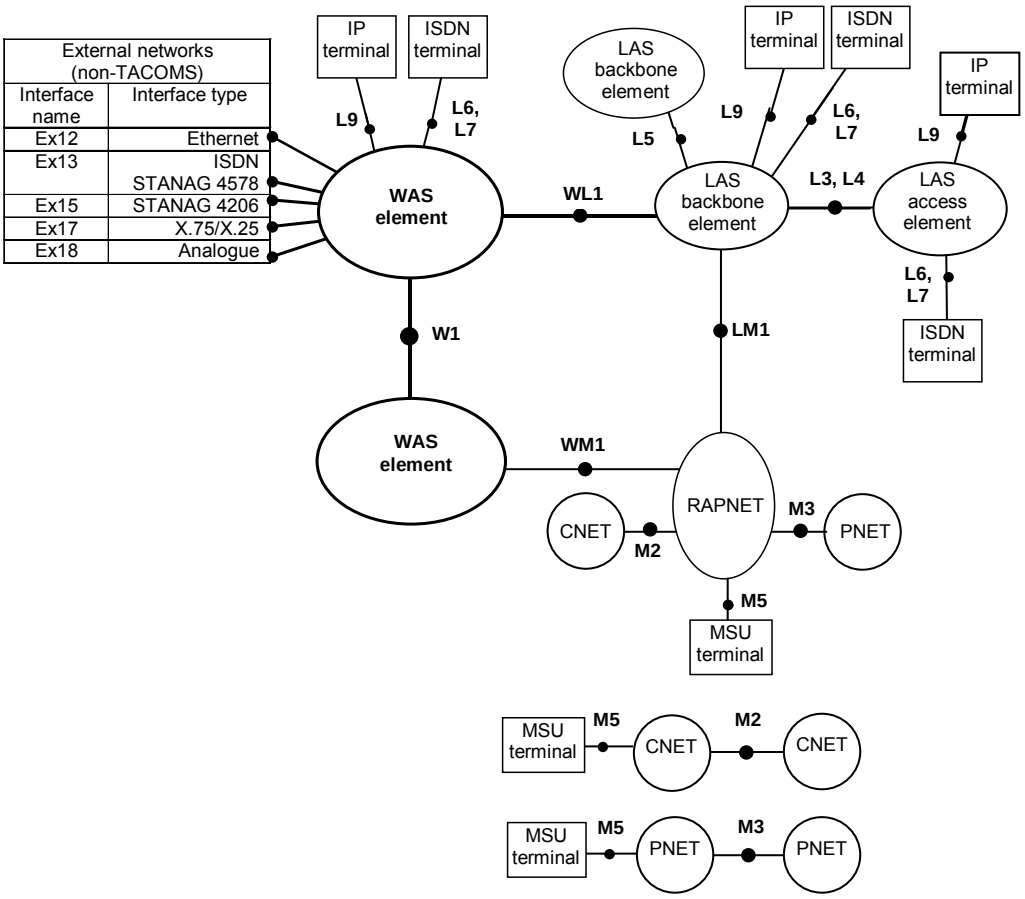

Figure 2-3: TACOMS Network Elements and Interfaces

- **Interoperability Points (IOP)**

4. The interoperability points defined for TACOMS are shown in Table 2-1.

Interoperability Point	Reference Point	Interface type
WAS- WAS Interoperability point	W1	Ethernet over fibre optics
WAS-LAS Interoperability point	WL1	Ethernet over fibre optics
WAS-MS Interoperability point	WM1	Ethernet over fibre optics
LAS-MS Interoperability point	LM1	Ethernet over fibre optics
LAS backbone to LAS access ISDN interoperability point	L3	ISDN PRI
LAS backbone to LAS access IP Interoperability point	L4	Ethernet over fibre optics
LAS backbone to LAS backbone Interoperability point	L5	Ethernet over fibre optics
CNET to CNET and RAPNET to CNET Interoperability point	M2	Ethernet over twisted pair (mandatory) Ethernet over fibre optics (optional)
PNET to PNET and RAPNET to PNET Interoperability point	M3	Ethernet over twisted pair (mandatory) Ethernet over fibre optics (optional)

Table 2-1: Interoperability Points (IOP)

- **User Terminal Access Points (UTAP)**

5. The User Terminal Access Points defined for TACOMS are described in Table 2-2.
6. The ISDN access protocols are defined in STANAG 4641.
7. The IP access protocols are defined in STANAG 4642.

User Terminal Access Point	Reference Point	Interface type
Civilian ISDN UTAP	L6	ISDN BRI (mandatory) ISDN PRI (optional) Civilian connectors
Military ISDN UTAP	L7	ISDN BRI (mandatory) ISDN PRI optional) Military connectors
IP UTAP	L9	Ethernet over twisted pair (mandatory) Ethernet over fibre optics (optional)
Radio UTAP	M5	Ethernet over twisted pair (mandatory) Ethernet over fibre optics (optional)

Table 2-2: User Terminal Access Points (UTAP)

- **External Network Access Points (ENAP)**

8. The External Network Access Points (ENAPs) defined for TACOMS are shown in Table 2-3.
9. The protocols used on each of these ENAPs are described in STANAG 4647.

External Network Access Point	Reference Point	Interface type
IP ENAP	Ex12	Ethernet over fibre optics (mandatory) Ethernet twisted pair (optional) G.703 (mandatory)
ISDN ENAP (STANAG 4578)	Ex13	ISDN PRI (mandatory) ISDN BRI (optional)
STANAG 4206 ENAP	Ex15	STANAG 4206
X.25/X.75 ENAP	Ex17	V.10 (mandatory) V.11 (optional)
Analogue ENAP	Ex18	Analogue two-wire

Table 2-3: External Network Access Points (ENAP)

- **Terminals**

10. TACOMS does not standardise terminals but, to accommodate roving users that move with their terminals, the terminal interfaces have been standardised. These are referred to as User Terminal Access Points (UTAP).

11. All terminals that will only be used inside a specific Nation's element will not be required to follow TACOMS standards from an interface point of view. As an example this means that nations may maintain legacy analogue or EUROCOM standard voice terminals, as long as their access element contains interworking functions to TACOMS traffic standards at their L3, L4, L5 or WL1 IOPs.

- **ISDN Terminals for UTAP (L6 and L7)**

12. For ISDN terminals, two variants of interface are standardised:

The standard civilian ISDN interfaces (Basic and Primary Rate Access) and

The military ISDN interfaces (Basic and Primary Rate Access).

The standard ISDN interfaces must be suited for connection of standard ISDN terminals, while additional requirements will apply to the military ISDN terminal. Such additional requirements are:

Military connector

Particular handling of security codes for affiliation or other aspect of access control: codes should not be stored, nor displayed by the terminal.

Dedicated keys for handling of precedence level

Display of security status of the current connection (if provided)

- **IP Terminals for UTAP (L9)**

13. The standard civilian interface based on IP over Ethernet enhanced with the following military features will apply to the IP terminal:

Military connector

Particular handling of security and access control.

- **MSU Terminals for Radio UTAP (M5)**

14. The standard civilian interface based on IP over Ethernet enhanced with the following military features will apply to the MSU terminal:

Military connector

Particular handling of security and access control.

A specific configuration of signalling protocols, as defined in STANAG 4645 Annex A.

TACOMS recommends "TCP-radio" and "TCP-radio-newRTO" as the transport protocols, which are better adapted to the environment of the MS as described in STANAG 4645 Annex B.

- **SYSTEM CHARACTERISTICS**

- **Introduction**

15. This chapter describes the main TACOMS system characteristics. This includes user and network services, mobility concept and quality of service (QoS) concept.

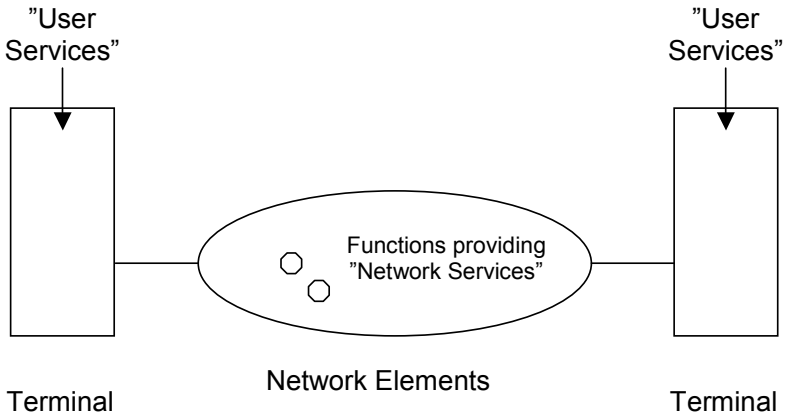

Figure 3-4: TACOMS Services

16. The TACOMS Network is formed by Network Elements (NE) that interconnect through Interoperability Points (IOP), forming a mesh network.

Within TACOMS there is a common numbering, naming and addressing scheme.

The ability to use TACOMS as a transit network between two external networks using Gateways as specified in STANAG 4647 is supported through the use of standard international numbering and routing schemes (NIAC) or, alternatively, using one of various defined numbering translation modes.

The ability to use an external network as a transit network between two TACOMS networks using Gateways will be supported, depending on the ability of the transit external network.

- **User Services**

17. The set of user services to be used in TACOMS had been defined in the NATO source document MC-337 (Reference 1) and augmented with updated information from the NC3A scenario study (CR 149) (Reference 2). This has been further updated to include user services needed to support the deployment of a coalition force exploiting Network Enabled Capabilities (NEC) or Network Centric Warfare (NCW) capabilities.

18. TACOMS network is designed to deliver all of the services listed in above documents, while only limited set of services is defined in detail in TACOMS standards. The resulting revised user services concept is described later in this document.

14. Users may communicate with other users without any knowledge of where the other users are physically located.

15. Users may communicate through gateways without any knowledge of which network element provides such gateways, or where the gateways are physically located. Users may also select a specific gateway for a call to a non-TACOMS network.

19. Reconfiguration of a TACOMS network for reasons of redeployment, attrition, failure or congestion will have no effect on users facilities, but may result in changed performance if, for example, lower bandwidth links are used.

16. The current set of user services is presented, indicating the TACOMS sub-systems that support them:

User Services	TACOMS Subsystem			Comments
	LAS	WAS	MS	
Telephony	M	M	M	
Voice Intercom	O			LAS internal, interoperable with the telephony service in the WAS and MS
Half Duplex Telephony			O	MS internal but supported across WAS and LAS as telephony with pressel (push to talk) signalling end to end
Secure Communications Interoperability Protocol (SCIP)	O	O	O	Capable to support encrypted voice and encrypted low rate data
Message Handling	O	O	O	application not standardised (using data transfers)
File Transfer	O	O	O	application not standardised (using data transfers)
Real Time Data Transfer	O	O	O	application not standardised (using data transfers)
Facsimile	O	O	O	Group 3/4 fax traffic converted to message traffic at external network WAS gateways or sent transparently through the network
Graphics Transfer	O	O	O	application not standardised (using data transfers)
Still Picture	O	O	O	application not standardised (using data transfers)
Low Rate Video	O	O	O	May be supported in some MS implementations
High Rate Video	O			LAS internal
Web Services	O	O	O	application not standardised (using data transfers)
Distributed Data Processing	O	O	O	application not standardised (using data transfers)
System Management	O	O	O	(*)
Security Management	O	O	O	(*)

√ = Supported
(*) = These applications use standard voice or data communications services, possibly with specific features in terms of access and use of dedicated channels, under national concern.

Table 3-4: User Services

- **Mobility concept**

20. TACOMS is required to handle both User and network mobility.

21. Users are able to move between network elements of a TACOMS network. This capability is facilitated by the subscriber profile information that is shared in the Battlefield Directory. This mobility, specified in STANAG 4644 Annex H, may take three different forms:

Terminal mobility: A single user with his terminal will move to a new UTAP at another network element. After a successful authentication sequence, the network management authority will acknowledge the re-affiliation, and the network directories will be updated to reflect the new location of this user with his specific subscriber profile, that may be updated to reflect the services that the new host network provides to the user.

User mobility: A single user may move without his normal terminal to affiliate at a new location on a terminal provided by the new host nation network authority. After a successful authentication sequence, the network management authority will acknowledge the re-affiliation, and the network directories will be updated to reflect the new location of this user with his specific subscriber profile, that may be updated to reflect the services that the new host network and the new terminal provide to the user.

Logical mobility: Users may be identified by the name of the person or the role that they have taken responsibility for. Logical links between roles and users can be made in the Battlefield Directory. Thus, logical mobility consists of re-assigning a role from one user to another.

17. Network mobility, facilitated by the IP Routing specified in STANAG 4644 Annex C and the CO Routing specified in STANAG 4643 Annex C:

A NE can disconnect, move, and re-connect at any other appropriate IOP in the TACOMS network.

An external network can disconnect, move, and re-connect at any other appropriate gateway.

- **Quality of Service Concept**

22. Where possible, TACOMS NEs are interconnected using a single cable with high speed Ethernet at the physical layer (see the definition of IOPs, UTAPs and ENAPs in Chapter above). To support a consistent set of network and user services across these interfaces, with in general different technologies used in the core of the NEs, a comprehensive Quality of Service concept is needed for TACOMS. Detailed specifications are in STANAG 4643 and STANAG 4644.

- **Traffic Handling Classes (CO/CL)**

23. At present most legacy systems incorporate circuit-switching technology for handling voice traffic and packet switching technology for handling data traffic.

24. From Quality of Service point of view the basic difference between these two technologies is related with traffic handling mode.

25. In the connection-oriented mode, it is possible to guarantee quality of service (QoS) (available bandwidth, delay, delay variation) for every connection throughout its duration time. If there are not enough resources in the network at the connection establishing time, the connection is

no established at all. This mode is more suitable when a service (e. g. voice) requires constant QoS guarantees for every single data flow in its whole duration time.

26. In connectionless mode the network is not aware of connections, but only of single packets. Then QoS may be guaranteed only in limited way, e.g. for the whole group of packets characterised in the same way. The advantage of connectionless mode is that it is faster at the start of data transmission (because the connection establishment phase is omitted) and there is more efficient usage of network resources. This mode is more suitable when a service (e. g. file transfer) may tolerate temporary changes of network performance in the data flow duration time.

18. To deal with these two modes, the concept of "Traffic Handling Classes" (THC) is introduced in TACOMS, with two classes defined: Connection Less (CL) and Connection Oriented (CO), as follows:

The Connection Less Traffic Handling Class is specified to handle IP Packets. The network is assumed to provide:

Quality of Service guaranties: Certain amount of network resources is allocated to serve packets containing the same QoS information present on the packet header (DSCP) regardless the number of flows these packets belong to.

Packet Routing: The network routes packets based on the IP destination address.

Packet Forwarding: The network uses the QoS information present on the packet header (DSCP) to determine the packet forwarding behaviour.

Boundary Protection: The network may perform the ingress traffic conditioning function, defined in Diffserv standards, in UTAPs, IOPs and ENAPs, depending on the User-Network and Network-Network Service Level Agreements. The network may discard packets in order to protect itself from overflow (e.g. to prevent a denial of service attack).

a. The Connection Oriented Traffic Handling Class is specified to handle calls. Depending on the interface type, H.323 (with IP) or ISDN protocols are used. The network is assumed to provide:

(1) Quality of Service guaranties: Certain amount of network resources is allocated to every single call and is guaranteed for the whole call duration time.

(2) Call Routing: The network routes all the signalling and traffic involved in a given call through the same sequence of TACOMS interfaces. In order to assure this sequence, the call is routed step-by-step, from one network element to the next, via call handlers present at both sides of each interoperability point (IOP). Between NEs the call is routed based on the destination address information contained in the call signalling. Routing within the NEs is of national concern.

(3) Resource Reservation: The network assigns network resources (e.g. bandwidth) and terminal access resources to admitted calls. Resource pre-emption mechanisms are applied when necessary, depending on the Precedence Level of the existing and new calls. The mechanism for resource reservation is of national concern.

(4) Call Admission Control: Each Network Element admits or rejects calls depending on the User Profile, the Precedence Level of the call and on the network and terminal resources available. National defined criteria may also be applied.

b. The CO and CL THCs have separate routing functions, i.e. between NEs routing information is exchanged separately for each THC.

- **Service Level Agreements and Service Level Specifications**

27. In TACOMS there is a requirement to support end-to-end services, over a variety of national LAS, WAS and MS network element implementations.

28. These services range from real-time services for voice and multimedia conferences, high priority mission critical C2 and sensor data, to low priority data traffic such as non-operational e-mail.

29. To define the network services, the concept of Service Level Specification (SLS) is adopted, according to the following definition: A Service Level Specification (SLS) is a set of technical parameters and their values, which together define the Quality of Service offered to the user traffic.

Some predefined service levels, called SLS Classes, are specified by TACOMS. This means that the TACOMS standards specify differentiated network behaviour for each of these SLS Classes. The SLS Classes handled by the CO THC are called CO SLS Classes and the SLS Classes handled by the CL THC are called CL SLS Classes.

The QoS guaranties for a service may be different for different deployments because of different role and importance of this service. These QoS guarantees are defined in pre-deployment phase and written in Service Level Agreement (SLA).

30. The SLA is defined in TACOMS as the documented result of a negotiation between a user or network element authority and the neighbour network element authority that specifies the levels of availability, serviceability, performance, operation or other attributes of the provided service.

31. The SLA contains description of relations of user services, Traffic Handling Classes, SLS Classes and other detailed information necessary to implement all of the services for given deployment.

Since neither network resources nor the offered traffic are constant over time, an SLA review cycle is needed to adjust either the network resources or the SLAs (or both). Establishment of additional SLAs during the life time of a deployment may be allowed, but this may have complex implications in terms of network dimensioning. To limit the complexity, it is suggested that spare resources are reserved during the planning phase for future unplanned additional SLAs.

19. In TACOMS there is a distinction between network-network and user-network SLAs.

20. The network-network SLA is established between interconnecting networks during the deployment planning phase and takes the deployed network capabilities into consideration. Under the TACOMS scope, the network-network SLA should contain the list of SLS Classes supported by the connecting network elements and the bandwidth constraints that the receiving network associates to each of them:

21. For the supported CL SLS Classes: maximum bandwidth allowed, minimum guaranteed bandwidth, period for bandwidth measures, assignment of the DSCPs corresponding to each type of service (if the TACOMS default assignment is not followed), etc.

22. For the supported CO SLS Classes: maximum per call bandwidth, maximum number of simultaneous calls, maximum bandwidth, etc. The relations between the values of these parameters are dependant on the particular NE technology.

23. The information from user-network SLA is a part of the Subscriber Profile stored in the user service entries of the BD. It contains the data that the network needs to know about the services provided to each particular user. It includes some QoS information showing the list of SLS Classes authorised to the user service entry and the constraints associated to each SLS Class:

24. For the supported CL SLS Classes: DSCP identifying the CL SLS Class/Subclass, maximum bandwidth, medium (sustainable) bandwidth.

25. For the supported CO SLS Classes: maximum call precedence level, maximum per call bandwidth, maximum number of simultaneous calls.

In the network, the traffic is handled according to the “SLS Class” and THC, i.e. when a user requests a service, the network will decide which of its standard services (i.e. SLS Classes and a THC) should be used for the requested service.

As TACOMS has defined two distinct Traffic Handling Classes, the CO THC, and the CL THC, CO Classes of Service (CoS) and Diffserv Per Hop Behaviours (PHBs) are defined:

The CL Diffserv PHBs are defined in relation with IP packet handling.

The Classes of Service (CoS) defined in relation with call handling, H.323 or ISDN.

26. Network Element performance parameters for the CO and CL THCs are specified separately in performance parameter sets in STANAG 4638. The CO CoS and the Diffserv PHBs are respectively associated to the CO and CL SLS Classes. The SLS Classes are also used in the Management Protocols specified in STANAG 4646. Relations between the CO CoS, Diffserv PHBs and SLSes are summarized below, in the Table 3-5.

CO THC CO Classes of Service (CoS)		**SLS Classes (Sets of performance parameters)**		**CL THC Diffserv PHBs**
		For CO THC	**For CL THC**	
CO-CoS-V (Voice)		CO SLS1	CL SLS1	CS6/7
CO-CoS-D (CBR Data)				EF
CO-CoS-M (Multimedia)	Interactive applications	CO SLS2	CL SLS2	AF4x
	Non-interactive applications	CO SLS3	CL SLS3	AF3x
-		-	CL SLS4	AF2x
-		-	CL SLS5	AF1x
				BE

Table 3-5: Relations between the CO CoS, Diffserv PHBs and SLSes

The IP nodes of the network provide different packet forwarding behaviour to the traffic belonging to each Diffserv PHB. Traffic coming from different sources, but sharing the same transmission link and indicating the same Diffserv PHB, is aggregated in flows that receive the same forwarding behaviour, following the Diffserv standards.

The TACOMS IP QoS specifications contained in STANAG 4644 Annex D specifies how the Diffserv paradigm applies to the TACOMS IP nodes, to the TACOMS Traffic Handling Classes and to the user and network applications generating IP traffic. The TACOMS IP QoS specifications are concretised in three areas: Packet Marking Function, Per Hop Behaviour specifications and DSCP Assignment.

Table 3-6 shows a simplified view of the TACOMS PHBs, indicating the default assignment of type of services to each **Diffserv PHB**.

Diffserv PHB		DS Queuing Priority	DS Drop Preced.	Default Assignement of Type of Services to each Diffserv PHB	
PHB for preferential Class Selector codepoints CS6/7		1	Non applicable	- Network Control (IP-layer keep alive, critical control messages, routing, etc.)	
Expedited Forwarding PHB - EF		2	Non applicable	- Voice - SCIP applications - CBR Data	
Assured Forwarding PHB Group - A4x	AF41 CS5	3	Low	- Flash Override - Flash	- Time-critical Applications - Multimedia Conferencing
	AF42		Medium	- Immediate - Priority	
	AF43		High	- Routine	
Assured Forwarding PHB Group - A3x	AF31 CS4	4	Low	- Flash Override - Flash	- Multimedia Streaming
	AF32		Medium	- Immediate - Priority	
	AF33		High	- Routine	
Assured Forwarding PHB Group - A2x	AF21 CS3	5	Low	- Flash Override - Flash	- Call Signalling - Client-Server Applications - Web-based Applications
	AF22		Medium	- Immediate - Priority	
	AF23		High	- Routine	
Assured Forwarding PHB Group - A1x	AF11 CS2	6	Low	- Flash Override - Flash	- Non-critical Management - File transfer - Messaging - Messaging
	AF12 CS1		Medium	- Immediate - Priority	
	AF13		High	- Routine	
Default PHB (Best Effort) - BE CS0		7	Non applicable	- Others applications	

Table 3-6: TACOMS Diffserv PHBs

The network services are provided by the CO THC in a per call basis for all the CO CoS, which allows the NEs to provide per call features like Multi Level Precedence and Pre-emption (MLPP) and Codec Negotiation, as specified in STANAG 4643 Annex B and Annex D respectively.

As it is expected that not all the NEs will support all the CO CoS, the optional QoS enhanced CO Routing specified in STANAG 4643 Annex C is able to provide differentiated call routing for calls belonging to each defined CO CoS. If the QoS enhanced CO Routing is not used, then the NEs not supporting some CO CoS should not be deployed as transit networks between NEs that support those CO CoS.

The CO CoS defined by TACOMS are based on the call characteristics indicated during the call signalling. The NEs supporting a given CO CoS has to provide the required network capabilities.

Table 3-7 shows the three predefined CO CoS that have been established, indicating some examples of User Services for each CO CoS.

CO CoS	Call characteristics defining each CO CoS	Network capabilities specifically required for each CO CoS	Example of User Services for each CO CoS
Voice	A call that signals only one audio media stream in each direction, or only one at all, even if the call signals various alternative voice codecs using alternative audio capabilities.	Support of the voice coding protocols and voice trans-coding procedures specified in STANAG 4643 Annex D.	- Telephony - Voice Intercom - Half Duplex Telephony
CBR Data	A call that signals only one data media stream in each direction, or only one at all, even if the call signals various alternatives data bit rates using alternative data capabilities.	Support of the CBR data coding protocols specified in STANAG 4643 Annex D. The actual traffic of the call may not have constant bit rate, but the network has to be prepared to support it.	- SCIP (encrypted voice and low rate data) - Legacy tactical data
Multimedia	A call that signals one or more video or multimedia streams, or more than one media stream in at least one direction.	Support of multimedia, video and voice coding protocols specified in STANAG 4643 Annex D.	- Low Rate Video - High Rate Video - Still Picture - Videoconference - Streaming Multimedia

Table 3-7: TACOMS CO Classes of Service (CO CoS)

Inside each CO Class of Service, five levels of call precedence are specified:

Flash Override.

Flash.

Immediate.

Priority.

Routine.

1.1.1 QoS Information through TACOMS Interfaces

32. The traffic transported by a TACOMS network is marked with QoS information determined by the originator of the traffic. This QoS information is passed through TACOMS interfaces, allowing the receiving system to determine which of the supported SLS Classes should be used for the received traffic.

27. In TACOMS the procedures to transmit QoS information through TACOMS interfaces, depending on the type of interface and the Traffic Handling Class (THC) is specified:

    a. Through CO ENAPs (STANAG 4206, STANAG 4578 and Analogue gateways). The QoS information is included in the call signalling information passing through the

gateway which describes the service requested in a call. This signalling includes MLPP in some of the gateway types.

b. Through CL ENAP (IP gateway). The option of passing DiffServ information (i.e. DSCP) through the gateway is specified, as well as the mapping of the TACOMS PHBs to the DSCP values of the external network (see STANAG 4647 Annex A).

c. Through TACOMS ISDN IOPs and UTAPs. The QoS information is included in the call signalling information passing through the interface and describes the service requested in a call. This signalling includes MLPP.

d. Through TACOMS IP IOPs and UTAPs. The type of QoS information passed through IP interfaces will depend on the THC in use.

(1) If the CL THC is in use, the QoS information is based on DiffServ principles and is specified in the TACOMS IP QoS specification (see STANAG 4644 Annex D).

(2) If the CO THC is in use, the QoS information is contained in the H.323 call signalling information passing through the interface and describing the service requested in the call. This signalling includes MLPP. The IP packets that transport the H.323 traffic (signalling and media streams) through TACOMS IP interfaces should also be marked as specified in the TACOMS IP QoS specification (see STANAG 4644 Annex D).

28. Figure 3-5 contains a simplified protocol stack of the TACOMS IOP and UTAP interfaces, showing where the TACOMS CO CoS and TACOMS PHBs definitions are applied.

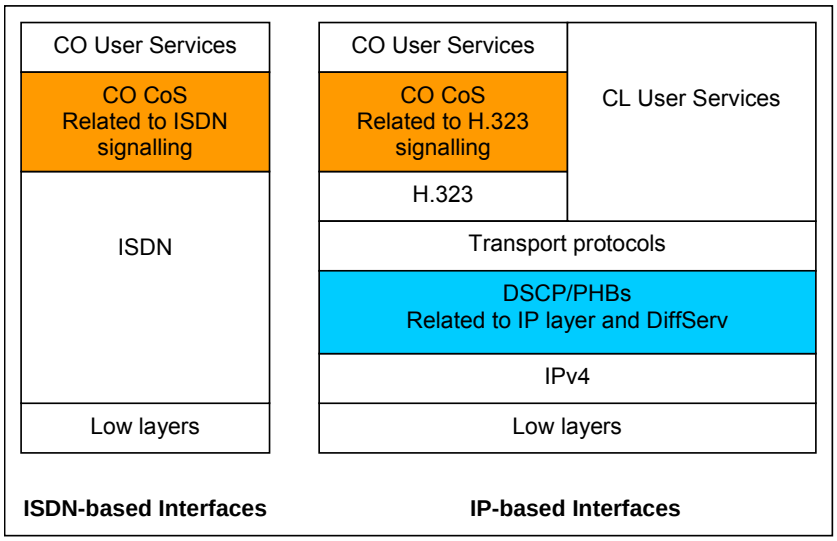

Figure 3-5: CO CoS and DSCP/PHBs definition at the TACOMS Interfaces

- **QoS Provision in the Network Elements**

33. In addition to the behaviour specified for the TACOMS interfaces, the TACOMS network elements shall apply their own specific QoS mechanisms. These are necessary to assure the performance required for the CO and the CL Traffic Handling Classes (e.g. per call bandwidth reservation/assignment in the CO THC and DiffServ mechanisms in the CL THC). Bandwidth over-provisioning may also be an option as a QoS mechanism.

29. STANAG 4638 defines the minimum number of Interoperability Points and of User Terminal Access Points that each type of TACOMS Network Element must provide, and its required

minimum performance in terms of overall traffic handling capacity and quality of service for each of the five TACOMS Service Classes.

Network Services

34. Network Services group all functionality that are necessary to support the User Services through the network such as directory services, mobility support, routing, call handling etc is provided.

- **Battlefield Directory**

35. The Battlefield Directory (BD) in a TACOMS network is a distributed and replicated database. It manages the data for several purposes: to support user mobility, location of gateways to external users, etc. A full definition of the BD is given in STANAG 4644.

36. The BD is built around the standard protocol suites DNS, X.500 and LDAP. It is enhanced with the use of caches and chaining controls to improve performance, and authoritative queries to improve accuracy.

30. The BD Directory Information Tree (DIT) is consistent with and linked to the structure of ACP 133. It also re-uses some of the attribute definitions as well as defining new ones.

31. A TACOMS User might be: a person or a role (e.g. an operational function or a network server).

32. A User may own several (addressable) user services (identified by telephonenumber1, telephonenumber2, computer_application1..). The admitted services of a user are recorded in the BD.

33. There are two categories of user services:

    a. CO: using Call set-up, traffic, call release

    b. CL: CL User services are not standardised in TACOMS

34. All User services (CO and CL) are identified by a unique Distinguished Name (DN) in the DIT

    c. The DNs of the User service entries (both for CO and CL) are as follows: TNC (3 digits) SMD (3 digits) and USN (User Service Name)

    d. The USN for CO: The “CO user service” of a User is identified and addressed as a telephone number (7 digits)

    e. The USN for CL: The “CL User service” name is defined by the nations and must comply with the ACP 133 commonName attribute.

35. BD information is accessed using two protocols:

    f. DNS: From a query containing a Fully Qualified Domain Name (FQDN) an IP address can be retrieved.

    g. LDAP (X.500): From a query containing a Distinguished Name (DN) the associated data can be retrieved, e.g. a service, a gateway or a user entry in the DIT.

36. Mobility:

    h. Terminal mobility: The FQDN is constant, and associated with a new IP address when moved

    i. User service mobility: Different user services are moved independently and the services may at any point in time be associated with different terminals

    j. User services therefore have separate entries in the BD and for each

    k. Logical mobility: A role being assigned to a person. Logical mobility is the movement of a role from one person to another.

37. Two profile are defined for server to server BD data replication:

38. DNS/X.500 Battlefield Directory Replication.

39. LDUP Battlefield Directory Replication.

- **IP Addressing**

37. A homogeneous IP Addressing Plan is required in TACOMS to assure high efficiency, reliability, performance and maintainability. It is based on the use of Private Address space.

38. The network elements are assigned unique IP network prefixes. However, it is a national responsibility to allocate the IP addresses inside their network elements.

39. The use of Dynamic Host Control Protocol (DHCP) servers is recommended to provide the IP addresses to the terminals. This provides:

a. the ability to define ranges of addresses to be given out

b. the ability to lease an address for a finite period of time

c. the ability to recover addresses that are no longer used.