INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR DA FORÇA AÉREA

2006/2007

TII
VERSÃO PROVISÓRIA

DOCUMENTO DE TRABALHO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IESM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DA FORÇA AÉREA PORTUGUESA.

O CONCEITO "GUERRA CENTRADA EM REDE" E A MODERNIZAÇÃO DOS SISTEMAS DE ARMAS DA FORÇA AÉREA PORTUGUESA

Paulo Alexandre de Sousa dos Santos
Capitão Navegador

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

O CONCEITO "GUERRA CENTRADA EM REDE" E A MODERNIZAÇÃO DOS SISTEMAS DE ARMAS DA FORÇA AÉREA PORTUGUESA

Capitão Navegador Paulo Alexandre de Sousa dos Santos

Trabalho de Investigação Individual CPOS/FA – 2006

Versão Provisória

Lisboa 2007

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

O CONCEITO "GUERRA CENTRADA EM REDE" E A MODERNIZAÇÃO DOS SISTEMAS DE ARMAS DA FORÇA AÉREA PORTUGUESA

Capitão Navegador Paulo Alexandre de Sousa dos Santos

Trabalho de Investigação Individual CPOS/FA – 2006

Orientador:
Major Navegador António Luís Beja Eugénio

Versão Provisória

Lisboa 2007

“Nada é mais difícil de tomar nas mãos, ou mais perigoso de conduzir, ou ainda de sucesso mais incerto, do que assumir a liderança na introdução de um novo estado de coisas. Porque o inovador tem como inimigos, todos aqueles que se deram bem sob as velhas condições e defensores oportunistas entre aqueles que poderão se dar bem sob as novas”.

MAQUIAVEL

Índice

Índice de Figuras

Índice de Tabelas

Resumo

A nova vaga civilizacional traduz-se no desvio das atenções para o poder da informação, em detrimento de outras fontes de poder. Tal como em épocas passadas, a instituição militar rapidamente adoptou os novos conceitos percebendo o valor da informação e da sua partilha como vector catalizador do sucesso no combate.

A presente investigação pretende avaliar de que forma os recentes sistemas de armas e os programas de modernização da Força Aérea Portuguesa estão de acordo com os requisitos técnicos impostos pelas novas linhas de orientação da NATO, apoiadas em redes globais de informação, de forma a garantir a interoperabilidade das forças nacionais com as forças de outros estados membros da Aliança Atlântica, num hipotético cenário de guerra centrada em rede.

As conclusões apresentadas demonstram que os meios aéreos estudados, apesar do esforço realizado pela Força Aérea Portuguesa no sentido de alcançar as metas traçadas pela Aliança Atlântica, apenas garantem níveis baixos ou médios de interoperabilidade, tendo por referência o nível tecnológico aplicado nos sistemas de armas.

Abstract

The new civilizational wave reflects a course deviation concerning the attention given to the power of information, leaving behind other sources of power. Like in previous times, military organizations quickly adopted the new concepts, realizing the value and sharing of information in order to enable combat sucess.

This investigation intends to evaluate if the recent Portuguese Air Force weapon systems and modernization programs have complied with the technical requirements imposed by the new NATO guidelines, supported by global information networks, in order to assure interoperability between national forces and Alliance member states, in an hipothetic networked-centric warfare scenario.

The conclusions of the investigation show that the researched air assets, despite the effort made by the Portuguese Air Force trying to reach the goals established by the Atlantic Organization, can only comply with low and medium levels of interoperability, when referenced to the technical degree applied to the weapon systems.

Palavras-chave

INTEROPERABILIDADE, SUPERIORIDADE INFORMACIONAL, GUERRA CENTRADA EM REDE, SISTEMAS DE ARMAS, CONCEITO NNEC, SUPERIORIDADE DE DECISÃO, OPERAÇÕES CONJUNTAS E COMBINADAS.

Lista de abreviaturas

ACT	*Allied Command for Transformation*
AGS	*Allied Ground Surveillance*
AIP	*ASuW Improvement Program*
ASuW	*Anti-Surface Warfare*
BMUP	*Block Modification Upgrade Program*
CAOC	*Combined Air Operations Center*
COI	*Community of Interest*
COTS	*Commercial off-the-shelf*
CSAR	*Combat Search and Rescue*
CUP	*Capability Upkeep Programme*
C2	*Command and Control*
C4ISR	*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconaissance*
DoD	*Department of Defense*
EO	Electro-Óptico
ECM	*Electronic Counter-Measures*
ESM	*Electronic Support Measures*
EUA	Estados Unidos da América
FFAA	Forças Armadas
FAP	Força Aérea Portuguesa
FTBCB	*Full Tail Biting Convolutional Block*
GCR	Guerra Centrada em Rede
GIG	*Global Information Grid*
GOTS	*Government Off-The-Shelf*
HF	*High Frequency*
HSI	*Hiper Spectral Infra-red*
IP	*Internet Protocol*
IR	*Infra-red*
ISR	*Intelligence, Surveillance and Reconaissance*
ISAR	*Inverse Synthetic Aperture Radar*
JTIDS	*Joint Tactical Information Distribution System*
JTRS	*Joint Tactical Radio System*
LWIR	*Long-wave Infra-red*

MIDS	*Multifunctional Information Distribution System*
MPA	*Maritime Patrol Aircraft*
MLU	*Mid-Life Update*
NATO	*North Atlantic Treaty Organization*
NCW	*Network-Centric Warfare*
NEC	*Network Enabled Capability*
NII	*Networking and Information Infrastructure*
NMI	*NATO C3 Technical Architecture Reference Model for Interoperability*
NNEC	*NATO Network Enabled Capability*
NNII	*NATO Networking and Information Infrastructure*
NR	*Net Readiness*
NRF	*NATO Reaction Forces*
OCU	*Operational Capabilities Upgrade*
RATT	*Radio Tele Type*
SA	Sistema de Armas
SAM	*Surface-to-Air Missile*
SAR	*Synthetic Aperture Radar*
SATCOM	*Satellite Communications*
SLEW	*Single Tone Link Eleven Waveform*
SOSTAR	*Stand-Off Surveillance and Target Acquisition Radar*
SWIR	*Short-wave Infra-red*
TADIL	*Tactical Digital Information Link*
TDL	*Tactical Data Link*
TI	Tecnologias da Informação
TMD	*Theatre Missile Defence*
UE	União Europeia
UAV	*Unmanned Aerial Vehicle*
UHF	*Ultra High Frequency*
VHF	*Very High Frequency*
VNIR	*Visible-to-near Infra-red*

Introdução

O processo de comunicação entre os seres humanos tem evoluído continuamente. Durante muitos séculos a um ritmo lento e por vezes algo estagnado, mas a partir do século XIX registou-se uma crescente aceleração, convidando o século XX, particularmente a partir da década de 50, a assistir à explosão das tecnologias da informação. Fundamentalmente, alterou-se a forma como passaram a interagir entidades separadas geográfica e temporalmente (Alberts, 2003b: 74).

O novo milénio tem sido arauto de um novo ciclo na história da humanidade, revelando uma extraordinária transformação social que se vinha insinuando nas últimas décadas do século transacto. A Revolução Informacional. Tal como em outros marcos da biografia da sociedade humana, rapidamente se concebeu uma nova era militar, afectando aos recentes cenários bélicos ambientes estratégicos altamente dinâmicos, inspirados na incessante evolução tecnológica.

O conceito *Network Centric Warfare* (NCW) – Guerra Centrada em Rede (GCR) – decorre da Era da Informação que pretende alterar, a todos os níveis, o processo de planeamento e condução da guerra. A expressão "guerra centrada em rede" implica uma combinação de organizações, doutrina, tácticas, técnicas, procedimentos e tecnologia, que quando empregues, de acordo com um determinado enquadramento pré-definido, podem ser determinantes para garantir uma vantagem decisiva em combate (Alberts, 2003a: 3).

O mérito incontestável deste novo conceito promoveu, em muitos países, estudos e análises que deram origem a novas formas de pensar a Guerra e consequentemente à redefinição e criação de modernos conceitos, embora com directrizes dependentes da concepção original. A título de exemplo, podem referir-se os casos da Suécia – *Network Based Defence* (NBD), da França, da Alemanha, da Holanda, da Bulgária, do Reino Unido – *Network Enabled Capability* (NEC) ou da Austrália, cujo conceito se apresenta em Apêndice.

Além do trabalho desenvolvido por estas nações, merece especial destaque o trabalho desenvolvido pela *North Atlantic Treaty Organization* (NATO), cujo conteúdo será apresentado de forma sumária ao longo da investigação, pela sua importância, influência e consequências na política de defesa nacional, com óbvios efeitos no planeamento estratégico da Força Aérea Portuguesa (FAP). Particularmente, será apresentado o conceito *NATO Network Enabled Capability* (NNEC) que corresponde a uma adaptação do conceito britânico à organização multinacional (Vicente, 2005: C-2).

Perante este enquadramento, julgou-se pertinente realizar uma investigação que permitisse verificar em que medida as aquisições e programas de modernização de sistemas de armas da FAP encerram os requisitos técnicos impostos pela interoperabilidade, factor absolutamente fundamental num cenário de GCR (Alberts, 2003b: 107).

O presente trabalho pretende reflectir a investigação, elaborada de acordo com os padrões definidos pelo Método de Investigação em Ciências Sociais de Raymond Quivy, cujo objectivo era responder à questão: “Em que medida foram satisfeitos os requisitos técnicos impostos pela necessidade de interoperabilidade, num cenário de utilização das tecnologias de GCR, nas aquisições e programas de modernização de sistemas de armas da Força Aérea Portuguesa?”

Perante a pergunta de partida, julgou-se conveniente derivar algumas perguntas secundárias, de acordo com os parâmetros referidos anteriormente, que estabelecessem os racionais de apoio ao desenvolvimento sustentado do processo de investigação. Assim, foram definidas as seguintes questões derivadas:

- Quais as recentes abordagens aos conceitos GCR e NNEC?
- Quais são as tecnologias da GCR?
- Em que consiste a interoperabilidade?
- Quais são os requisitos técnicos das tecnologias da GCR?
- Quais foram as recentes aquisições e programas de modernização de sistemas de armas da FAP?
- As recentes aquisições e programas de modernização de sistemas de armas da FAP cumprem com os requisitos técnicos necessários para a interoperabilidade num cenário de GCR?

Em virtude da enorme complexidade que envolve a temática da GCR e das restrições inerentes à elaboração deste trabalho, foi necessário condicionar a investigação aos aspectos que se consideraram mais importantes e significativos no cenário da GCR, tendo em especial atenção as capacidades operacionais relacionadas com sensores ISR e sistemas de comunicação aplicados a meios aéreos de países da NATO.

No que respeita ao universo de estudo, restringido a três plataformas aéreas, após a análise das recentes aquisições e dos programas de modernização a decorrer, foram escolhidos o F-16 *Mid-Life Update* (MLU), o EH-101 e o P-3C *Capability Upkeep Programme* (CUP)+.

O critério de selecção baseou-se na maior probabilidade de emprego destes meios, face aos restantes, em cenários de GCR, num futuro próximo. Nomeadamente, em missões de Luta Aérea, Busca e Salvamento em Combate (CSAR) e Operações Aéreas contra Forças de Superfície em Ambiente Marítimo, respectivamente.

Concluída a primeira etapa da investigação, que correspondeu à formulação da pergunta de partida, foram desenvolvidas quase em simultâneo as fases de exploração e de definição da problemática, onde foram evidentes as dificuldades em encontrar bibliografia que inequivocamente fosse iluminando o caminho da investigação. As entrevistas efectuadas apenas vieram acentuar a imaturidade do tema no contexto nacional, não concorrendo para um esclarecimento absoluto sobre o mesmo. Muito pelo contrário, foram conclusivas no sentido de revelar a pouca exploração realizada no âmbito dos requisitos técnicos – o cerne da investigação.

Seguiu-se a fase de observação, onde foram analisados os trabalhos cujo conteúdo foi julgado relevante para a investigação. Foram assim seleccionados, entre uma grande diversidade de referências bibliográficas, os documentos que permitiram ir respondendo, passo a passo, às questões que inicialmente tinham sido enunciadas.

A análise da informação foi-se fundindo com a fase anterior, permitindo estudar os sistemas de armas (SA), apresentando os seus sistemas de comunicação e sensores, para depois os observar face aos modelos de interoperabilidade referidos e depois proceder à elaboração das Conclusões.

Deve referir-se que foram duas as razões que motivaram o autor a elaborar este trabalho de investigação. A primeira advém da experiência como coordenador táctico da aeronave P-3P, o que permitiu verificar a importância da interoperabilidade para o sucesso de operações num ambiente conjunto e combinado. Por outras palavras, os exercícios e operações realizadas, ao longo de dez anos, demonstraram a importância da partilha da informação, assim como da celeridade com que este processo deve ocorrer, de forma a contribuir decisivamente para o desfecho vitorioso em combate.

Por outro lado, o processo de Transformação da NATO vai, mais tarde ou mais cedo, implicar o obrigatório desenvolvimento de réplicas ao nível interno dos vários estados membros. Este facto obriga a instituição militar portuguesa a uma profunda reflexão, no sentido de procurar manter a parceria estratégica com a Aliança Atlântica, através da participação de forças nacionais nos cenários operacionais que se adivinham (Araújo, 2005).

1. As tecnologias da Guerra Centrada em Rede

A nova ordem mundial iniciou a sua marcha na última década do século XX. As forças armadas devem agora perseguir padrões de flexibilidade e adaptabilidade, com carácter expedicionário, capazes de enfrentar com sucesso um alargado espectro de ameaças, desde o conflito tradicional até aos de natureza assimétrica e imprevisível (Vicente, 2006).

No presente capítulo procurou-se, além de genericamente definir algumas noções básicas, evidenciar as mais recentes abordagens ao conceito GCR e apresentar as tecnologias a ele associadas.

A ideia subjacente à GCR está intrinsecamente relacionada com a recolha de informação, o seu rápido processamento, análise e interpretação, bem como com a partilha, em tempo oportuno, de informações do espaço de batalha entre os decisores, aos vários níveis de comando, e o combatente em acção directa com as forças opositoras. Sintetizando, a validade e concretização deste novo paradigma de guerra estará fundamentalmente dependente das capacidades, potenciadas pelas novas tecnologias, inerentes às funções de Comando, Controlo, Comunicações, Computadores, Informações, Vigilância e Reconhecimento (C4ISR) (Harz, 2005).

A GCR promove a eficácia dos sistemas de armas através da rápida disseminação da informação, obtida por uma multiplicidade de sensores altamente sofisticados e dispersos por várias plataformas, entre os diversos actores do espaço de envolvimento. Esta forma de estruturar as operações militares permite alterar o tradicional modelo de comando, que se pode agora apoiar em processos de auto-sincronização potenciados pela consciência de situação partilhada (Alberts, 2002: 33).

O conceito GCR tem a sua génese na actividade comercial dos finais do século XX. Inicialmente desenvolvido pelas forças navais americanas, foi alvo de diversos ajustamentos, em função das especificidades próprias de cada país, o que implica alguma complexidade na a sua compreensão. A importância que lhe tem sido dedicado quer pela NATO, quer pela União Europeia (UE), ou mesmo em outras operações de coligação, tem servido de modelo para muitas nações que reconhecem as operações militares em rede como um instrumento de afirmação política e militar (Vicente, 2005: 3-5).

Uma fotografia rigorosa sobre um cenário GCR iria revelar três cores distintas que reflectiriam um fenómeno tridimensional: uma dimensão humana; uma dimensão de processos; e uma dimensão tecnológica (Hobbins, 2005). Cumprindo a linha orientadora da investigação, serão apenas abordadas as questões que directamente se referem à dimensão

tecnológica, pois será esta a providenciar as info-estruturas requeridas à comunhão entre os vários actores das operações militares, bem como promover a interoperabilidade.

Da síntese das ideias principais até agora manifestadas, irrompe a problemática que delimita a investigação – as recentes aquisições e programas de modernização de sistemas de armas da FAP cumprem com os requisitos técnicos necessários para a interoperabilidade num cenário de GCR?

a. O conceito GCR

De acordo com as perspectivas de diversos autores, podem encontrar-se várias hipóteses para a definição deste conceito, todavia todas revelam matrizes consensuais alicerçadas em pilares comuns – interligação, superioridade informacional, e consciencialização partilhada.

Resolveu apresentar-se neste trabalho uma definição que abrangesse todos os aspectos elementares do conceito. Assim, define-se GCR como “um conceito de operações impregnado de superioridade informacional que gera potencial de combate por meio da interligação em rede de sensores, decisores e atiradores, a fim de atingir uma consciencialização partilhada, velocidade de comando aumentada, um ritmo de operações mais elevado, maior letalidade, maior sobrevivência e um determinado nível de auto-sincronização. Essencialmente, GCR traduz superioridade informacional em poder de combate por meio da interligação de entidades reconhecíveis no espaço de batalha” (Alberts, 2003a: 2).

O conceito GCR abrange os elementos clássicos de uma força de combate incluindo o planeamento, a logística, os elos C4ISR, unidades de combate e os sistemas de emprego de armas.

Transferir os tradicionais conceitos de guerra para a GCR poderia traduzir-se na aplicação de uma única capacidade – partilha de conhecimento em tempo real. Em teoria, parece uma expressão demasiado simplista, contudo na prática implica a criação e manutenção de um universo imensamente rico em informação, só possível pelo uso das tecnologias adequadas.

Cada palavra encerra um vasto rol de significados. “Partilha” envolve um equilíbrio de redes interligadas que oferecem ligações tridimensionais a todas as unidades de uma força, o que representa um enquadramento significativamente

diferente daquele que ainda hoje se apresenta em cenários militares, demasiado estreito e vertical (Harz, 2005).

“Conhecimento”, quando comparado com “informação”, reflecte uma grandeza diferente. A geração do conhecimento, por vezes denominado “informação enriquecida”, tem implícita uma íntima ligação de comunidades especificamente dedicadas a áreas de interesse, apoiadas em eficazes fluxos de informação e na capacidade de sentir a *ground truth* – informação de elevada qualidade que é contextualizada, através de padrões de confiança, validada e distribuída (Harz, 2005).

Finalmente, a partilha de informação em tempo real, o que implica ultrapassar os tradicionais longos processos de recolha, tratamento e posterior disseminação de informação, através dos lentos níveis de comando.

Os processos na GCR deverão, por exemplo, permitir a recolha de imagem através de uma aeronave não tripulada (UAV), melhorada com detalhes de informação fornecidos por observadores aéreos, e enviá-la a uma unidade de combate que a poderá usar como factor de planeamento para a manobra. Os combatentes numa frente de batalha podem usar câmeras de vídeo para enviar informação de alvos, com base em tecnologia *Internet Protocol* (IP) sem fios, e assim potenciar o emprego de armas remotamente controladas.

Este nível de conectividade entre os quartéis-generais e as linhas da frente trouxe para o seio militar um novo conceito – *power to the edge*. Sucintamente, esta aproximação traduz-se numa nova forma de relacionamento e de operação entre os indivíduos, as organizações e os sistemas, envolvendo a transmissão de poder para os indivíduos que se encontram no extremo da organização (Alberts, 2003b: 4).

Considerando que informação e tecnologias da informação significam coisas diferentes para contextos diferentes, é importante compreender as distinções que desse facto possam advir. A palavra “informação” é usada frequentemente para identificar vários pontos do espectro da informação que transformam dados em conhecimento. Por conseguinte, informação tem um significado diferente, dependendo do domínio envolvente. Actualmente definem-se quatro domínios – físico, informacional, cognitivo e social (Figura 1) – cada um dos quais descreve e define a informação de modo diferente (DoD, 2005: 21). Existe, contudo, uma base fundamental que reside na evidência da informação como o resultado de observações individuais, dependentes de um contexto significativo. Assim, a

informação pode definir-se de acordo com o domínio onde vai ser considerada e operada (Phister, 2004).

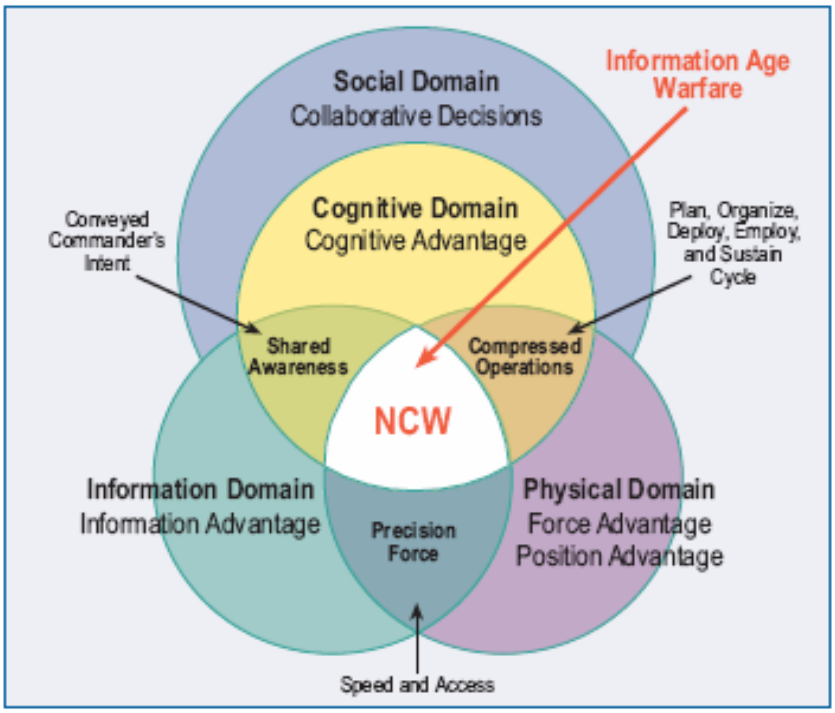

Figura 1 - Os Domínios (Fonte: DoD, 2005)

Resumindo, a GCR traduz a vantagem da informação colocando-a à disposição do processo de decisão em combate, aumentando a sua eficácia e rigor. A vantagem da informação só será evidente quando potenciada por uma rede robusta alicerçada em forças bem informadas e geograficamente dispersas. Esta vantagem caracteriza-se pela partilha de informação, pela partilha da consciência da situação e pelo conhecimento das intenções do comandante (Yang, 2004: 3).

Por outro lado, a vantagem em combate irá explorar as mudanças de comportamento e as novas doutrinas, aumentando a auto-sincronização de cada elemento, a velocidade de comando e o aumento do potencial de combate (Garstka, 2005).

b. O conceito *NATO Network Enabled Capability* (NNEC)

A génese do conceito NNEC está na adaptação do modelo britânico NEC que, por sua vez foi inspirado na ideia original de NCW, desenvolvida nos Estados Unidos da América (EUA).

A origem do NNEC pressupõe uma estreita relação entre os elementos envolvidos na ligação de sensores, decisores e executantes, promovendo uma capacidade operacional NATO, centrada em rede, baseada em efeitos (Figura 2). Desta forma pretende-se a projecção, o emprego e a sustentação de conjuntos de forças, capazes de transformarem a informação em aumento de potencial de combate e eficácia de missão. (Vicente, 2005: 2-5)

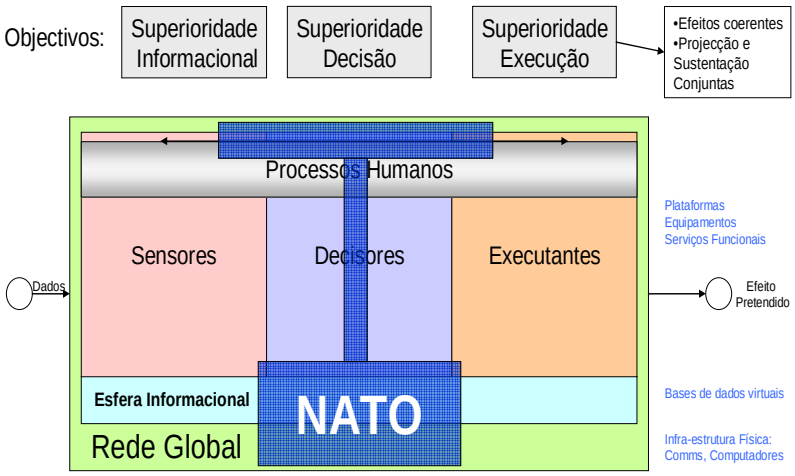

Figura 2 – NATO Network Enabled Capability (Fonte: ACT - NATO)

Quanto aos sensores, elementos cuja função é a recolha de dados e a posterior conversão em informação, podem ser humanos ou tecnológicos. No âmbito da investigação apenas serão considerados os sensores tecnológicos.

A rede global consiste na info-estrutura, composta por computadores e sistemas de comunicação, que fornece a capacidade física de *plug-and-play*[1], para se atingir a conectividade entre as diversas entidades participantes. Esta estrutura, considerada como uma "rede de redes", deve possuir como características essenciais um alcance e largura de banda suficientes para a execução de operações em todo o espectro, incluindo agências nacionais, internacionais e não-governamentais (Vicente, 2005: 2-5).

O desenvolvimento do conceito NNEC, expresso no *NNEC Feasibility Study*[2] (versão 2.0) e no *NATO NNEC Roadmap*[3], é recomendado por muitas das

[1] Característica de um computador que permite a adição de novos dispositivos, normalmente periféricos, sem requerer reconfigurações ou instalações manuais dos dispositivos.
[2] Estudo elaborado por 12 nações, para desenvolver o âmbito e a visão da NATO para a NNEC, assim como para estabelecer o contexto necessário para o desenvolvimento dos aspectos de C3 da NNEC.

nações aliadas como o mais eficaz, quando equacionadas as futuras operações militares. Por outro lado, será o melhor caminho para as nações investirem nas tecnologias da informação e em capacidades de GCR que possam contribuir para o sucesso das forças multinacionais (Figura 3). A NNEC possibilita o ambiente adequado para a criação de uma aproximação comum às futuras operações, através da implementação de estruturas, padrões, processos e procedimentos necessários para potenciar a flexibilidade e a agilidade, absolutamente vitais para a condução de operações GCR num contexto de coligação (NATO C3A, 2005: 2), ou em operações conjuntas.

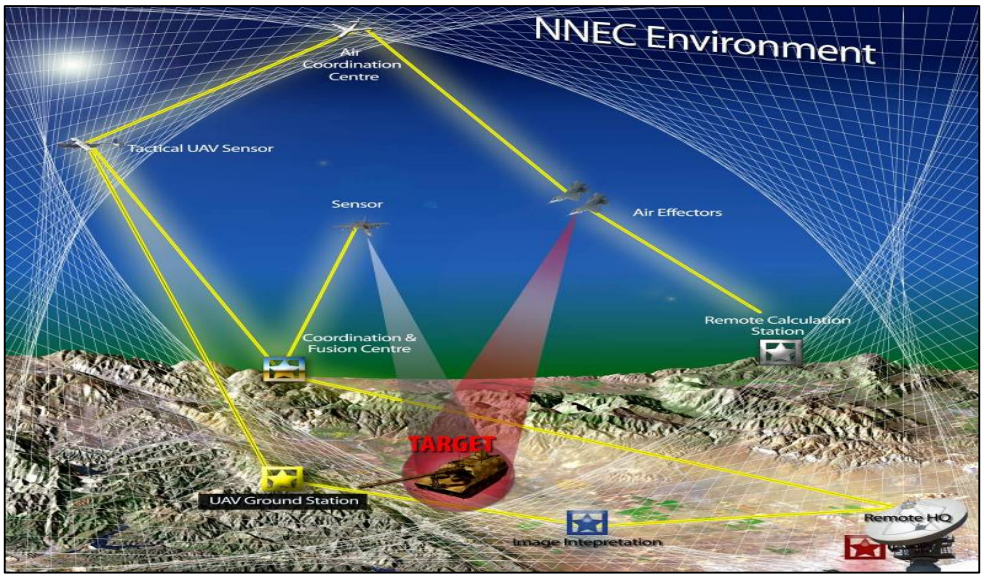

Figura 3 – Ambiente NNEC (Fonte: ACT - NATO)

Considera-se pertinente, antes de iniciar a análise de tecnologias e de requisitos técnicos relacionados com a GCR, no âmbito NATO, descrever os atributos que se reconhecem como potenciadores do conceito NNEC (NATO, 2006: 1-4):

- utilização de uma rede que encerra um “núcleo protegido” para comunicações em voz, dados e vídeo, com interoperabilidade melhorada entre redes estáticas e móveis, baseadas em tecnologia IP;
- utilização de várias formas de tecnologia de mensagens, capazes de suportar a transferência de dados entre máquina-máquina, utilizador-utilizador e máquina-utilizador;

[3] Documento que reflecte a estratégia e os planos de acção para o desenvolvimento e a implementação da NNEC.

- capacidade para utilizar ferramentas de consciência situacional comuns e adaptadas à realidade operacional (e.g., *Common Operational Picture*);
- identificação de Comunidades de Interesse (COI[4]) *ad hoc* formais e informais, como um meio para aumentar a colaboração entre organizações, missões e fronteiras nacionais;
- utilização de ferramentas de colaboração avançadas, capazes de providenciar sinergias entre estruturas verticais e horizontais, apoiando processos de planeamento adaptativo;
- proliferação de sensores e de capacidades de partilha de informação a todos os níveis de actividade, contribuindo para adaptações extremamente rápidas de acções operacionais, baseadas na contínua actualização da informação;
- transferência de informação *seamless*[5] entre utilizadores e entre aplicações ligadas de formas múltiplas sobre vários domínios.

Estes atributos chave que reflectem uma imagem do que o conceito NNEC poderá oferecer à Aliança Atlântica, determinam as bases do trabalho que foi iniciado em 2006 e que irá decorrer ao longo dos próximos anos. O completo estabelecimento da interoperabilidade tecnológica é um desiderato possível mas seguramente demorado, como se depreende do *NATO NNEC Roadmap*. Todavia, para os países que pretendem participar em futuras forças da NATO, implica uma rápida tomada de consciência, participando nos grupos de trabalho já existentes ou em formação, cujo objectivo passará pela definição de requisitos técnicos, estruturantes para as capacidades C4ISR de uma força em ambiente NNEC.

c. Tecnologias associadas

Um cenário de GCR inclui uma família de sistemas C4ISR baseados na superfície, no ar e no espaço, que partilham informação integrada, horizontal e

[4] Termo utilizado para descrever qualquer grupo de colaboração de utilizadores que devem trocar informação, perseguindo os seus objectivos partilhados, os seus interesses, missões ou processos de actividade e que, por conseguinte, devem possuir um vocabulário partilhado para a informação trocada. (Fonte: NATO C3 BOARD, 2006b): --)

[5] *Seamless* é definido como "perfeitamente consistente e coerente." Partilha de dados "*seamless*" significa que os dados serão utilizados entre múltiplas plataformas sem que sejam notadas alterações depois dos dados serem transferidos. (Fonte: http://www.thefreedictionary.com)

verticalmente, através de conexões entre equipamentos, potenciadas por uma rede de sensores, por centros de comando e por atiradores (Hobbins, 2005).

Um dos primeiros elementos a considerar no campo da tecnologia é a garantia da conectividade global – a rede. Actualmente, a pedra basilar da conectividade global, e que tem estado em grande evidência nos estudos da GCR, é a *Global Information Grid* (GIG), a qual será abordada em maior detalhe no segundo capítulo. Esta deverá ser conduzida até ao nível táctico, fundindo as informações de forma a produzir uma consciência situacional em tempo real, provocando uma maior eficácia nos processos de Comando e Controlo (C2). Para tal é necessário criar redes robustas e fiáveis, assim como sistemas periciais que corram nessas redes. As redes (espaciais, aéreas e terrestres) materializam os sistemas de recolha e entrega de informação processados pelas aplicações que apoiam as unidades envolvidas no espaço de batalha (Hobbins, 2005).

Ainda dentro da conectividade global, podem definir-se quatro subgrupos, que traduzem o esforço tecnológico da GCR (Hobbins, 2005):

- o investimento contínuo na modernização de sensores que contribuem para as capacidades inerentes ao C4ISR;
- a grande preocupação em melhorar os centros de comando para as componentes aérea, marítima e terrestre, dotando-os de equipamentos sofisticados e compatíveis com o nível tecnológico que é aplicado nos sistemas de armas;
- os esforços para aumentar a conectividade entre as redes e entre os nós móveis, através da extensão do alcance das comunicações para além da linha de vista. Os novos requisitos dos sistemas de comunicações centram-se no aumento da flexibilidade, da largura de banda e da cobertura global;
- o desenvolvimento de redes com IP no espaço de batalha, com quatro canais redundantes de comunicações e sistemas de *Data Link* comuns ou compatíveis, que sustentam as tecnologias de redes de *Tactical Targeting*[6], as formas de onda de redes de banda larga e os programas de

[6] Processo de selecção de alvos, assegurando a resposta adequada aos mesmos, tendo em atenção os requisitos e capacidades tácticas. (Fonte: JP 1-02 DOD)

Joint Tactical Radio System (JTRS), equipamento que será descrito no capítulo seguinte.

As aplicações integradas nos sistemas de *Data Link* reflectem também os avanços tecnológicos. O *software* do *Link 16* permite a recepção, o processamento e a transmissão em tempo real de informações sobre combustível, armamento, aspectos de manutenção, bem como da avaliação do piloto sobre os efeitos causados por um ataque a um alvo. Esta informação é automaticamente enviada a um Centro de Operações Aéreas Combinado (CAOC), onde os planeadores podem reavaliar a situação táctica e decidir em pouco tempo alterar o emprego dos sistemas de armas em face do novo cenário.

Este *software* foi testado com sucesso no exercício *Joint Expeditionary Force Experiment 2004*[7], tendo-se verificado uma drástica redução no tempo que decorreu entre a detecção de um alvo, o seguimento, a identificação, a aquisição para ataque pelo SA e a avaliação para posterior envio ao decisor (Hobbins, 2005).

Aceitando como pressupostos que uma conectividade robusta e sofisticados sistemas de informação são essenciais para um sistema completamente integrado, reveste-se de vital importância o fluxo de informação.

Num cenário de GCR a conectividade baseada em terra não é aparentemente problemática. A enfâse deve ser dada à conectividade da rede que se deve estabelecer nas comunicações ar-terra-ar e ar-ar, pois serão elas a determinar o sucesso das operações. O fluxo de informação começa quando um utilizador introduz dados através de um interface (normalmente um teclado, um rato ou uma combinação no monitor) ou quando um sensor recebe e transmite dados. A partir dessa fase, a informação flúi através de várias etapas de aplicação e controlo até à camada de codificação de transporte, onde é traduzida pelo protocolo adequado e posteriormente enviada pela linha de transmissão. Uma vez que o protocolo IP providencia o padrão flexível usado por todas as aplicações e programas actuais, a tradução da informação para IP torna-se o elemento crítico para a interoperabilidade. A transmissão da informação pode ocorrer por cabo (rede terrestre) ou por satélite e ou transmissão rádio para as redes aéreas. No destino,

[7] Exercício realizado pela Força Aérea dos Estados Unidos, na Base Aérea de Nellis, cujo objectivo é exercitar as operações aéreas e espaciais expedicionárias, num cenário de GCR. (Fonte: http://www.eiexpo.org/ documents/Award_Winners_Web_Write_Up_2005v3.pdf)

sucede o processo inverso, transformando a informação codificada em dados “legíveis”. A utilização de protocolos IP será seguramente aceite por todos os sistemas futuros, garantindo que forças conjuntas e combinadas possam comunicar entre si.

Para alimentar a referida rede, vamos encontrar outro factor cuja essência é baseada nos avanços tecnológicos – os sensores. Os radares de abertura sintética, os satélites, os sistemas de geo-localização ou os sistemas electro-ópticos de alta definição, entre muitos outros, ameaçam alterar o equilíbrio de forças nos modernos teatros de operações.

Os sensores, considerados como um dos grandes catalizadores da GCR e das capacidades C4ISR, são instrumentos que respondem a estímulos físicos (como o calor, a luz, a pressão do som, o magnetismo ou o movimento). Eles recolhem e medem dados referentes a fenómenos, objectos ou materiais. Tipicamente, os sensores que equipam plataformas militares correspondem a câmaras de vídeo ou fotográficas, sistemas de laser, sistemas de infra-vermelho, receptores de frequências rádio, sistemas de *radar*, sistemas *sonar*, dispositivos de leitura térmica e magnetómetros.

As tecnologias que passaram a integrar as arquitecturas dos sistemas de sensores, oriundas do universo digital, aumentaram o seu alcance e a sua polivalência, tornando-os mais activos e partilhados.

A grande diversidade de sensores, aliada à capacidade centrada em rede proporciona a combinação e sobreposição de dados recolhidos, quer por sensores orgânicos, quer por sensores de outras plataformas (*off-board sensors*). Este esforço sinérgico é fundamental para incrementar a probabilidade de detecção e reduzir os falsos alarmes, um dos grandes obstáculos às missões de reconhecimento e vigilância, assim como às fases de aquisição de alvos.

Finalmente, o outro factor responsável pelo sucesso das operações num ambiente de GCR, também dependente da tecnologia, é representado pelos sistemas de comunicações. Nos dias de hoje, os terminais para troca de informação baseiam-se em tecnologias digitais. Actualmente a troca de informação pode ser executada por equipamentos terminais de diversos tipos, como: um telefone; um computador que pode transmitir texto, voz, áudio, imagem parada ou vídeo; uma fotocopiadora ou um *scanner*; ou um equipamento que execute multi-funções. Estas tecnologias possibilitaram o aparecimento de equipamentos de rádio,

altamente versáteis, que permitem a utilização de diversos tipos de forma de onda como seja o JTRS, ou a evolução dos equipamentos de *Data Link*. Por outro lado, os satélites de comunicações vêem agora as suas capacidades aumentadas pelas exigências da troca de informação em rede.

Após uma breve apresentação dos conceitos da GCR, bem como dos seus reflexos no âmbito da Aliança Atlântica, dando origem ao NNEC, foram sumariamente introduzidas as tecnologias inerentes à materialização dos referidos conceitos. Foram desta forma abordadas as questões derivadas – Quais as recentes abordagens aos conceitos GCR e NNEC? – e – Quais são as tecnologias da GCR?

O próximo capítulo irá aprofundar as temáticas da tecnologia e dos requisitos técnicos, enquadrados por um dos pilares das operações em rede – a interoperabilidade.

2. Requisitos técnicos para operações em ambiente NNEC

Os requisitos técnicos estão intrinsecamente relacionados com os sistemas que promovem as capacidades C4ISR, que por sua vez materializam o elemento nuclear das operações em rede. Por conseguinte, serão apresentados os sistemas que apoiam as três áreas já identificadas anteriormente – os sensores, os sistemas de comunicações e as redes. Por outras palavras, restringiu-se o espaço de investigação à capacidade de disponibilizar a informação obtida pelos sensores ou as ordens do comandante, em tempo oportuno, às entidades apropriadas e com a segurança adequada, o que depende exclusivamente da robustez e eficácia da rede de comunicações existente.

Por outro lado, será também definida uma das características essenciais para uma eficaz operação em rede – a interoperabilidade. Deste desiderato, amplamente estudado e desenvolvido no areópago da GCR, depende o valor dos sensores e sistemas envolvidos.

Unidades interoperáveis são o grande catalizador das operações em rede, donde resulta a extraordinária preocupação com as questões relacionadas com a interoperabilidade.

O capítulo irá remeter uma primeira parte para assuntos do foro da interoperabilidade, onde serão apresentados conceitos, níveis e requisitos.

Seguidamente serão analisados os sistemas, que configuram os requisitos técnicos, já referenciados. A sua exposição decorrerá em dois tempos distintos: sistemas actuais e sistemas emergentes. Desta forma, pretende-se esclarecer quais os requisitos necessários, considerados como atributos essenciais para a interoperabilidade entre sistemas de armas, no âmbito de operações NNEC.

a. Interoperabilidade

As tecnologias da informação tornaram-se o farol das operações militares, facto evidente na crescente dependência nos sistemas de informação para a recolha, a organização, o auxílio à tomada de decisão e à sua disseminação. Por conseguinte, a colaboração entre sistemas próprios de cada estado para apoiar as operações de coligação é fundamental. Este tipo de colaboração é referido como a interoperabilidade de sistemas.

A capacidade para trabalhar em conjunto necessita simultaneamente de ocorrer a um determinado nível para permitir a comunicação entre entidades, a partilha de informação e a colaboração. O grau de interoperabilidade entre forças irá afectar directamente a sua capacidade para conduzir operações num ambiente de GCR (Alberts, 2003b: 107).

A interoperabilidade deve estar presente em todos os domínios: o físico; o informacional; o cognitivo e o social. Primeiro, todas as unidades pertinentes necessitam de estar ligadas à rede. Segundo, as unidades devem ser capazes de fornecer informação às outras unidades que estão na rede. Terceiro, as unidades devem saber encontrar, recolher e compreender a informação disponível na rede. Quarto, as unidades podem ter a necessidade de participar num ou mais ambientes ou processos de colaboração (Alberts, 2003b: 108).

As entidades que não sejam interoperáveis, ou que tenham uma interoperabilidade limitada, não conseguirão ter acesso a toda a informação disponível, não terão a capacidade para oferecer informação às entidades que dela venham a necessitar e estarão limitadas nas formas de colaboração e esforço conjunto.

(1) Conceito de Interoperabilidade

Interoperabilidade é a capacidade que os sistemas, unidades ou forças, detêm para disponibilizar dados, informações, materiais ou serviços, assim como recebê-los de outros sistemas, unidades ou forças. É ainda a capacidade que os mesmos sistemas, unidades ou forças, possuem para utilizar os dados, informações, materiais ou serviços, transferi-los entre entidades, potenciando uma eficaz operação conjunta (Call, 2003).

As perspectivas sobre a interoperabilidade são diversas e requerem contextualização específica. No âmbito da investigação, apenas será estudada a interoperabilidade técnica.

(2) Níveis de Interoperabilidade

Existem diversos modelos de referência que procuram caracterizar os níveis de interoperabilidade técnica entre sistemas. A comunidade militar identificou dois modelos principais fundamentais: o modelo *NATO C3 System Architecture Framework Reference Model for Interoperability* (NMI), incluído na *NATO Consultation, Command and Control (C3) TechnicalArchitecture* (NC3TA) (Anexo A); e o modelo *Level of Information Systems Interoperability* (LISI), publicado pelo Departamento de Defesa (DoD) dos EUA.

O modelo de referência para a interoperabilidade NMI está definido em níveis e sub-níveis. Os níveis de interoperabilidade definem um modelo de maturidade que reflecte a sofisticação da mesma. Os sub-níveis de interoperabilidade descrevem um modelo de capacidade que reproduzem a funcionalidade disponível. Estes níveis enfatizam o valor residente na troca de dados estruturada e automatizada, bem como na interpretação dos dados, para um aumento na eficácia operacional (Carney, 2004).

O modelo LISI (Figura 4 – Modelo original no Anexo B) identifica quatro domínios: procedimentos e políticas, aplicações, dados e infra-estrutura. Em cada um destes domínios, são enumerados níveis de interoperabilidade, que dão origem a cinco categorias de interoperabilidade técnica (Clark, 2001):

Nível 0: Isolado (Manual) – Não ligado, mecanismos manuais (e.g. disquete);

Nível 1: Ligado (*Peer-to-Peer*) – Ligação electrónica; dados e aplicações separados (e.g. correio electrónico);

Nível 2: Funcional (Distribuído) – Funções mínimas comuns; dados e aplicações separados (e.g. HTTP);

Nível 3: Domínio (Integrado) – Dados partilhados; aplicações separadas;

Nível 4: Empresa (Universal) – Manipulação interactiva; dados e aplicações partilhados.

<table>
<tr><th colspan="3" rowspan="2">Nível (Ambiente)</th><th colspan="4">Atributos de interoperabilidade</th></tr>
<tr><th>Procedimentos</th><th>Aplicações</th><th>Infra-estrutura</th><th>Dados</th></tr>
<tr><td rowspan="3">Empresa (universal)</td><td rowspan="3">4</td><td>c</td><td>Multi-nacional</td><td rowspan="2">Interactivo</td><td rowspan="3">Topologias Multi-dimensionais</td><td>Modelos de empresa cruzados</td></tr>
<tr><td>b</td><td>Intra-governamental</td><td rowspan="2">Modelos de empresa</td></tr>
<tr><td>a</td><td>Departamento de Defesa</td><td>Cortar e colar objectos</td></tr>
<tr><td rowspan="3">Domínio (integrado)</td><td rowspan="3">3</td><td>c</td><td rowspan="3">Domínio</td><td>Dados partilhados</td><td rowspan="3">Rede Alargada (WAN)</td><td>DBMS</td></tr>
<tr><td>b</td><td>Colaboração em grupo</td><td rowspan="2">Modelos de Domínio</td></tr>
<tr><td>a</td><td>Cortar e colar texto</td></tr>
<tr><td rowspan="3">Funcional (Distribuído)</td><td rowspan="3">2</td><td>c</td><td rowspan="2">Ambiente de operação comum</td><td>Motor de busca</td><td rowspan="2">Rede Local (LAN)</td><td rowspan="3">Modelos de programa & formatos de dados avançados</td></tr>
<tr><td>b</td><td>Aplicação Office</td></tr>
<tr><td>a</td><td>Programa</td><td>S. Mensagens avc.</td><td>Rede</td></tr>
<tr><td rowspan="4">Conectado (ponto-a-ponto)</td><td rowspan="4">1</td><td>d</td><td rowspan="2">De acordo com padrões</td><td>S. Mensagens bsc.</td><td rowspan="2">Dois sentidos</td><td rowspan="3">Formatos básicos de dados</td></tr>
<tr><td>c</td><td>Transferência ficheiros</td></tr>
<tr><td>b</td><td>Perfil de segurança</td><td>Interacção simples</td><td>Um sentido</td></tr>
<tr><td>a</td><td colspan="3"></td></tr>
<tr><td rowspan="5">Isolado (manual)</td><td rowspan="5">0</td><td>d</td><td>Procedimentos de troca de Media</td><td rowspan="4">Não aplicável</td><td>"Media" retirável</td><td>Formatos de "media"</td></tr>
<tr><td>c</td><td rowspan="3">Controlos de acesso de pessoal</td><td rowspan="3">Reentrada manual</td><td rowspan="3">Dados privados</td></tr>
<tr><td>b</td></tr>
<tr><td>a</td></tr>
<tr><td>0</td><td colspan="4">Sem interoperabilidade conhecida</td></tr>
</table>

Figura 4 – Modelo LISI (Fonte: Clark, 2001)

De acordo com alguns autores o modelo NMI apenas encerra quatro graus, não considerando o grau "0". Todavia, se nos referenciarmos a um autor que também apresente o referido grau, é pertinente a existência de uma correspondência entre os dois modelos (Nunes, 2004). Esta correspondência será fundamental para definir o nível de interoperabilidade dos sistemas de armas em análise neste estudo.

b. Sistemas Actuais

A revolução contínua nas tecnologias de sensores promete vantagens consideráveis para as capacidades C4ISR. A nova geração de sensores miniaturizados, de alta resolução, com boa razão custo-eficácia, que podem ser equipados em veículos espaciais, aéreos, terrestres ou marítimos, irão significativamente aumentar a capacidade militar nas áreas da vigilância, detecção, seguimento e aquisição de alvos em tempo real, prometendo levantar o “nevoeiro da guerra” e oferecendo aos comandantes militares uma melhor consciência da situação.

(1) Sensores

A parte mais importante dos dados de Informações, Vigilância e Reconhecimento (ISR) provém dos satélites, e das plataformas aéreas, tripuladas ou não tripuladas (Nolin, 2006).

Actualmente, existem sistemas para plataformas aéreas, que permitem em tempo real, ou quase real, a recolha de informações do espaço de batalha e aquisição de alvos, que são usados na detecção de unidades escondidas, camufladas e em movimento. Estes sistemas incluem câmeras electro-ópticas *dual band* de alta resolução (gama do visível e infra-vermelho), sensores hiper espectrais de infra-vermelho (HSI) *visible-to-near* (VNIR), *short-wave* (SWIR) e *long-wave* (LWIR), radares de abertura sintética (SAR), sensores acústicos, sensores de guerra electrónica (ESM) entre outros (Duncan, 2004?).

A NATO encetou em 2001 o projecto *Coalition Airborne Surveillance and Reconnaissance* (CAESAR), cujo objectivo é ligar os vários meios de vigilância da Aliança, incluindo o J-STARS norte-americano. Este projecto foi substituído pelo *Multisensor Aerospace-Ground Joint ISR Interoperability Coalition Architecture* (MAJIIS), que mantém as mesmas matrizes de operação, tentando alcançar a partilha de dados obtidos por todos os sensores ao serviço da NATO (Nolin, 2006).

(2) Sistemas de comunicações

A era digital promoveu as comunicações via satélite, fazendo emergir outras capacidades e fundamentalmente incrementando os alcances de transmissão, que passaram a ser à escala global. As comunicações via satélite (SATCOM) combinam a capacidade de comunicação para além da linha de vista, usada pelos rádios HF, com a qualidade de transmissão usada pelos rádios VHF. O sistema usa um conjunto de satélites que fazem de relé entre si ao longo de toda a superfície terrestre. O efeito alcançado é uma comunicação global de alta qualidade.

Actualmente, as comunicações militares nos cenários de conflito assentam em pressupostos de comunicação em rede. Começam, assim, a invadir o espaço militar conceitos como protocolos TCP/IP ou WEB.

Nos modernos cenários, onde surgem como elementos nucleares as capacidades C4ISR, podem identificar-se dois tipos de *Data Link*, com modo seguros e capazes de transmissão a longo alcance e linha de vista: os *Data Link* para partilha de consciência da situação, que disseminam automaticamente a informação actualizada do espaço de batalha entre plataformas aéreas, navais ou terrestres, formando uma rede de informação; e os *Data Link* ISR de banda larga (Goodman Jr., 2005).

***Link 11*.** Também conhecido como TDL A (ou TADIL A) nos EUA, o *Link 11* aplica técnicas de comunicação em rede usando formatos de mensagem padrão. Os dados são trocados através de uma forma de onda convencional para *Link 11*. Uma vez que este tipo de onda é susceptível às contra-medidas electrónicas (ECM), foi efectuada uma recente alteração que permite uma grande resistência ao empastelamento, através de tecnologias *Single Tone Link Eleven Waveform* (SLEW) e *Full Tail Biting Convolutional Block* (FTBCB).

Link 16. O *Data Link* para partilha da consciência situacional mais conhecido é o *Joint Tactical Information Distribution System* (JTIDS), ou *Multifunctional Information Distribution System* (MIDS), numa versão mais recente e uma menor volumetria, permitindo a sua integração nas aeronaves F-16 e F-18. Este sistema vulgarmente denominado em terminologia militar por *Link 16*, cuja tecnologia remonta a 1970, foi implementado pelas forças armadas dos EUA, bem como pela NATO e mais de doze países, incluindo Portugal, nas suas diversas componentes, tornando-o uma excelente ferramenta para o estabelecimento de interoperabilidade entre forças.

Os terminais de *Link 16* são rádios de distribuição de informação digital, resistentes a operações de *jamming*, que permitem a transferência automática (até 256Kbps), em tempo real, da informação referente à situação táctica tridimensional do espaço de batalha. Particularmente, são evidenciadas as localizações das forças terrestres, navais e aéreas, amigas e opositoras, que serão disponibilizadas nos terminais operados pelas forças amigas, como sejam aviões de caça, aeronaves de vigilância, centros de comando e controlo em terra, unidades de defesa aérea ou navios. Todavia, o sistema permite a troca de mais informações com especial relevo para as unidades de comando e controlo, tais como dados de interesse operacional que incluem além da localização, o armamento e o combustível disponíveis, a velocidade, o rumo e a altitude (Goodman Jr., 2005).

(3) Redes

Os recentes estudos sobre as capacidades centradas em rede sugerem o contributo fundamental de conceitos como *Net Readiness* (NR) – prontidão da rede – e da GIG.

O conceito *Net Readiness* implica a existência de condições que cumpram com os requisitos técnicos necessários para a transferência de informação, como por exemplo a acreditação, assim como a eficácia operacional entre terminais (NATO C3 Board, 2004).

O conceito GIG foi desenhado para providenciar uma infra-estrutura integrada para todas as necessidades de informação militares – C4ISR, controlo de fogo e logística – bem como para apoiar a projecção de forças. A GIG permite a separação geográfica e a integração funcional de comando, *targeting*, emprego de armas e ainda funções de apoio. Para além disso, possibilita às forças conjuntas uma compreensão da situação comum, disponibilizando o cenário operacional comum e a informação necessária para um célere processo de decisão. Devem ressalvar-se algumas características chave do GIG, de acordo com o *NATO C3 Board* (2004):

- é uma rede de redes que preconiza uma estrutura distribuída, providenciando conexões integradas;
- perspectiva a utilização de um único ambiente de transporte, baseado na tecnologia IP, com uma declarada intenção de migração para a versão IPv6;
- deve assegurar uma rede nuclear utilizando codificação IP de elevado grau;
- deve suportar a mobilidade quer dos utilizadores quer da própria rede.

As redes proporcionam os serviços de transporte e, dependendo da interpretação do conceito NR, os serviços de informação para os terminais ligados às primeiras. As redes devem ser extensivas a vários domínios – terra, mar, aeroespacial aos níveis estratégico, operacional, táctico – e às várias nações participantes num determinado teatro de operações.

Uma rede consistirá, assim, numa mistura heterogénea de camadas físicas tecnológicas. Em última instância será uma rede de redes, cuja espinha dorsal poderá ser composta pelos próprios terminais (arquitectura típica em rádios de combate ou tecnologia de *datalink* táctico) ou fazendo uso de meios dedicados (nós LAN e ou WAN ou terminais de satélite).

c. Sistemas Emergentes

Quando se fala em sistemas emergentes pode rapidamente extrapolar-se a discussão para as tecnologias emergentes, porque serão estas de facto a determinar as capacidades dos novos sensores.

A aplicação da GCR carece dos recursos mais avançados das tecnologias da Informação (TI), tais como comunicações satélite de banda larga, *Data Links* de alta velocidade, *softwares* de rede, recursos de criptografia, tecnologia de segurança em rede, entre outras (Dias, 2006).

. As tecnologias que seguramente terão um papel principal no palco das acções militares irão trazer novos conceitos e expressões, às quais nos teremos que habituar, como sejam: *Windows Security; Wireless Networking; Ad Hoc Networking; Grid Computing; Power over Ethernet; Nanotechnology; Software Defined Radio*; *Radio Frequency Identification; Fibre Intrusion Detection; Identity Management; Web Services* (NATO C3 Board, 2006a) (Anexo B).

(1) Sensores

O futuro próximo parece não trazer grandes surpresas no que respeita ao aparecimento de novos sensores. As grandes alterações prevêem-se na forma de os integrar e rentabilizar. Este facto remete-nos para um outro projecto da NATO – *Alliance Ground Surveillance* (AGS). Este projecto inclui plataformas aéreas ISR tripuladas e não tripuladas, que permitirão aos comandantes aliados obter uma imagem de superfície do teatro de operações, em tempo real, mesmo durante a noite ou em condições de fraca visibilidade. Contudo, o sistema AGS não conseguirá garantir a identificação de alvos, o que implicará o emprego de plataformas aéreas equipadas com sensores ópticos de alta precisão. Muito provavelmente o sistema AGS será baseado num sensor radar – *Stand-Off Surveillance and Target Acquisition Radar* (SOSTAR) – desenvolvido por cinco países europeus, membros da NATO. O sistema AGS é considerado como uma capacidade essencial para as missões das *NATO Reaction Forces* (NRF) e deverá estar operacional em 2012 (Nolin, 2006).

(2) Sistemas de comunicações

***Link 11*.** No âmbito da NATO, o *Link 11* é primariamente utilizado como um *Data Link* naval. Contudo, a organização pretende adaptá-lo para permitir a introdução de informação respeitante aos mísseis de defesa (*Theatre Missile Defence* - TMD), o que implica a aplicação de *Link 11* nos sistemas de mísseis terra-ar (*Surface-to-Air Missile* – SAM).

***Link 16*.** O sistema *Link 16* é composto por uma componente de *software* (protocolo) e outra componente de *hardware* (rádios). A este binómio *software* e *hardware* está associada uma forma de onda específica do sistema, daí que alguns autores inclusivamente definam *Link 16* como uma forma de onda. (Goodman Jr., 2005)

A conversão deste sistema apenas para uma componente de software permitiria o seu uso por tipos de rádio mais versáteis e capazes de melhorar os critérios de interoperabilidade.

Um destes rádios é conhecido por *Joint Tactical Radio System* (JTRS). É um equipamento definido por *software*, ou seja, permite a utilização conjunta com computadores. Um equipamento deste tipo converte sinais de rádio analógicos em dados digitais. Desta forma, é possível alterar a forma de onda e as frequências, tal como se estivessem a operar diferentes aplicações num normal computador pessoal. O *Link 16* será um dos diferentes sistemas legados instalados como software no JTRS, permitindo a interoperabilidade entre as plataformas que possuam este equipamento e os terminais JTIDS ou MIDS (Goodman Jr., 2005).

IPv6. Para cumprir os desígnios da GCR, é aceite pela comunidade internacional que o futuro protocolo comum de comunicações será o IPv6, permitindo a partilha de voz, dados e vídeo, entre todos os níveis de uma operação, desde o combatente e os sensores, até às plataformas de armas, à logística, ao planeamento e às operações estratégicas.

O IPv6 é já considerado o alicerce da interoperabilidade para o GIG da DoD, que actualmente desenvolve sistemas que utilizam a tecnologia da Internet para oferecer a integração, sem erros, de informação entre UAV, helicópteros ou soldados no terreno, e o Pentágono.

Provavelmente, o passo inicial para integrar sistemas legados numa GIG com IPv6, será a inclusão de portas (*gateways)*. Este procedimento consiste na colocação de um subsistema inteligente, que integra uma ligação externa de banda larga, permitindo a interligação à GIG. Os *gateways*, além da ligação de rede, providenciam a tradução da informação de sistemas legados (MIL-STD-1553B[8] ou RS-485[9]) para o novo protocolo IP.

O modo ideal para implementar as referidas portas, será através de componentes Commercial Off-The-Shelf (COTS), como seja uma placa *Ethernet*[10] para IPv6.

Conseguir implementar os sistemas de comunicações baseados em *Ethernet* será um enorme desafio, pois requer mais largura de banda, sem fios, do que a que actualmente dispomos. Todavia, a intenção de introduzir o IPv6 irá levar os sistemas de comunicações ao coração das plataformas, aos seus sistemas e subsistemas.

Este facto irá potenciar a partilha de dados mas também a operação e o controlo de sensores, armas, sistemas de navegação e até da potência das aeronaves, a partir de uma agência remota ou múltiplas agências e utilizadores.

A curto ou médio prazo, os sistemas de comunicação em aeronaves, alvo do nosso estudo, além das óbvias características de mobilidade, devem suportar tecnologia de serviços *WEB* e portais.

(3) Redes

O valor da GCR poderá ainda estar por provar, subordinando-se o seu futuro reconhecimento aos avanços que deverão acontecer nas diversas tecnologias envolvidas (Dias, 2006). Novas redes de comunicações, móveis, de alta velocidade, altamente seguras, que possam ser estabelecidas em minutos, serão seguramente desenvolvidas.

[8] Protocolo e canal de transmissão de dados. (Fonte: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber =562795

[9] Tecnologia de interconexão para redes locais – *Local Area Networks* (LAN) – baseada no envio de pacotes.

[10] Idem

> Novos algoritmos de compressão, que poderão reduzir significativamente o tamanho dos pacotes de dados transmitidos pelo vastíssimo rol de fontes de informação, deverão ser criados para que coincidam com os avanços na tecnologia de redes móveis.
>
> Finalmente, deverá ser construída uma aplicação baseada em componentes integrados que suporte elementos *plug-and-play*. Deverão ainda ser desenvolvidas outras aplicações integradas, que apoiem a gestão estratégica do espaço de batalha, da logística e da atribuição de recursos dinâmicos, para possibilitar a exploração eficiente e eficaz dos aspectos relacionados com a administração de conhecimento, decorrente das capacidades da GCR. Apesar da enorme tarefa que se adivinha, o valor acrescentado pelas novas capacidades é previsivelmente compensador.
>
> Enquadrando a descrição e os conceitos associados aos requisitos técnicos necessários para a operação em ambiente NNEC, deve dizer-se que a estratégia da NATO, para o desenvolvimento dos aspectos relacionados com as redes e com a partilha de informação, se centraliza num esforço conjunto para estabelecer quer a rede de sistemas, quer os sistemas de informação nacionais e NATO. Daqui resultaria uma capacidade decorrente de uma “federação de sistemas” que implementaria uma *Networking and Information Infrastructure* (NII). O conceito “federação de sistemas” refere-se a um conjunto de diferentes sistemas, que não são geridos por uma entidade central, mas que estão interligados de forma a produzir resultados que não seriam alcançáveis pela intervenção dos sistemas de forma isolada. A referida NII deverá ser considerada como uma combinação de segmentos de NII nacionais e de uma NII NATO (NNII), que conjuntamente poderão providenciar capacidades que nenhum outro sistema único será capaz de oferecer (NATO C3A, 2005:5).

Ao longo deste capítulo ficaram expressos o conceito, os níveis e os requisitos para a interoperabilidade, assim como foram dissecadas diversas áreas da tecnologia, que pretenderam reflectir os cenários tecnológicos actuais e emergentes. Deste modo, foram satisfeitas mais duas questões derivadas que contribuem para a realização da investigação: “Em que consiste a interoperabilidade?”; e “Quais são os requisitos técnicos das tecnologias da GCR?”

Seguidamente, serão observados os sistemas de armas, alvo do presente estudo, onde será verificada a presença dos requisitos técnicos, anteriormente mencionados, que contribuem para a interoperabilidade, de acordo com os modelos de análise definidos.

3. As recentes aquisições e programas de modernização dos sistemas de armas da Força Aérea Portuguesa

Neste capítulo será apresentado o problema da interoperabilidade face aos sistemas de armas adquiridos e programas de modernização da FAP. Para tal, foram destacados três programas como objecto de investigação: F-16 MLU, EH101e P-3C CUP+.

Para a caracterização do problema, considerou-se a partilha de informação entre os referidos sistemas de armas e entidades que estejam integradas no espaço de batalha.

Assim, para os diferentes sistemas de armas, será feita uma análise dos sistemas de comunicação, particularmente no que respeita a sistemas de *Data Link* ou outros afectos à partilha de informação táctica em tempo real, de modo seguro. Serão também mencionados os sensores que integram os sistemas de armas, uma vez que também estes são essenciais para a eficácia das capacidades C4ISR.

No final, e tendo por referência os níveis de interoperabilidade, resultantes dos requisitos técnicos que foram descriminados nos capítulos anteriores, serão enunciadas as conclusões que determinarão a menor ou maior capacidade de cada SA para a operação em ambientes NNEC.

a. F-16 MLU

A Força Aérea Portuguesa decidiu aderir ao programa de modernização das aeronaves F-16 denominado MLU, perseguindo diversos objectivos, entre os quais suprir as lacunas evidenciadas pelo F-16 *Operational Capabilities Upgrade* (OCU) em diversas capacidades, particularmente a capacidade para partilha de informação táctica num cenário NNEC.

Tabela 1 – Sensores do F-16 MLU (Fonte: Lockheed, 2004)

Sensores				
Activos		Passivos		Outros
Radar	Guerra Electrónica	Electro-óptico	Guerra Electrónica	
APG-66(V2)	ALQ-131	Targeting POD (Laser e IR)	RWR SPS-1000 (V5)	*Joint Helmet Mounted Cueing System* (JHMCS)

Tabela 2 – Sistemas de comunicações do F-16 MLU (Fonte: Lockheed, 2004)

Sistemas de Comunicações		
Voz		Dados
VHF	UHF	*Data Link*
ARC-164 (Have Quick II)	ARC-164 (Have Quick II)	MIDS (*Link 16*) Improved Data Modem (IDM)

O F-16 MLU, baseado no sistema de comunicações de *Data Link* MIDS (*Link 16*) que permite a transmissão e recepção de dados em tempo real, garante um nível médio de interoperabilidade que equivale ao grau ou nível 2a para o modelo LISI (Clark, 2001), apresentado anteriormente. O que corresponde, no modelo NMI também referido anteriormente, à troca de dados estruturados, envolvendo a troca de informação interpretável por humanos, destinada a processamento manual ou automático, requerendo, porém, mecanismos manuais de compilação, recepção e ou envio.

Os sensores que integram a plataforma F-16MLU contribuem para a capacidade C4ISR de uma força, sendo altamente desejáveis num cenário NNEC auxiliando a compilação da imagem do espaço de batalha.

b. EH-101

O helicóptero EH 101 veio melhorar a capacidade CSAR e de fiscalização de embarcações de pesca na Zona Económica Exclusiva, em colaboração com a Marinha de Guerra portuguesa e com a Inspecção Geral das Pescas.

As capacidades de detecção e de comunicações do EH 101 fazem desta plataforma uma unidade mais apta na operação conjunta das FFAA portuguesas, face ao anterior helicóptero SA-33O PUMA.

O "Merlin" assume-se, por conseguinte, como um banco de ensaio para que o processo de transformação seja estendido a toda a estrutura da FAP e, como nicho tecnológico na capacidade de CSAR, representará uma mais-valia disponível também para a NATO e para a UE.

Tabela 3 – Sensores do EH-101 (Fonte: C-IETP Issue 4.00.00 DEC2006)

Sensores					
Activos		Passivos			Outros
Radar	Guerra Electrónica	Electro-óptico	Guerra Electrónica	Magnético	
APS-717P	N/A	FLIR STAR SAFIRE	RWR SKY GUARDIAN 2000	N/A	MWS AN/AA R-54

Tabela 4 – Sistemas de Comunicação do EH-101 (Fonte: C-IETP Issue 4.00.00 DEC2006)

Sistemas de Comunicações			
Voz			Dados
HF	VHF	UHF	
ELMER SRT-170/M6	ANDVT AIRTERM KY-100	ANDVT AIRTERM KY-100 CV/UHF ELMER SRT-651/N-SH	N/A

Embora se reconheça no EH-101 um esforço nacional para adquirir sistemas com alta tecnologia, não é possível defini-lo como um esforço eficaz para a interoperabilidade entre forças conjuntas ou combinadas. O EH-101 não possui qualquer tipo de sistema de comunicação que lhe permita a transferência de dados, uma vez que apenas possui a capacidade de comunicar através de voz. Assim o seu nível de interoperabilidade corresponderá grau ou nível 1b do modelo LISI (Clark, 2001). Para o modelo NMI estará no patamar da troca de dados não estruturados, interpretados humanamente.

Os sensores que integram a plataforma EH-101 serão um grande auxílio para as missões de CSAR pois concorrerem para as capacidades C4ISR, necessitando apenas de um sistema de partilha de informação, como por exemplo um sistema de *Data Link,* para incrementar o seu nível de interoperabilidade.

c. P-3C CUP+

O programa da FAP para a modernização das aeronaves P-3C adquiridas ao governo holandês, designado por CUP+, consiste em adicionar capacidades, oriundas dos requisitos operacionais definidos pelo Ministério da Defesa Nacional, ao programa CUP holandês. O programa CUP constituiu-se como a adaptação aos requisitos operacionais holandeses, dos programas intermédios da marinha dos EUA: ASuW *Improvement Program* (AIP) e *Block Modification Upgrade Program* (BMUP).

Assim, e numa perspectiva da salvaguarda dos interesses nacionais permanentes e actuais, quer em operações estritamente nacionais quer integrado em forças multinacionais, o programa de modernização do MPA português consiste em aplicar melhoramentos ao nível dos sistemas associados às capacidades C4ISR e à interoperabilidade num cenário de GCR. Para tal, desenhou-se um sistema de arquitectura aberta e de tecnologia de última geração COTS e *Government Off-The-Shelf* (GOTS).

Tabela 5 – Sensores do P-3C CUP+ (Fonte: Esquadra 601)

Sensores					
Activos		Passivos			
Radar	Guerra Electrónica	Electro-óptico	Guerra Electrónica	Magnético	Acústico
ISAR / Strip SAR / Spot SAR / MTI / GMTI / Air Picture	ALQ-131	Wescam MX-15D (vídeo / IR)	ESM com RWR MWS	Digital MAD CAE	USQ-78 AR/TR

Tabela 6 – Sistemas de Comunicação do P-3C CUP+ (Fonte: Esquadra 601)

Sistemas de Comunicações				
Voz				Dados
HF	VHF	UHF	SAT	
ARC-210	SINGARS (Have Quick II)	SINGARS (Have Quick II)	SATCOM INMARSAT	JTIDS (*Link 16*) TADIL (*Link 11*) TCDL (video) MITTS-ICE (imagem e texto) RATT (UHF/HF)

De acordo com os requisitos técnicos anteriormente apresentados, o P-3C CUP+ garante, face ao modelo LISI, um grau ou nível de interoperabilidade 2a (Clark, 2001), conferido pelo JTIDS.

Deve referir-se que todos os sensores, descriminados na Tabela 6, garantem um forte contributo para a capacidade C4ISR de uma força conjunta, não sendo todavia considerados para a interoperabilidade.

Recordando a pergunta de partida – "Em que medida foram satisfeitos os requisitos técnicos impostos pela necessidade de interoperabilidade, num cenário de utilização das tecnologias de GCR, nas aquisições e programas de modernização de sistemas de armas da Força Aérea Portuguesa?" – e observando a óbvia transposição que foi efectuada ao longo do estudo da GCR para o conceito NNEC, dada a sua pertinência e validade para o caso nacional, devem retirar-se conclusões a dois tempos.

Num primeiro tempo, e no que concerne ao nível de interoperabilidade, conclui-se que o F-16 MLU e o P-3C CUP+ se encontram numa posição relativa mais avançada quando comparado com o EH-101, uma vez que garantem um nível médio de interoperabilidade (nível 2a no modelo LISI), concedido pelo sistema *Link 16*.

Deve, porém, notar-se que este nível de interoperabilidade é o mais baixo do nível 2, perspectivando-se a médio prazo, no âmbito da NATO, uma transição para outros graus que possibilitem a partilha de informação sobre redes globais.

Quanto ao helicóptero EH-101, com base nos sistemas de comunicação de voz, apenas pode ser atribuído o nível 1, dos referidos modelos; este facto traduz-se num baixo grau de interoperabilidade.

Para os três casos estudados, deve relevar-se o esforço para equipar as aeronaves com sensores sofisticados e decisivos para a capacidade C4ISR, e subsequentemente para o conceito NNEC, como se infere dos atributos previstos no *NATO NNEC Roadmap* – “Proliferação de sensores e de capacidades de partilha de informação a todos os níveis de actividade (…)” (NATO, 2006). Porém, não poderão ser considerados para a atribuição de níveis de interoperabilidade, face aos modelos apresentados.

Numa fase mais avançada, para cenários NNEC evoluídos e consolidados, tal como são actualmente perspectivados, os sistemas de armas estudados não estão equipados de acordo com os requisitos técnicos previstos, cujas características conduzem a elevados níveis de interoperabilidade. Recordem-se requisitos, como por exemplo as redes para comunicações em voz, dados e vídeo, baseadas em tecnologia IP ou os rádios definidos por software que permitem a utilização de várias formas de onda, que garantirão o fluxo de informação por redes multi-dimensionais, apoiadas por aplicações interactivas.

Conclusões

Ao longo deste trabalho, pretendeu desenvolver-se uma investigação que respondesse à questão: “Em que medida foram satisfeitos os requisitos técnicos impostos pela necessidade de interoperabilidade, num cenário de utilização das tecnologias de GCR, nas aquisições e programas de modernização de sistemas de armas da Força Aérea Portuguesa?”

Para que o problema fosse correctamente delimitado e analisado, procurou identificar-se o âmbito e os conceitos que poderiam concorrer para a resposta à pergunta de partida, passo que define a primeira fase do Método de Investigação em Ciências Sociais de Raymond Quivy.

No que respeita ao âmbito, decidiu trabalhar-se num cenário definido pelos padrões orientadores da NATO, dadas as manifestas ligações entre Portugal e a Aliança Atlântica, que, de alguma forma, irão influenciar decisivamente o planeamento estratégico da FAP. Por outro lado, e uma vez que a temática remetia para requisitos técnicos promotores da interoperabilidade, foi dado especial enfâse às capacidades operacionais evidenciadas pelos sensores ISR e pelos sistemas de comunicação dos meios aéreos a operar nos países da NATO. Do universo de SA da FAP, optou-se por seleccionar o F-16 MLU, o EH101 e o P-3C CUP+, que consistem na melhor amostra das aquisições e programas de modernização de sistemas de armas da Organização.

Da pergunta de partida, foram delineadas as perguntas derivadas que iriam orientar o rumo do trabalho, nas fases da exploração e definição da problemática.

Durante a exploração, foram realizadas algumas entrevistas que permitiram verificar o interesse pela temática da GCR e NNEC, mas também o desconhecimento sobre requisitos técnicos essenciais para a obtenção da interoperabilidade, que corresponde a uma capacidade determinante para o sucesso de operações no âmbito NNEC.

Perante este facto, foram analisados diversos documentos que constituíram os alicerces da definição dos conceitos que iriam ajudar a enquadrar a problemática.

Decidiu-se no primeiro capítulo apresentar noções sobre GCR e NNEC, sendo este último o conceito de GCR proposto pela NATO, bem como as tecnologias a eles associadas. Ficou expresso neste estudo que estas tecnologias, decorrentes da era digital, estão intrinsecamente relacionadas com as capacidades C4ISR, conferindo-lhe um estatuto fundamental na estrutura da GCR.

Seguidamente, foi abordado o envolvimento tecnológico dos sistemas de comunicações, dos sensores e das redes de informação.

Quanto aos sistemas de comunicações, foram referidos os mais recentes sistemas de *Data Link* utilizados por aeronaves de estados membros da NATO, bem como as preocupações com a cobertura global, com novas formas de onda e a imperiosa necessidade de maior largura de banda, características concedidas por novos tipos de rádio, como por exemplo o JTRS.

No que respeita às tecnologias relativas aos sensores, foram mencionados os modernos radares, os sistemas electro-ópticos, entre outros, que permitem agora maiores alcances e altas definições, reduzindo o “nevoeiro” de um conflito, ou seja, contribuindo para uma melhor percepção do espaço de batalha.

Posteriormente, foram evidenciadas as tecnologias que distinguem o eixo de todas as operações de GCR – as redes – tendo sido particularizada a importância do protocolo IPv6, como factor chave para a implementação segura e eficaz das futuras redes de informação em ambiente militar.

No segundo capítulo, ainda inserido na definição da problemática, começou por apresentar-se o conceito de interoperabilidade, realçando o seu teor fundamental para as operações de GCR, complementando seguidamente a sua definição com a introdução dos requisitos para a interoperabilidade e com a apresentação dos dois modelos mais importantes para a comunidade militar, que identificam níveis ou graus de interoperabilidade: o modelo *NMI*, da NATO; e o modelo *LISI*, publicado pelo DoD dos EUA. A compreensão destes modelos foi fundamental para se poder afirmar as conclusões que viriam a responder à pergunta que iluminou a investigação.

Ainda no mesmo capítulo, elaborou-se uma descrição sobre os sistemas actuais e emergentes que, em última análise e no caso dos sistemas de comunicações, configuram os requisitos técnicos indispensáveis para teatros de operações em ambiente NNEC. Os referidos sistemas foram divididos, uma vez mais, por sistemas de comunicações, sensores e redes.

A referida descrição, além da pesquisa de outras fontes, foi referenciada a dois documentos essenciais para o desenvolvimento do processo de transformação da NATO, no âmbito do conceito NNEC: o *NATO NNEC Roadmap*; e o *NNEC Feasibility Study* (versão 2.0).

O terceiro capítulo teve por objectivo consolidar a investigação através da análise dos SA, face aos modelos de interoperabilidade mencionados, e da elaboração das conclusões. Para tal, foram observados os três sistemas de armas previamente definidos como objecto de estudo: o F-16 MLU, o EH101 e o P-3C CUP+. Após uma breve

introdução a cada uma das plataformas, foram elencados os vários equipamentos – sensores e sistemas de comunicações – que integram as referidas aeronaves.

Como ficou expresso ao longo do trabalho, o nível de interoperabilidade de um sistema é determinado pela sua capacidade de partilha de informação com outros actores do espaço de batalha, factor intimamente relacionado com os sistemas de comunicação. Daqui resulta uma primeira aproximação às conclusões particulares de cada plataforma, através da apreciação dos sistemas de comunicação instalados, face aos dois modelos de referência anteriormente introduzidos que, como oportunamente mencionado, são susceptíveis de correspondência directa.

As conclusões obtidas permitiram colocar os sistemas de armas estudados em patamares de baixo e médio nível de interoperabilidade, sendo o EH-101 a aeronave com menor grau de interoperabilidade, em virtude de não estar equipada com sistemas de comunicação de dados, mas apenas voz. Os níveis médios de interoperabilidade, atribuídos ao F-16 MLU e ao P-3C CUP+, são baseados na capacidade *Link 16*, permitindo-lhes a operação em cenários apoiados nas redes de *Data Link*, cuja validade se prevê para os anos mais próximos.

Quanto ao espectro de sensores ISR integrados nas diversas aeronaves, conclui-se que qualquer uma das plataformas está equipada com sistemas modernos, cujo contributo será valioso para a capacidade C4ISR de uma força conjunta e combinada, promovendo a tão desejada compilação da imagem do espaço de batalha.

A FAP, perseguindo os modernos preceitos que promovem o progresso da organização militar, nomeadamente no que concerne à garantia da capacidade de interoperabilidade com os seus aliados, deverá encetar ou manter a presença em grupos de trabalho, nomeadamente no âmbito da NATO, que promovam estudos sobre a GCR, na perspectiva de uma futura adaptação dos seus recursos a este, provável, novo ciclo do pensamento da Guerra.

Concorrendo para o desiderato acima exposto, a FAP terá que obrigatoriamente pensar novos caminhos, cujos objectivos passam por analisar o conceito NNEC e recomendar as alterações que deverão ser introduzidas nos sistemas de armas existentes, assim como nos programas de modernização ou aquisição, para que possa continuar a ser eficaz na forma de combater, quer seja de forma independente, conjunta e ou combinada.

A modernização das aeronaves F-16, através do programa MLU, e P3-C CUP+ traduz-se num aumento de potencial na transmissão e recepção de informação táctica em tempo real, segura e sem recurso à comunicação de voz. Desta forma, promove-se a

eficácia de um SA e a integração de múltiplos sistemas de armas dissimilares da ordem de batalha (terrestre, aérea e naval). Todavia, ainda insuficiente para assegurar o estado final que o conceito NNEC preconiza, não a transmissão e recepção de informação, mas a partilha de informação.

As características que anteriormente se reconheceram ao F-16 MLU e ao P3-C CUP+ conferem, actualmente, um grau adequado de interoperabilidade com outras forças, condição essencial e fundamental para operar em futuros conflitos. Altos responsáveis afirmam que, por exemplo, sem *Link 16* e sem armamento de precisão não há possibilidade de integrar forças em qualquer coligação, considerando os riscos de baixas e a incapacidade de respeitar as restrições ao nível dos danos colaterais.

Pelo potencial dos sistemas de armas acima referidos e pelo potencial de desenvolvimento que ainda possuem (permanente possibilidade de actualização do *software* que integra toda a panóplia de sistemas aviónicos), estes meio constituem para a FAP um salto muito elevado em capacidade, uma vez que coloca Portugal em paridade com as congéneres forças aéreas europeias e da NATO.

Para concluir este trabalho, recordam-se as palavras do Tenente-General da USAF Ronald Keys, “(…) *a Força Aérea deveria fornecer a todas as plataformas e unidades de comando um portal com a velocidade dot-com, flexibilidade e compatibilidade com os níveis de segurança adequados*”. Para tal descriminou os seguintes requisitos técnicos que serão determinantes para o sucesso das operações militares em ambiente de GCR:

- um sistema integrado tão bom como o sistema *Yahoo*;
- características de personalização tão boas como as da *Amazon.com*;
- um motor de busca tão bom como o *Google*,
- uma ferramenta de partilha de ficheiros tão boa como a *Roxio Inc.'s*, a *Napster* ou a *Sherman Networks' Kazaa*; e
- um programa de mensagens instantâneas tão bom como o *America Online Inc.'s*.

Bibliografia

ALBERTS, David S. (2001). *Understanding Information Age Warfare*. Washington D.C.: CCRP.

ALBERTS, David S. (2002). *Information Age Transformation: Getting to a 21st century military*. 2ª Ed., revista e actualizada. Washington D.C.: CCRP.

ALBERTS, David S., GARSTKA, John J., STEIN, Frederick P. (2003a)). *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington D.C.: CCRP.

ALBERTS, David S., HAYES, Richard E. (2003b)). *Power to the Edge: Command… Control… in the Information Age*. Washington D.C.: CCRP.

ARAÚJO, Luís E. E. (2005). *A Visão Prospectiva da Força Aérea Portuguesa* [em linha]. [Sine loco]: ASPJ Em Português 2º trimestre de 2005. [referência de 01 de Dezembro de 2006]. Disponível na Internet em <http://www.airpower.maxwell.af.mil/ apjinternational/ apj-p/2005/2tri05/araujo.html>.

BAILEY, Andreas (2004). *The implications of Network Centric Warfare* [em linha]. Pennsylvania: USAWC Strategy Research Project. [referência de 22 de Janeiro de 2007]. Disponível na Internet em <http://www.strategicstudiesinstitute.army.mil/ksil/files/00034 .doc>.

CALL, Christopher D. (2003). *US Army Special Forces Operational Interoperability with the US Army's Objective Force - The Future of Special Forces Liaison and Coordination Elements* [em linha]. Fort Leavenworth: [s.n.]. [referência de 21 de Janeiro de 2007]. Disponível na Internet em <http://www.stormingmedia.us/94/9485/A948514.html>.

CARNEY, David., OBERNDORF, Patricia (2004). *Integration and Interoperability Models for Systems of Systems* [em linha]. Pittsburg [referência de 15 de Janeiro de 2007]. Disponível na Internet em <http://www.sei.cmu.edu/isis/presentations/sstc-incose/sstc-incose.pdf>.

CLARK, Thea., MOON, Terry (2001). *Interoperability for Joint and Coalition Operations* [em linha]. [Sine loco]: Australian Defence Force Journal, No. 151, November/December 2001, pp. 23-36. [referência de 21 de Fevereiro de 2007]. Disponível na Internet em <http://www.dsto.defence.gov.au/publications/2901/Interoperability%20Paper.pdf>.

DIAS, João C. M. (2006). *A Guerra Centrada na Rede* [em linha]. [Sine loco]: [s.n.]. [referência de 12 de Fevereiro de 2007]. Disponível na Internet em <http:// www.mar.mil.br/caaml/passadico/2006/15aguerra.pdf>.

DOD, Office of Force Transformation (2005). *The Implementation of Network-Centric Warfare* [em linha]. Washington [referência de 04 de Janeiro de 2007]. Disponível na Internet em <http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_ LowRes.pdf>.

DUNCAN, M.D., et al. (2004). *Netcentric Multi-INT Fusion Targeting Initiative (NCMIFTI)* [em linha]. Washington D.C: US Naval Research Laboratory. [referência de 02 de Dezembro de 2006]. Disponível na Internet em <http://www.nrl.navy.mil/content. php? P=04REVIEW140>.

EUGÉNIO, António L. (2002). *Guerra Centrada em Rede***.** Trabalho Individual de Pesquisa, DIAEFA 310-58. Granja do Marquês: IAEFA.

GARSTKA, John, (2005). *Network Centric Operations*. Comunicação apresentada no âmbito da *NDIA Network Centric Operations Conference*. [Sine loco]. Disponível na Internet em <http://www.dtic.mil/ndia/2005netcentric/monday/garstka.pdf>.

GOODMAN JR, Glenn (2005). *Understanding DATA LINK’s*. C4ISR Journal Washington D.C.. CCRP.

HARZ, Christopher (2005). *Network Centric Warfare: Allied Progress* [em linha]. [Sine loco]: 6 Sense Newsletter. [referência de 02 de Dezembro de 2006]. Disponível na Internet em <http://www.usipv6.com/6sense/2005/aug/07.htm>.

HOBBINS, William T. (2005). *Airmen on the Battlefield: Warfighting Integration in Support of Special Operations Forces* [em linha]. [Sine loco]: Air & Space Power Journal - Spring 2005 [referência de 12 de Dezembro de 2006]. Disponível na Internet em <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/spr05/hobbins.html>.

LOCKHEED MARTIN CORPORATION (2004). *Technical Order 1F-16AM-1*. Change 13. Fort Worth: EUA.

NATO , Allied Command for Transformation (2006). *NATO NNEC Roadmap (Working Draft - version 3.0)*. Norfolk: NATO.

NATO C3A (2005). *NATO Network Enabled Capability, Feasibility Study, Executive Summary (version 2.0)*. Brussels: NATO.

NATO C3 BOARD, Joint C3 Requirements and Concepts Sub-committee (2004). *Net Ready Key Performance Parameters*. Brussels: NATO.

NATO C3 BOARD (2006a)). *Emerging Technologies* [em linha]. [Sine loco]: NC3TA Volume 2, Chapter 2. [referência de 02 de Fevereiro de 2007]. Disponível na Internet em <http://194.7.80.153/website/book.asp?menuid=15&vs=0&page=vol2%2Dsup2%2Fch02%2Ehtml>.

NATO C3 BOARD (2006b)). *Appendix C. Terminology* [em linha]. [Sine loco]: NC3TA Volume 5. [referência de 02 de Março de 2007]. Disponível na Internet em <http://194.7.80.153/website/book.asp?menuid=15&vs=0&page=volume5%2Fapc%2Ehtml>.

NOLIN, Pierre C. (2006). *Interoperability: the need for transatlantic harmonisation* [em linha]. Brussels: NATO Parliamentary Assembly (2006 Annual Session). [referência de 23 de Fevereiro de 2007]. Disponível na Internet em <http://www.nato-pa.int/Default.asp?SHORTCUT=1004>.

NUNES, Sérgio S. (2004). *Alternativas para a Interoperabilidade entre Sistemas de Informação Universitários* [em linha]. Porto [referência de 16 de Janeiro de 2007]. Disponível na Internet em <http://paginas.fe.up.pt/~mgi01016/dissertacao/dissertacao .pdf>.

PHISTER, Paul W., PLONISCH, Igor G. (2004). *Aplicações militares das tecnologias da informação* [em linha]. [Sine loco]: ASPJ Em Português 4º trimestre de 2004. [referência de 05 de Dezembro de 2006]. Disponível na Internet em <http://www.airpower.maxwell. af.mil/apjinternational/apj-p/2004/4tri04/phister.html>.

QUIVY, Raymond, CAMPENHOUDT, Luc Van, (2005). *Manual de Investigação em Ciências Sociais*. 4ª ed. Lisboa: Gradiva.

TOLK, Andreas (2003). *Overview of recent Findings of the Study Groups of the Simulation Interoperability Workshop dealing with C3I and M&S Interoperability* [em linha]. Norfolk: Virginia Modeling Analysis & Simulation Center. [referência de 18 de Janeiro de 2007]. Disponível na Internet em <http://www.vmasc.net/pubs/tolk-overview01.pdf>.

VICENTE, João P. N. (2005). *A Transformação da NATO com base nas capacidades centradas em rede.* Trabalho Individual de Pesquisa, DIAEFA 302-46. Granja do Marquês: IAEFA.

VICENTE, João P. N. (2006). *A (R)Evolução do Pensamento Estratégico* [em linha]. [Sine loco]: ASPJ Em Português 2º trimestre de 2006 [referência de 12 de Janeiro de 2007]. Disponível na Internet em <http://www.airpower.maxwell.af.mil/apjinternational/ apj-p/2006/2tri06/vicente.html>.

YANG, Ang., (2004). *Understanding Network Centric Warfare* [em linha]. [Sine loco]: ASOR Bulletin, Volume 23, Number 4. [referência de 21 de Janeiro de 2007]. Disponível na Internet em <http://www.cs.adfa.edu.au/~ruhul/ang.pdf>.

Anexo A – Modelo NMI

O modelo NMI (Carney, 2004) apresenta perfis de interoperabilidade e define cinco graus:

Grau 0: Troca de dados não existente

Este nível implica a não existência de conexão física entre entidades.

Grau 1: Troca de dados não estruturada

Este nível envolve a troca de dados não estruturados, interpretados humanamente, tais como, texto expresso em estimas operacionais, análises e outros documentos. Os sub-níveis são:

- Conectividade da Rede
- Troca básica de documentos
- Troca básica de documentos informais

Grau 2: Troca de dados estruturados

Este nível envolve a troca de dados estruturados, humanamente interpretáveis, destinados ao processamento manual e/ou automático, mas que necessita de compilação, recepção e/ou despacho manual. Os sub-níveis são:

- Troca melhorada de mensagens informais
- Troca melhorada de documentos
- Gestão de Rede
- Sobreposição de Mapas / Troca de gráficos
- Serviços de Directoria
- Acesso aos serviços *WEB*
- Aplicações multi-ponto
- Troca de dados

Grau 3: Partilha de dados *seamless*

Este nível envolve a partilha de dados automatizados dentro de sistemas baseados num modelo de troca comum. Os sub-níveis são:

- Troca de mensagens formais
- Troca de dados comuns

- Gestão de sistema
- Gestão de sistema de segurança
- Gestão de Segurança
- Troca de dados em tempo real

Grau 4: Partilha de informação *seamless*

Corresponde a uma extensão do grau 3. Este nível estabelece interpretação universal de informação através do processamento cooperativo de informação. Os sub-níveis são:

- Troca de informação comum
- Aplicações distribuídas

Anexo B – Modelo LISI

Modelo LISI (Fonte: Clark, 2001)

LEVEL (environment)			Interoperability attributes			
			Procedures	Applications	Infrastructure	Data
Enterprise (universal)	4	c	Multi-national	Interactive	Multi-dimensional topologies	Cross-enterprise models
		b	Intra-government			
		a	Defence department	Object cut & paste		Enterprise models
Domain (integrated)	3	c	Domain	Shared data	WAN	DBMS
		b		Grp collaboration		Domain models
		a		Txt cut & paste		
Functional (distributed)	2	c	Common Operating Environment	Web browser	LAN	Program models & advanced
		b		Office software		
		a	Program	Adv. messaging	NET	data formats
Connected (peer-to-peer)	1	d	Standards compliant	Basic messaging	Two way	Basic data formats
		c		Data file transfer		
		b	Security profile	Simple interaction		
		a			One way	
Isolated (manual)	0	d	Media exchange procedures	*Not applicable*	Removable media	Media formats
		c	Personnel access controls		Manual re-entry	Private data
		b				
		a				
		0	NO KNOWN INTEROPERABILITY			

Anexo C – Definições

Windows Security – conjunto de aplicações cujo objectivo é a protecção contra ameaças como os vírus, vermes (*worms*) e *spyware*. No caso de existir um comprometimento num computador, originado por um ataque, estas aplicações deverão minimizar os danos.

Wireless Networking – refere-se a qualquer rede que transmita sinais de rádio pelo ar, tais como uma rede local sem fios, uma rede de telefones celulares ou uma rede de satélites.

Ad Hoc Networking – é uma rede local ou qualquer outra rede de pequenas dimensões, especialmente uma rede sem fios, na qual os dispositivos de rede são parte da rede apenas durante uma sessão de comunicações ou, no caso de dispositivos móveis ou portáteis, quando em proximidade do resto da rede. O termo *Ad Hoc* (para este efeito) tem sido aplicado a redes de empresas ou particulares, nas quais novos dispositivos podem ser rapidamente aplicados, usando, por exemplo, a tecnologia *Bluetooth* que permite aos diversos dispositivos comunicar com computadores ou outros dispositivos utilizando transmissões sem fios.

Grid Computing – é um modelo computacional capaz de alcançar uma alta taxa de processamento dividindo as tarefas entre diversos computadores, podendo ser em rede local ou rede de longa distância, formando um computador virtual; consiste em aplicar os recursos de muitos computadores numa rede para resolver um problema, normalmente científico ou técnico que requeira uma grande quantidade de ciclos de processamento ou o acesso a grandes bases de dados. Um exemplo de *Grid Computing* do domínio público é o projecto *SETI (Search for Extraterrestrial Intelligence) @Home*, no qual milhares de pessoas partilham os ciclos de processamento não utilizados dos seus computadores pessoais para pesquisar sinais que provêm do espaço.

Power over Ethernet (PoE)– é uma tecnologia revolucionária que integra dados, voz e corrente eléctrica, numa infra-estrutura *Ethernet* padrão, providenciando assim novas opções para a distribuição de corrente eléctrica. Esta tecnologia permite alimentar, através de cablagem CAT5, telefones IP, pontos de acesso a redes locais sem fios, câmaras de vigilância, entre muitas outras aplicações e sistemas de computadores.

Nanotechnology – A nanotecnologia é a capacidade potencial de criar coisas a partir do mais pequeno, usando as técnicas e ferramentas que estam a ser desenvolvidas nos dias de hoje para colocar cada átomo e cada molécula no lugar desejado. Se conseguirmos este sistema de engenheria molecular, o resultado será uma nova revolução industrial. Além disso, teria também importantes consequências económicas, sociais, ambientais e militares.

Software Defined Rádio (SDR) – refere-se a comunicações sem fios, nas quais a modulação do transmissor é gerada ou definida por computador e o receptor utiliza também um computador para receber e decifrar o sinal. O tipo de modulação desejado é processado por microprocessadores que controlam o transmissor e o receptor.

Radio Frequency Identification (RFID) – trata-se de um método de identificação automática através de sinais de rádio, utilizando dispositivos chamados *tags*. Um *tag* é um pequeno objecto, que pode ser colocado numa pessoa, animal ou produto. Este tag contém *chips* de silício e antenas que lhe permitem responder aos sinais de rádio enviados por uma base transmissora.

Fibre Intrusion Detection (FID) – é um tipo de sistema de gestão de segurança para redes e computadores. Este sistema recolhe e analisa informação de várias áreas de um computador ou rede, para identificar possíveis quebras de segurança, incluindo ataques executados dentro de uma organização e ou do exterior da organização. O FID inclui as seguintes funções:

- Monitorização e análise dos utilizadores e dos sistemas
- Análise das configurações e vulnerabilidades do sistema
- Avaliação da integridade do sistema e dos ficheiros
- Reconhecimento dos padrões típicos de ataque
- Análise dos padrões de actividade anormais
- Seguimento das políticas de violação dos utilizadores

Identity Management – é uma vasta área administrativa que visa identificar indivíduos dentro de um sistema (através de um país, de uma rede ou de uma empresa) e controlar o seu acesso a recursos do sistema, associando direitos e restrições de utilizador à identificação estabelecida.

Web Services – é uma solução utilizada na integração de sistemas e na comunicação entre aplicações diferentes. Com esta tecnologia é possível que novas aplicações possam interagir com aquelas que já existem e que sistemas desenvolvidos em plataformas diferentes sejam compatíveis. Os *Web services* são componentes que permitem às aplicações enviar e receber dados em formato XML. Cada aplicação pode ter a sua própria "linguagem", que é traduzida para uma linguagem universal, o formato XML.

Para as empresas, os *Web services* podem trazer agilidade para os processos e eficiência na comunicação entre cadeias de produção ou de logística. Toda e qualquer comunicação entre sistemas passa a ser dinâmica e principalmente segura, pois não há intervenção humana.

Apêndice

Science & Technology for Australian Network-Centric Warfare: Function, Form and Fit

Science & Technology for Australian Network-Centric Warfare: Function, Form and Fit

Tim McKenna, Terry Moon, Richard Davis & Leoni Warne

Introduction

A network-centric approach to warfighting was officially launched by the Defence Minister and the Chief of the Defence Force in May 2003 (Hill 2003). The Australian concept for this new approach to warfighting is best summed up by the following quote (DFW 2004):

'On the surface, Network Centric Warfare (NCW) is a simple concept that involves the linkage of engagement systems to sensors through networks and the sharing of information between force elements. Consequently, much of the discussion and early development of the concept revolved around connecting information systems and creating software applications that allow people to use the available data. However, NCW is also based on the idea that information is only useful if it allows people to act more effectively: this makes the human dimension fundamental to NCW.'

In response, DSTO has established an S&T initiative to help capture and focus the NCW work it is undertaking, identify directions for longer-term military capabilities, distil key research issues that need to be addressed through long-range research (LRR) and provide a good interface with Defence's NCW stakeholders. This article provides some background to the development of Australian NCW, discusses its Science and Technology underpinnings, and introduces the DSTO NCW S&T Initiative.

International Context for NCW

The term 'network-centric' as applied to warfare was probably borrowed from network-centric computing which arose through advances in information technology that allowed computers to interact with each other while using different operating systems. The end of the Cold War, coupled with advances in computer technology, spurred the reassessment of military strategy in the US and other Western countries. NCW thus emerged as a high-tech approach to addressing what was perceived to be a new global security environment.

NCW was originally championed by Cebrowski (1998) with David Alberts and John Garstka providing much of the intellectual framework underpinning it. Although their seminal work 'Network Centric Warfare' gives a carefully worded and detailed definition of NCW (Alberts, Garstka & Steins 1999), the following four tenets probably provide a simpler and clearer picture of the US perspective of NCW (CCRP 2005):

1. A robustly networked force improves information sharing.
2. Information sharing and collaboration enhance the quality of information and shared situational awareness.
3. Shared situational awareness enables self-synchronisation.[i]
4. These, in turn, dramatically increase mission effectiveness.

To these can be added Alberts (2002) view that NCW thus involves both:

- The provision of vastly increased access to information at all echelons.
- A redefinition of the relationships among participants in a mission and between commanders and subordinates.

Similar concepts of networked warfare have been developing elsewhere. Of particular note are the network-based defence (NetDefence) concept of Sweden (Lundqvist 2000) and the network-enabled capability (NEC) concept developed in the UK (Borgu 2003; dstl 2004;

MoD 2005). More recently the People's Republic of China has announced its intention to adopt NCW-related technologies (Wellfare 2005). The US, however, was the progenitor of NCW and remains the powerhouse of technological developments that support its implementation.

The technological focus of the US is highlighted by their drive to establish a robust and global high-capacity network that would enable US forces to undertake NCW. A global approach dominated by technology may, however, be less suited to Australia's capability requirements and levels of Defence funding. The question then arises as to how applicable are these US tenets to Australian NCW or do we need a different approach? The work to date indicates that Australia is already taking a different path in establishing five premises that include, not only the technological aspects of networks, shared situational awareness and self-synchronisation, but the human dimensions of professional mastery and command philosophy (DFW 2004).

Having noted the different network-centric concepts being pursued internationally, perhaps the following description provides the best overview: *NCW is an approach to warfighting where the network supplies the **right information** at the **right time** in the **right form** to the **right person***. To these 'four rights' can be added '*and is put to the **right use***' (Fewell & Hazen 2003). Adding 'right use' is particularly important as NCW is about producing effective military outcomes.

Good Ideas or Latest Fad?

Like any new concept NCW has its advocates and critics. Enthusiastic advocacy from some has almost reached the fervour of a high-pressure sales campaign while critics can be equally passionate. Comments on NCW range from referring to it as the 'new fashion in modern warfare' (Borgu 2003) to 'our worldwide, blue-water Navy always has been a networked environment' (Barnett 1999). Alberts, Garstka & Stein (1999) acknowledge that there are 'exaggerated claims, unfounded criticisms and just plain misinformation' about NCW and go into detail identifying then discussing some of the myths of NCW. These myths include:

- NCW is all about the network.
- NCW applies only to large-scale conflict.
- The commercial world has shown us the way.
- NCW will not survive first contact with the fog and friction of war.
- NCW is an attempt to automate war that can only fail.

Kaufman (2004) has argued that NCW is a technology-led response to the situation the Western nations find themselves in following the end of the Cold War. He then questions whether future conflicts will be against a comparatively equipped conventional enemy or subversive groups practicing terrorism. When challenging whether investing in an NCW approach is an appropriate response to emerging national security concerns,[ii] Kaufman notes the importance of developing new technology for warfare and that, historically, this became organised at a national level to both spur and focus technology developments – a process he calls 'command technology'.

While the debate as to the value of NCW continues, the military operations in Iraq that led to the removal of Saddam Hussein have demonstrated that NCW concepts can assist in the conduct of rapid and decisive military operations (Moores 2002). Use of unmanned aerial

vehicles (UAVs) in Afghanistan for surveillance, reconnaissance, targeting and weapons delivery, has also demonstrated some aspects of NCW, in particular the value of sensor-to-shooter links. That said, the application of NCW concepts to operations in complex terrain, particularly involving counter-insurgency, is still a developing field (Bowley & Gaertner 2005).

Advances in technology continue and, while there is still much to debate about NCW, it is probably now reasonable to say that:

- The underpinning concepts of NCW are sufficiently well developed and tested for its implementation in military operations.[iii]
- Recent conflicts have demonstrated that an NCW approach can lead to swift and decisive military operations conducted as planned with minimal casualties and within constraints placed on collateral damage.
- There are historical examples that illustrate how new technology can dramatically change the nature of warfare.

For the Australian Defence Force (ADF), an underlying belief has emerged that improved integration and connectivity can lead to an enhancement of military effectiveness. What is probably not clear is how best Defence could, and to what extent it should, embrace concepts and technological solutions developed elsewhere. In identifying what advances in NCW-related technologies are most suited to Australia's Defence requirements (within current and projected funding for Defence), the issue of the degree to which technologies developed for the civil sector can be readily incorporated into new and existing military capabilities must also be addressed.[iv]

ICT and Modern Warfare

The profound effect of advances in information and communications technologies (ICT) on warfare can be traced back to the American Civil War, considered by historians as the first modern war. From an ICT perspective this was the first time there had been widespread use of the telegraph, photography and aerial observation (Aeragon 2005).

The world's first telegraph message was sent from Washington D.C. to Baltimore, Maryland in 1844. By the time the Civil War began, telegraph lines had been established over most of the Eastern United States. Because of the war, the Western Union Telegraph Company completed construction of a telegraph line through the Rocky Mountains connecting the West Coast to the network in October of 1861.[v] When the Civil War began, the telegraph was used to report battle information and became the most important form of military communication. In particular it was used for the rapid reporting of intelligence information but also became a prime target for military counter-operations. At these earliest stages there were even some instances where messages were intercepted and replaced with disinformation!

Figure 1 *Telegraph sabotage: cutting telegraph wires and connecting the ends so that the point where the connection is broken cannot be detected from the ground (c. 1863).*

Technological advances continued apace with the newly developed 'wireless' communications which were used for the first time during a war to report on the naval battle between Russia and Japan in 1905. Following the first transatlantic radio telephone conversation in 1915, radio quickly become an essential component of military operations as it offered a mobile communications capability. Along with the telephone that replaced the telegraph for fixed (wire) communications, two-way radios became an integral part of most, if not all, military operations.

Devices and machines for numerical calculation date back thousands of years to the abacus (Abacus 2005). The modern computing age was, however, heralded by the advent of electronic devices which enabled the development of electronic computers. In the Second World War (WWII) a valve computer known as 'Colossus' was developed and used by Britain to decode the Germans' coded messages (Tedeschi 2005). Towards the end of WWII the US developed ENIAC, a large digital electronic computer, to compute ballistics tables - a task that required many tedious calculations. Because ENIAC was programmable, it could also perform many other tasks (Information Age 2005).

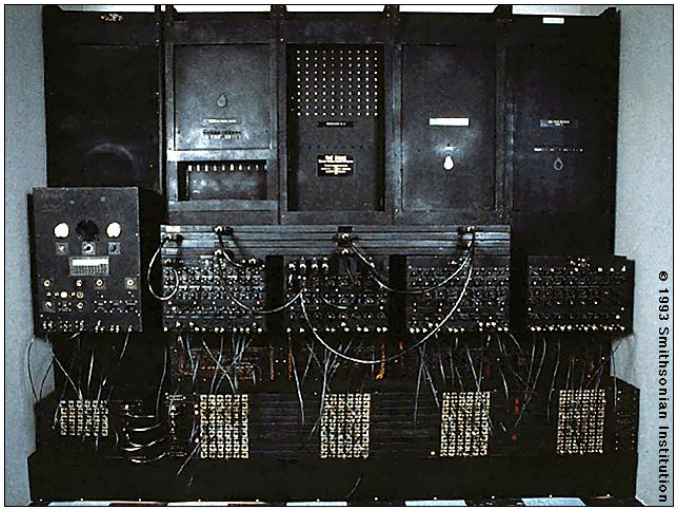

Figure 2 *The ENIAC programmable computer*.

A more recent, and local example of the impact of advances in ICT on military operations is the introduction of a Theatre Broadcast System (TBS) into the ADF. Based on commercial satellite transmission systems, and developed by DSTO, TBS was first demonstrated to the Australian Army in 1999. Services offered by this new capability include file transfer, a video/audio channel for teleconferencing and data streaming access. TBS has since been subject to an evolutionary (spiral) development process and has been deployed on operations in East Timor, Solomon Islands, Middle East and in Banda Aceh for the humanitarian relief operations following the tsunami (DSTO 2005).

Figure 3 *The Australian Theatre Broadcast System (TBS) as deployed with the ADF during UN Peacekeeping operations in East Timor*.

Inventions such as the telegraph, telephone, radio, and computer set the stage for the Internet and with it an unprecedented integration of ICT capabilities. The Internet is not only a world-wide broadcasting capability, but a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location (Internet Society 2005).

Australian NCW Concept

Premises

The development of an Australian NCW concept was based on the following premises (DFW 2004):[vi]

- Professional mastery (and appropriate training) is essential to the effective implementation of NCW.
- Mission command will remain an effective command philosophy into the future.
- Information and intelligence will be shared if a network is built connecting engagement, sensor and command & control systems.
- Robust networks will facilitate effective collaboration and shared situational awareness.
- Shared situational awareness will enable self-synchronisation. This helps warfighters to adapt to changing circumstances and apply Multidimensional Manoeuvre (MDM) effectively.

In a nutshell, the Australian concept of NCW focuses on supporting a manoeuvre type of approach to military operations. In addition, there is a strong link to an Effects Based approach, which focuses on the outcomes to be achieved. At a strategic level, the Effects Based approach to planning is termed Net Assessment.[vii] Additional to the acquisition and application of suitable technologies, the human dimension is highlighted as key to achieving effective NCW and it is here that a significant difference between the Australian and US approaches to developing NCW is evident. Lambert & Scholz (2005) discuss this difference noting that the first two premises of Australian NCW have no equivalent representation in the US concept. They further note that Australia sees NCW more as a means to improve joint warfighting rather than a mechanism for unifying forces.

The Network

The network dimension, introduced by the third and fourth premises of Australian NCW, is described as having four aspects (DFW 2004):

- **Connect** units, platforms and facilities through networking, appropriate doctrine, training and organisational processes and structure.
- **Collect** relevant information using these networked assets and distribute it via the network.
- **Use** the information, and the intelligence derived from it, to effectively achieve military objectives.
- **Protect** the network established from external interference or technical failure.

Again the human dimension is explicitly included through mention of doctrine, training and organisational aspects.

These ‘connect’; ‘collect’; ‘use’; ‘protect’ (CCUP) aspects are also consistent with the OODA-cycle concept introduced by John R. Boyd of the USAF in 1985 (see Polk 2000) and similar concepts for organisational adaptive loops put forward by Limerick & Cunnington (1993) and Haeckel (1999). Connecting sensors to shooters with a feedback mechanism for their control and adaptation is another instantiation of this concept. The CCUP model thus provides a means for monitoring and managing the development and

implementation of Australian NCW but does it also provide a means for addressing science and technology issues?

What is more important - Technology or the People using it?

New information and communications technologies such as personal computers, satellite communications, video teleconferencing, digital communications systems and the Global Positioning System are already available and influencing approaches to warfare (Alberts 2002). The Australian Future Warfighting Concept further discusses the impact of technology in modern warfighting noting that *'… technological developments, such as offensive information warfare capabilities, space-based sensors and communications, weapons of mass effect, and long-range weapons such as ballistic and cruise missiles have the potential to reach targets that were previously difficult to strike*' (Australian DoD 2002). Any such discussions of new technologies for warfighting should note, however, that to effectively harness technology advances, corresponding organisational and doctrinal changes are needed (DFW 2004). Attempts to introduce new technology often meet with failure when the interactions between technology and people are not adequately addressed.

While Houston (2005) has been careful to note the importance of the human dimension for Australian NCW, Bryans (2005) has also cautioned against 'simplifying things too much' and downplaying the role technology plays. Perhaps this interplay between technology and people is adequately summed up by the US Chief of Naval Research who defined NCW as: *'Military operations that exploit state-of-the-art information and networking technology to integrate widely dispersed human decision makers, situational and targeting sensors, and forces and weapons into a highly adaptive, comprehensive system to achieve unprecedented mission effectiveness'* (ONR 2005). Put more simply, we could say a balanced view of NCW is: '*Defence people applying advances in information technologies to improve operations*': where Australia's NCW approach involves improving operations by:

- collecting better information from sensors and intelligence sources;
- using that information for more effective command and target engagement;
- building networks to better connect the ADF and protect its information; ***but also***
- adjusting culture, organisation, procedures, training and information system design so that Defence people can use these advances.

Striking a balance between technology and people by providing suitable organisational structures and processes, doctrine and training will remain as much a challenge for the implementation of an NCW-capable force as developing and integrating new technologies.

Role of Science & Technology

In addressing the role science and technology, it may be useful to consider the following as salient features of Australian NCW:

- Network Concepts. NCW treats military platforms, facilities, combat equipment and other materiel as a network of nodes and links where information is the key 'currency of exchange'.
- Primacy of Information. For NCW, information is seen not only as important, but key to efficiently undertaking swift, decisive and effective military operations. In NCW-type operations combat units have access to information from other sources

rather than relying on their own organic assets. Thus information in NCW operations is 'universally' available.

- Exploitation of Technology. NCW exploits the capability and capacity of modern technology (particularly ICT) to gather, store, process, and distribute information. This supports sharing of information to facilitate greater understanding of a military situation and thus the undertaking of swift, decisive military operations.
- Human and Socio-cultural Aspects. Underlying most NCW discussions there are some important assumptions about how humans will behave and organisational elements will be structured and function in this new environment. For instance, information sharing will not occur without collaborative and cooperative behaviour on the part of the humans involved, however efficient the technical connectivity may be. Therefore cognitive load, information presentation, information overload, information verification, cooperative behaviours, trust, education, training, organisation, doctrine, and the human-machine interface need to be optimised in an NCW environment. Science has as much a role to play in understanding the human response to these new technologies as it does in developing the new technologies themselves.

Australia has a moderate-sized economy but its S&T infrastructure and pool of expertise are probably not sufficient to enable continual and sustained groundbreaking research and development (R&D) in the wide range of technologies of interest for NCW. Although Australia has traditionally aimed to be a 'fast follower' in applying R&D rather than a major progenitor of new R&D (Batterham 2003), maintaining an edge, even in niche areas of NCW technology, will be challenging. Despite this, there are likely to be areas of technology of specific relevance to Australian Defence requirements, and these should be identified. In addition to identifying the underpinning sciences and technologies central to the implementation of NCW, it would be useful to decide the degree to which they are already receiving adequate investment for their further development (in either the civil or military industry sectors), then establish priorities for further research in the key areas of S&T that would best support realisation of Australian NCW. Understanding the differences between the Australian concept of NCW and those of other countries such as the US, UK and Sweden may also help with identifying Australian Defence S&T priorities for NCW-related research.

The NCW S&T Initiative

Development of NCW concepts has now reached sufficient maturity for Defence to formulate an NCW Roadmap to guide the implementation of an NCW approach, and establish the NCW Program Office (NCW PO) to monitor the development of capabilities for an NCW-capable force. In response, DSTO has raised an NCW S&T Initiative (NSI) to coordinate and focus its S&T activities. This aims to:

- Improve the delivery of DSTO S&T support to key NCW stakeholders in Defence.
- Provide S&T support to the further development of NCW concepts.
- Position the DSTO to support the implementation of the NCW Roadmap.[viii]
- Identify major S&T issues for further research so that DSTO can shape its supporting R&D program.

'Enabling Future Warfighting - Network Centric Warfare' (DFW 2004) and the 'ADF NCW Roadmap' (introduced and discussed by Houston 2005) provide a starting point for exploring what S&T is needed. Using these, a systems engineering approach can be taken by extracting the capabilities sought, activities envisaged and effects desired to derive the

'Function and Form' sought for Australian NCW.[ix] Following this, an alignment or 'Fit' of proposed S&T support (and any underpinning research) to the derived Function and Form can be explored; Figure 4 illustrates this process. As shown, the DSTO Client program for NCW should provide S&T support to: further development of NCW concepts, implementation of the NCW Roadmap and the work undertaken by the NCW PO. In addition, DSTO's long-range research (LRR) program for NCW must be suitably tuned to provide a strong S&T base for the further development and implementation of NCW.

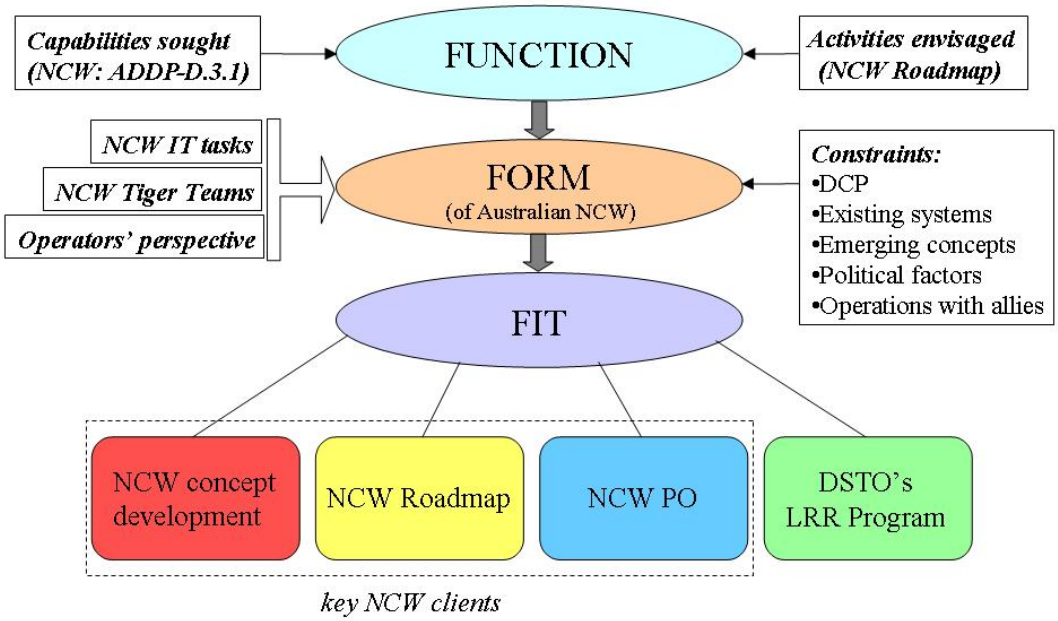

Figure 4 *A systems engineering approach to the NCW S&T Initiative.*

While the top-down approach outlined uses systems engineering (SE) principles, the NSI will also borrow heavily from operational research (OR) methods and those of the human and social sciences (HSS) in its quest to understand the wide range of S&T issues surrounding the development of Australian NCW. The approach also builds on existing work, including that done by DSTO Tiger Teams under the guidance of the NCW Steering Group (see DSTO NCW Tiger Team reports 2003 & 2005 and the NSI website 2005). One of the jobs of the NSI is to identify potential S&T inhibitors and enablers of NCW. A clear knowledge of the S&T stumbling blocks faced in implementing NCW and the potential benefits of new advances in technology should then assist in better defining further S&T work and research to underpin it.

For aligning DSTO's S&T work it is useful to apply one of the technology-oriented NCW frameworks, which views an NCW force as being made up of four 'grids' (Stein 1998):

- A **Sensor** grid that collects intelligence, surveillance and reconnaissance (ISR) information.
- The **Command & Control (C2)** grid that uses the information collected for assessment, collation with other information, planning and decision-making.
- The **Engagement** grid which uses the decisions made to direct military action.

- An **Information** grid that connects the other three grids together by providing the network infrastructure and networking.[x]

This description is also consistent with the CCUP model introduced earlier where the Sensor grid provides the **collect** function, the Information grid a **connect** function and the C2 and Engagement grids the **use** function, while the **protect** function applies to all grids.[xi] The grids are not only a means for describing in simple terms the infrastructure that makes up an NCW force but they are also useful for sorting the diverse S&T aspects of NCW spanning weapons, sensors, platforms, information technology, communications, electronic warfare, command & control, systems and organisational and doctrinal aspects as well as the human factors.

Early Assessments

From an initial understanding of the concept and premises on which Australian NCW is based, coupled with an understanding of the likely scale and nature of an Australian NCW force, it is suggested that:

1. The purpose of Australian NCW is to enable a manoeuvre approach to warfare and, at a strategic level, Net Assessment.
2. Australian NCW has more of a focus on the Human Dimension than its US counterpart with particular emphasis on Professional Mastery.[xii]
3. The concept of sharing information involves more than providing a Common Operating Picture. It includes the ability to 'tailor' a shared situational awareness for local operations and augment it with local knowledge. It also requires appropriate cooperative human behaviours based on sound education and training.
4. Australian networks are likely to comprise fewer nodes (perhaps by a factor of 10 or more) than US networks.
5. Infrastructure and available bandwidth may thus be a problem for offshore operations.
6. For Australian NCW a whole-of-nation approach is envisaged where civil telecommunications, national assets and information from other government agencies would be made available. This Civil Military Cooperation (CIMIC) introduces a further layer of complexity in the human aspects of effective collaboration and cooperation across different organisations.
7. In addition to a whole-of-nation approach, the ability to operate effectively in coalition operations is an important determinant for developing suitable capabilities and approaches to NCW.

While a structured approach, as broadly outlined above, will be followed to identify those sciences and technologies key to implementing NCW, a reality check will be provided through the views of S&T experts. The NSI has just started and it would be unwise to start prioritising S&T areas where further work is needed. The following have, however, already been suggested as potential candidates for further work:

- Sensing & Collection
    - Fusion of Information.
    - Adaptive sensing.
- Using: C2 and Engagement
    - Net-ready weapons.
    - Combat ID.
- Connecting & Protecting

    - Bandwidth limitations (and access to spectrum issues).
    - Network topologies.
    - Information Assurance and Security (multi-level security).
- Human Issues
    - Required skill sets, training and education for NCW.
    - Optimising Joint, Coalition and CIMIC cooperation.
    - Information sharing behaviours.
    - Information trust and relationship trust in NCW operations.
- Cross-cutting issues
    - Automation.
    - Methods for evaluation of military outcomes for NCW.

The future battlefield will also demand that personnel cooperate to a far greater extent than ever before, hence social and psychological factors must be addressed when new technology is adopted. For that reason, a better understanding of the psychological underpinnings of interpersonal and inter-group cooperation in military contexts is also needed. This will have significant implications for workforce planning, recruitment and training in the ADF (see Warne et al. 2004).

Conclusion

Some may consider Network Centric Warfare (NCW) the latest Defence fad but recent experience suggests that NCW is improving operational success and, applied intelligently, will continue to have that impact. As a result Australia has developed its own version of NCW and is pressing on with implementation.

Put simply, Australia's NCW approach is: '*Defence people applying advances in information technologies to improve operations.'* Specifically our NCW approach involves improving operations by:

- collecting better information from sensors and intelligence sources;
- using that information for more effective command and target engagement;
- building networks to better connect the ADF and protect its information; and
- adjusting culture, organisation, procedures, training and information system design so that Defence people can use these advances.

Defence science and technology will continue to provide support to the ADF as Defence moves forward with its implementation of NCW. DSTO's NCW S&T Initiative is the latest step in not only, improving S&T support to Defence's current NCW actions, but positioning DSTO's research program to continue to do so in the future.

Research into continuing improvements to information technologies will be crucial to further ADF implementation of NCW, with particular emphasis on collection, fusion, processing, dissemination and presentation of vast amounts of information. As well, for Defence to use these technologies to maximum effect, research will continue to be needed into the way in which people interact with information and share it with each other to achieve the better understanding needed to improve operations. Striking the best balance between technology and people is then essential in an ongoing quest to maintain a military technological edge while improving the ADF's high level of professional mastery.

In all these aspects, Australia's Defence Science and Technology can, and will, play an important role.

References

Abacus 2005, ' History', URL: http://www.ee.ryerson.ca:8080/~elf/abacus/history.html

Aeragon 2005, 'The US Civil War, the First Modern War.' URL: http://www.aeragon.com/03/

Alberts, DS 2002, *Information Age Transformation*, CCRP, United States, ISBN: 1-893723-06-2.

Alberts, DS, Garstka, JJ & Stein, FP 1999, *Network Centric Warfare*, 2nd Edn, CCRP, United States, ISBN: 1-57906-019-6.

Australian Department of Defence (DoD) 2002, *Future Warfighting Concept*, ADDP-D.3, December.

Barnett, TPM 1999, 'The Seven Deadly Sins of Network-Centric Warfare', *Proceedings of the US Naval Institute*. URL: www.nwc.navy.mil/WARDEPT/7deadl~1.htm

Batterham, R 2003, 'Leadership in R&D', Presentation to the DSTO Strategic Context Seminar for the Executive Leadership Development Program [accessed 16 July 2003], URL: http://web-vic.dsto.defence.gov.au/workareas/PS/activities/lead/scs.htm

Borgu, A 2003, 'The Challenges and limitations of Network Centric Warfare – The initial views of an NCW sceptic', Presentation to the conference: *Network Centric Warfare: Improving ADF capabilities through Network Enabled Operations*, 17 September.

Bowley, D & Gaertner P 2003, 'Virtual War, Military Revolutions, and Networks: A guide through the concepts from an Australian perspective', *Proceedings of the SPIE AeroSense 2003 Conference on Battlespace Digitization and Network Centric Warfare III*, Vol. 5105, pp. 138-149.

Bryans, N 2005, Interview with Gregor Ferguson, *Australian Defence Magazine*, Vol. 13, No. 5, May, p. 50.

Cebrowski, AK 1998, 'Network-Centric Warfare: Its Origin and Future', *Proceedings of the US Naval Institute* URL: www.usni.org/Proceedings/Article98/PROcebrowski.htm

Command and Control Research Program (CCRP) 2005, URL: http://www.dodccrp.org/research/ncw/ncw.htm

Directorate of Future Warfighting (DFW) 2004, *Enabling Future Warfare: Network Centric Warfare*, ADDP-D.3.1. Canberra, Australia. (March) ISBN: 0-642-50184-X.

Dstl 2004, *Distillation*, 3rd themed issue: Network Enabled Capability, UK MoD.

DSTO 2005, 'Theatre Broadcast System sets world standards', *Australian Defence Science*, Vol. 13, No. 1, Autumn.

DSTO NCW Tiger Team reports 2003 & 2005, URL: http://web-jsb.dsto.defence.gov.au/ncw/

Fewell, MP & Hazen, MG 2003, 'Network-Centric Warfare – Its Nature and Modelling', *DSTO Report RR-0262*, September.

Garstka, JJ 2005, Network Centric Warfare: An Overview of Emerging Theory. URL: www.mors.org/publications.phalanx/dec00/feature.htm

Haeckel, S 1999. *Adaptive Enterprise*, Harvard Business School Press.

Hill, R (Senator) 2003, Speech by Minister of Defence, Senator Robert Hill, ADF Network Centric Warfare Conference, Canberra, 20 May.

Houston, A 2005, 'The RAAF and the NCW Roadmap', *Australian Defence Magazine*, March, pp. 32–36.

Information Age 2005, People, Information & Technology, URL: http://www.hrw.com/science/si-science/physics/waves/infoage/infoage.html

Internet Society 2005, URL: http://www.isoc.org/internet/history/brief.shtml

Kaufman, A 2004, *Curbing Innovation: How Command Technology Limits Network Centric Warfare*, Argo Press, Canberra, Australia, ISBN: 0 9580238 4 0.

Lambert, D & Scholz, J 2005, 'A Dialectic for Network Centric Warfare', preprint, to be published in: *Proceedings of the 10th International Command and Control Research and Technology symposium (ICCRTS)*, MacLean, VA, June 13-16.

Limerick, DC & Cunnington, B 1993, *Managing the New Organisation: A Blueprint for Networks and Strategic Alliances*, Business & Professional Publishing, Chatswood, NSW.

Lundqvist, A 2000, 'NetDefence: the current Revolution in Military Affairs', *Military Technology*, No. 12, pp. 72-73, December.

Ministry of Defence (MoD) 2005, *Network Enabled Capability*, 01/05 C100, UK.

Moores, B 2002, 'The Dawn of Network Centric Warfare?' 22 January, URL: http://defence-data.com/features/fpage48.htm

NSI website 2005, URL: http://web-sa.dsto.defence.gov.au/DSTO/research/NCW/index.shtml.

Office of Naval Research (ONR) 2005, 'Command, Control & Combat Systems Applied Research', *US Department of Navy Broad Agency Announcement*, ONR BAA #05-013

Polk, RB 2000, 'A Critique of Boyd Theory – Is it Relevant to the Army?', *Defense Analysis*, Vol. 16, No. 3, December, pp. 257-276.

Stein, FP 1998, 'Observations on the Emergence of Network-Centric Warfare', URL: http://www.dodccrp.org/research/ncw/stein_observations/steinncw.htm

Tedeschi, E 2005, A Concise History of Electronics, URL: http://www.etedeschi.ndirect.co.uk/museum/concise.history.htm

Warne, L, Ali, I, Bopping, D, Hart, D & Pascoe, C 2004, 'The Network Centric Warrior: The Human Dimension of Network Centric Warfare', *DSTO Report CR-0373*.

Wellfare, J 2005, 'Awakening the new-age dragon', *Defence*, March, pp 18 & 19.

Notes

[i] Here 'synchronisation' may be viewed as the coordination and orchestration of military actions so that they occur at the desired time and place.

[ii] It may be argued that an increase in the influence of UN since its establishment in 1945, along with the emergence of an international media, has further complicated national security. A useful by-product of an NCW approach that is seldom discussed is the ability to be able to provide accurate information as to the nature of the targets attacked and hence the legitimacy of military actions undertaken.

[iii] Included in testing are modelling and simulation, experimentation and military exercises.

[iv] The argument revolves around whether to simply incorporate off-the-shelf (OTS) systems designed for civil applications, to continue to design bespoke systems for specific military applications or to explore some mixture of these two approaches. Cost, timescales for acquisition and entry into service, technical risk, and the military utility provided, should all be taken into account. The issue of matching COTS systems to purpose-designed military platforms, weapons and equipment should also be addressed.

[v] This brought an almost immediate end to the pony express messenger service that had been in operation for less than two years!

[vi] At the time of writing the NCW Concept was under review with the prospect of the issue of a revised version of ADDP-D.3.1.

[vii] Net assessment is a concept for planning at the strategic level. It aims to assess effects at a national level through a process that analyses the total situation considering friendly forces and neutral elements, the adversary, their perception of us and the environment.

[viii] At the time of writing a new NCW Roadmap was under development.

[ix] Constraints to this Function and Form would include: the Defence Capability Plan, existing military systems, societal and political factors, emerging NCW concepts and doctrine, and NCW as practised by our allies.

[x] This concept also fits in well with the Sense-Decide-Act (S-D-A) human cognitive behaviour model that crops up in many forms from an Action-Learning Cycle to an OODA (observe-orient-decide-act) loop as it is referred to in military circles. The sensor-to-shooter chain with feedback may also be thought of in terms of an S-D-A cycle. The important aspects are the adaptive and cyclic nature of the process.

[xi] The CCUP model can be thought of as a protected OODA loop.

[xii] Professional Mastery is said to be as much about mentoring and experience as training and education.