2009/02/04

Operações em Rede: da promessa à realidade (I Parte)[1]

João Vicente[2]

Assistimos com agrado a uma presença habitual da temática de Operações Centradas em Rede (OCR) na literatura nacional de Segurança e Defesa[3], assim como em inúmeras iniciativas de divulgação promovidas pelos diversos Institutos de Ensino Militar[4]. Também nós já discorremos em artigos anteriores sobre as vantagens e oportunidades desta doutrina[5]. Aproveitamos no entanto esta possibilidade para abordar alguns desafios que nos parecem sintomáticos, motivados pelo imperativo de aplicação desta doutrina nos apparatus de Defesa. Este imperativo de Transformação da Defesa, ou fatalidade como lhe chama António Telo[6], decorre da procura de interoperabilidade e consequentes aumentos de eficiência e eficácia na execução de missões militares.

O paradigma das OCR provocou uma alteração qualitativa no pensamento militar. A capacidade de combater em espaços de batalha remotamente dispersos, com uma consciência situacional acrescida poderá ter implicações futuras na estrutura da força. No entanto, como todas as promessas, são acompanhadas por desafios e vulnerabilidades. As lições aprendidas dos conflitos recentes revelaram as potencialidades assim como as fraquezas, alertando os seus proponentes para possíveis condicionantes, que se não forem tidas em consideração podem conduzir ao fracasso.

Não sendo de todo inclusivos, e estando muitas vezes interdependentes, os seguintes aspectos demonstram a atenção que esta temática tem vindo a suscitar na comunidade internacional, reflectindo por isso a sua importância. Conscientes da interactividade destes fenómenos, decidimos organizar a discussão tendo como ponto de partida as diferenças conceptuais, que enquadram os desafios em quatro dimensões: tecnológica, operacional, estratégica e cultural.

Diferenças conceptuais

O conceito OCR não é novo, tendo sido adaptado de práticas comerciais. Teve as suas origens na década de 90 nas forças navais norte-americanas, em resultado de uma nova forma de pensar acerca das operações militares e da vantagem competitiva resultante da superioridade informacional[7]. Desde então tem sofrido diferentes adaptações conforme as doutrinas de cada país, tornando difícil a sua compreensão. A maioria das nações está a procurar os benefícios das forças centradas em rede, entendendo o seu contributo na NATO, União Europeia ou em coligações ad hoc como fundamentais para a sua afirmação política. As diferenças de nome reflectem o diferente entendimento dos conceitos e traduzem o empenhamento dos recursos disponíveis, tendo por base o espectro de operações desejado. A conversão do conceito em capacidades encontra-se em vários estágios, dependendo do entendimento da importância que as OCR têm para cada país. Enquanto os EUA procuram um conceito “Network Centric Operations” (NCO) que lhes permita uma operação em todo o espectro de conflito, até ao nível estratégico, os outros países salientam a ligação dos vários componentes chave, com maior preponderância para o emprego táctico[8].

Apesar da necessidade de operar em rede ser aceite pela maioria dos países, a adopção dos vários níveis conceptuais pode gerar a disseminação de várias doutrinas e sistemas não compatíveis, pelo que se torna necessária uma acção integrada entre as várias nações. Essa função de análise e orientação está em parte a ser feita pela NATO, em estreita colaboração com as nações.

Dimensão tecnológica

As inovações militares afectam a balança de poder de cada época, introduzindo assimetrias no campo de batalha[9]. A introdução da cavalaria acelerou a queda do Império Romano. A besta e o arco e flecha permitiram que combatentes apeados disputassem a primazia dos cavaleiros. O telégrafo e os caminhos-de-ferro permitiram que as tropas da União desfrutassem de vantagens de comunicação e logísticas durante a Guerra Civil Americana. O surgimento do avião transpôs a Guerra para a 3ª dimensão, enquanto que a arma nuclear garantiu o fim da 2ª Guerra Mundial. O mesmo se tem verificado nas Guerras de última geração, em resultado de um novo estágio da Revolução nos Assuntos Militares, com o domínio espacial dos EUA e a extensão do conflito ao ciber-espaço.

A assumpção de que a tecnologia conduz à certeza militar está demonstrada historicamente não ser verdadeira. As lições retiradas dos conflitos recentes demonstram que a superioridade tecnológica não pôs cobro à incerteza da guerra. A experiência da Somália demonstrou que os sensores e as tecnologias de recolha e processamento de informação não foram suficientes para o sucesso da missão[10]. Também no Kosovo, ficou provado que a superioridade de informação não significa informação perfeita[11].

A mudança sem precedentes da tecnologia não deverá afastar as importantes lições históricas. Nem mesmo os melhores sensores podem dar resposta à incerteza causada pela interacção com o adversário.

Acções assimétricas com tecnologia Commercial Off-The-Shelf (COTS)

O termo assimétrico, relacionado com estratégias de combate, está normalmente associado a ataques de uma força mais fraca. Os conflitos americanos recentes mostram uma vantagem assimétrica esmagadora no plano tecnológico. No entanto essa vantagem tecnológica pode ser confrontada com contra-medidas, usualmente de custos reduzidos, com o intuito de reduzir a sua eficácia.

A tendência para a padronização e interdependência dos sistemas aumenta a facilidade com que uma vulnerabilidade, quando detectada e explorada por um adversário, possa afectar todo o sistema[12]. A ênfase crescente na utilização de sistemas e software comercial COTS, juntamente com a competitividade comercial e as práticas globalizadas de outsourcing, implicam que grande parte do software e hardware utilizado nos sistemas de armas e redes seja desenvolvido a nível internacional. O outsourcing de funções tecnológicas pode conduzir à transferência de conhecimento e tecnologia para eventuais adversários, assim como aumentar o risco de acções de espionagem e sabotagem.

As transferências de tecnologias de defesa constituem sempre um ponto de discórdia entre os EUA e os países Aliados, tentando os primeiros preservar a sua supremacia tecnológica, e os últimos obter o conhecimento completo sobre os sistemas de armas adquiridos[13]. Num relatório conjunto EUA/Reino Unido[14] é revelada a preocupação em evitar a disseminação de tecnologias críticas de defesa. O avanço tecnológico esmagador dos EUA está a diminuir em virtude da disseminação de tecnologias COTS, colocando ferramentas militares significativas à disposição dos adversários, incluindo tecnologias wireless de comunicação, sistemas GPS, imagens de satélite[15], capacidade de encriptação e a ubíqua internet.

Estas tecnologias, de custos reduzidos, permitem a criação de sistemas robustos e globais de C4[16], ao mesmo tempo que possibilitam a capacidade de interferir de modo eficaz com a operação de um adversário superiormente equipado. Por exemplo[17]:

- O Comando e Controlo (C2) pode ser efectuado através da tecnologia de comunicações móveis, recorrendo à internet para coordenar e controlar grupos dispersos;
- Os jammers de GPS podem degradar a precisão dos bombardeamentos, impedindo a sua utilização sobre centros populacionais;
- A utilização de decoys pode implicar o desperdício de munições dispendiosas e escassas;
- O ciber-terrorismo pode por si só provocar danos irreversíveis na cadeia de C2 adversária. Para além dos aspectos relativos a vírus informáticos e acções de sabotagem comercial, a sua operação pode ser degradada e mesmo destruída através do emprego de armas de pulso electromagnético elevado[18]. O efeito de surpresa é elevado, na medida em que não afectam fisicamente os combatentes, mas influenciam drasticamente as suas interacções, tornando inoperativos os sistemas electrónicos;
- Os sistemas de mísseis portáteis constituem uma ameaça credível contra alvos de alto valor, como aeronaves;
- Emprego de tácticas para negar o uso dos sistemas de detecção e de emprego de armas de precisão, como a camuflagem e a escavação de túneis e bunkers[19];
- Em última análise, ataques directos a satélites[20].

Sustentando a necessidade de compreender as vulnerabilidades da tecnologia, Loren Thompson acrescenta o exemplo[21] das redes que integram os sistemas navais de última geração não terem protecção electromagnética contra ataques assimétricos com armas nucleares. Segundo este autor, o importante é percebermos como os adversários podem explorar as vulnerabilidades nas novas tecnologias, mantendo uma necessária redundância nos sistemas militares.

Paralisia tecnológica e informacional

É um dado adquirido que novas tecnologias trarão novas dependências, e com elas novas

vulnerabilidades. Quem se lembra como era o mundo antes da televisão? Não será necessário recuar tanto tempo, bastando pensar como organizávamos o nosso quotidiano dez anos atrás sem o telemóvel ou o email.

Mesmo em conflitos altamente assimétricos, adverte-nos Stephen Wolthusen[22], não deveremos assumir que a superioridade tecnológica garantirá por si só o sucesso, uma vez que a crescente dependência militar na infra-estrutura tecnológica é um factor de vulnerabilidade. Tentando contrariar os seus efeitos, deveremos planear as operações tendo em conta, a mais que provável, degradação de sistemas em resultado da interferência do adversário, da própria falência dos sistemas ou da operação em coligação com uma força menos sofisticada.

Esta competência de integração da componente humana em fases críticas de processamento e análise da informação, deve garantir uma capacidade para reverter, caso necessário, a um modelo de operação pré-OCR, no sentido de impedir uma paralisia decorrente da dependência tecnológica e informacional. Este é o preço a pagar por sistemas altamente complexos e interligados.

3.3. Capacidade de transmissão de informação

A capacidade de omnisciência do espaço de batalha implica custos, que se traduzem na largura de banda. Ou na falta dela.A insuficiência de largura de banda é um dos desafios mais complexos das OCR, podendo afectar a capacidade de em tempo oportuno se partilhar informação crítica. A largura de banda traduz a razão de transmissão de informação entre sistemas (bits por segundo). A sua falta produz efeitos imediatos no quotidiano, reflectidos no congestionamento de comunicações. Como recurso limitado, necessita por isso de uma gestão criteriosa, até porque se vem constatando que os conflitos da era RAM são autênticos “devoradores” de largura de banda.

Estima-se que desde 2001, as necessidades de largura de banda do Comando Central Americano, tenham aumentado 8 vezes[23]. Os 500.000 homens envolvidos na operação Desert Storm em 1991 dispunham de uma largura de banda de 100 megabit por segundo (Mbit/s). Na OIF, os 350.000 homens dispuseram de 3.000 Mbit/s de largura de banda por satélite. Ou seja, 30 vezes mais para uma força com 45% do tamanho[24]. No entanto, durante a OIF, existiu a necessidade de prioritizar a transmissão de mensagens devido à reduzida largura de banda, quando comparada com o volume de informação transmitida. Esta situação provocou demoras de transmissão e interpretação de ordens, atrasando o processo de decisão[25].

- A tecnologia de comunicação sem fios (wireless) é o meio essencial de transmissão de informação nas operações militares modernas. No entanto, esta dependência levanta alguns problemas relativamente à transmissão dos sinais, que podem afectar a eficácia das OCR[26]:
- Segurança da transmissão – os links digitais têm de ser encriptados para impedir possíveis intercepções de informação. Mesmo assim, basta a detecção de um sinal para fornecer informação valiosa ao oponente acerca da presença, posição e actividade da entidade emissora.
- Potência de transmissão – as barreiras à propagação dos sinais, como o mau tempo ou o jamming, não devem constituir impedimento ao funcionamento das redes.
- Capacidade de transmissão – numa era de digitalização do espaço de batalha, a rapidez com que se transmitem os dados é de importância vital. No entanto, a robustez contra jamming e a encriptação são feitas à custa da largura de banda. O desenvolvimento de processos de compressão digital de dados tendem a reduzir este problema, mas não a eliminá-lo.
- Protocolos de comunicação – existem variedades incomportáveis de protocolos, frequências de operação e modulação de sinais que necessitam de ser compatibilizadas para que os sistemas possam interoperar de forma eficaz. A harmonização dos sistemas é por isso uma necessidade.

Dimensão operacional

Validação operacional do conceito

A influência humana na aplicação de um conceito tem sempre um factor não mensurável, com resultados diferentes dos planeados[27], reflectindo que a diferença entre a guerra real e a guerra no papel continua a existir. As experiências, os exercícios e as operações reais têm contribuído para a validação do conceito. Mesmo os jogos de guerra, essenciais para testar conceitos e tácticas, não devem ser interpretados como reprodutores fiéis da realidade, na medida em que podem ser amplamente controlados para conduzir a resultados desejados[28]. Os exercícios se bem que mais realísticos do que as experiências não reproduzem os rigores e a complexidade de uma operação real.

Apesar do conflito do Iraque de 2003 ser usado como exemplo das vantagens do conceito OCR, é necessário colocar em perspectiva a maneira como foi obtida a vitória. As capacidades iraquianas sofreram pesadas baixas após a Guerra de 1991, decorrentes de embargos e de ataques cirúrgicos

aos centros de defesa aérea, durante mais de 10 anos. De igual modo, a estratégia e liderança iraquianas deixaram muito a desejar, possibilitando o desmembramento rápido das forças. Não se deve por isso pensar que a superioridade de informação, por si só, significou a vitória. A dependência na superioridade de informação é por vezes inibidora da tomada de riscos e audácia, não substituindo maus processos de decisão ou estratégia errada. De acordo com alguns autores, a incompetência iraquiana possibilitaria a validação de qualquer conceito[29].

Excesso de informação

As OCR visam comunicar a intenção de comando enquanto promovem a auto-sincronização dos escalões inferiores na procura dos efeitos desejados. No entanto tem de se considerar o contexto em que estas operações se desenrolam. Numa era onde os altos níveis de interoperabilidade e operação conjunta interagem com formas inovadoras de combater, torna-se obrigatório desenvolver uma capacidade de consciência situacional partilhada. Apesar das tecnologias de informação contribuírem para um aumento da consciência situacional dos comandantes, contribuem também para um aumento da complexidade do ambiente de tomada de decisão.

Este processo é severamente prejudicado pelas limitações relacionadas com o excesso de informação, em particular do seu colossal volume; da dificuldade de gestão em tempo útil (filtrar, rever, interpretar); da irrelevância de grande parte; e da miríade de fontes que a originam, com fortes possibilidades de desinformação[30].

O excesso de informação está intimamente ligado às limitações de largura de banda. Ambos contrariam a agilidade do processo de decisão, provocando uma paralisia incompatível com os requisitos de execução das OCR. Durante a Guerra do Iraque de 2003 os comandantes foram inundados por uma quantidade sem precedentes de informação. Para além disso tinham de participar em vídeo-conferências com dirigentes civis e militares nos antípodas, alimentando ao mesmo tempo o apetite insaciável das organizações noticiosas. Enquanto isto dirigiam uma guerra, tomando decisões estratégicas com rapidez suficiente para manter o “tempo” das operações.

Mais informação não significa a solução dos problemas militares. A dificuldade de seleccionar informação pertinente pode causar baixas colaterais importantes. A indecisão dos comandantes pode estar dependente do excesso de informação e da pressão em obter resultados precisos, sendo por isso essencial a prioritização das necessidades de informação. Este potencial de “inundar” os participantes com informação a todos os níveis da guerra, através da Imagem Operacional Comum, pode conduzir a uma percepção incorrecta do que é táctico, operacional ou estratégico[31], implicando interferências entre as competências dos vários participantes. É essencial que a gestão individual do volume de informação seja compreendida, tendo em conta a aplicação dessa realidade virtual em combate.

Operação conjunta

A operação em coligação acrescenta mais desafios à implementação das OCR, nomeadamente ao nível de tomada de decisão e à interoperabilidade das forças. As complexas cadeias de decisão tornam lentos os processos de consenso acerca de objectivos, meios e formas de os alcançar. Para além disso, a integração de capacidades para executar uma missão com maior eficácia envolve também a contribuição de civis, indústria e parceiros de coligação. Através desta integração torna-se possível que uma organização de dimensão reduzida possa contribuir para a execução de tarefas complexas. Neste âmbito, as vertentes sociais e psicológicas assumem de novo função relevante, ao estabelecerem as bases para a confiança e a vontade de cooperar e partilhar informação[32]. A formação dos intervenientes para um pensamento e comportamento conjuntos é por isso um dos aspectos centrais aos esforços de Transformação.

[1] Texto originalmente publicado na Revista Nação e Defesa, nº 120, Verão 2008.

[2] Major piloto aviador, mestre em Estudos de Guerra e Paz.

[3] ALVES, Armando – A GNR e o futuro. CORREIA, Armando – Forças Armadas em rede. CORREIA, Armando – Uma Marinha em Rede. EUGÉNIO, António – A Transformação das Forças Armadas de Portugal. NUNES, Luis – Network Centric Warfare e a sua influência nas unidades de infantaria de baixo escalão. SANTOS, Eduardo – Network Centric Warfare.

[4] ALBERTS, David – New C2 Concepts and Capabilities for the Future Joint Armed Forces. HAYES, Richard; HAYES, Margaret – Homeland Security e Operações Centradas em Rede. NUNES, Viegas – Informação e Guerra. STEIN, Frederick [et al.] – Network Centric Operations Short Course.

[5] A (R)Evolução no pensamento estratégico; Operações em Rede: contributos para o seu estudo;

Operações Baseadas em Efeitos: o paradigma da Guerra do séc. XXI; Estratégia Baseada em Efeitos: em busca da clarificação conceptual.

[6] TELO, António – Portugal e a Transformação da Defesa.

[7] CEBROWSKI, Arthur; GARSTKA, John – Network Centric Warfare: its origin and future.

[8] BORGU, Aldo – The challenges and limitations of Network Centric Warfare: the initial views of an NCW sceptic, p. 4.

[9] LAMBAKIS, Steven – Reconsidering asymmetric warfare, p. 106.

[10] Como o caso mediático do abate do abate do helicóptero Blackhawk e dos corpos de militares americanos arrastados pelas ruas.

[11] Relembre-se o bombardeamento à embaixada da China em Belgrado.

[12] Por exemplo o Future Combat System do Exército americano é um exemplo de um "sistema de sistemas" com os seus 18+1+1 componentes em rede (18 sistemas mecânicos, mais a rede e o soldado) multiplicando a sua potência. No entanto se um dos sistemas individuais se danifica, isso implicará uma degradação completa do sistema. DAVIS, Daniel – Flawed Combat System: FCS is too costly, overly complex and potentially dangerous.

[13] Por exemplo as controvérsias sobre a transferência de tecnologias relacionadas com o projectoJoint Strike Fighter provocaram ameaças, por parte do Reino Unido, de cancelamento da encomenda de aeronaves norte-americanas.

[14] United States Defense Science Board; United Kingdom Defence Scientific Advisory Council – Defense critical technologies report.

[15] Veja-se o caso do Google Earth ou o IGeoE-SIG do Instituto Geográfico do Exército em http://www.igeoe.pt/.

[16] Comando, Controlo, Comunicações e Computadores.

[17] DICK, Charles – Conflict in a changing world: looking forward two decades, p. 12. Em vez de tentar acompanhar a superioridade do inimigo no desenvolvimento de capacidades em todo o espectro de conflito, um adversário assimétrico poderá investir em áreas críticas, como a defesa aérea, mísseis móveis e ADM.

[18] Designadas como HPM (high-power microwave), estas armas podem queimar um sistema electrónico, como um radar, um GPS ou um computador.

[19] WILSON, Clay – Network Centric Warfare: background and oversight issues for congress, p. 12-14.

[20] No futuro irá colocar-se a questão da segurança física dos satélites. Por enquanto os EUA detêm o domínio espacial, beneficiando por isso de segurança e liberdade de acção.

[21] THOMPSON, Loren – Two cheers for Transformation, and some words of caution.

[22] WOLTHUSEN, Stephen – Self-inflicted vulnerabilities.

[23] HUGHES, David – Pentagon targets bandwidth expansion, p. 59. Por exemplo os UAV são um dos grandes consumidores de largura de banda, hipotecando recursos dedicados para transferirem vídeo e imagens radar.

[24] RADUEGE, Harry – Net-Centric Warfare is changing the battlefield environment. Considerando apenas a componente aérea registou-se um aumento de 596% para 783 Mbit/s. MOSELEY, Michael – Operation Iraqi Freedom: by the numbers, p. 12.

[25] WILSON, Clay – op. cit., p. 23.

[26] KOPP, Carlo – Understanding Network Centric Warfare.

[27] BORGU, Aldo – The challenges and limitations of Network Centric Warfare: the initial views of an NCW sceptic, p. 2.

[28] MCMASTER, H. – Crack in the foundation: Defense Transformation and the underlying

assumption of dominant knowledge in future warfare, p. 83.

[29] KAGAN, Frederick – War and aftermath.

[30] WARNE, Leoni; ALI, Irena; BOPPING, Derek; et. al. – The network centric warrior: the human dimension of Network Centric Warfare, p. 20.

[31] BARNETT, Thomas – The seven deadly sins of Network Centric Warfare.

[32] WARNE, Leoni [et al.] – op. cit.,p. 21.

5 Textos Relacionados:

2009/02/05

Operações em Rede: da promessa à realidade (II Parte)[1]

João Vicente[2]

2008/07/21

Operational Preparation Directorate Core Business – NATO Response Force

Pedro Brito Teixeira and Alex Mezynski[1]

2007/05/30

Operações em Rede. Contributos para o seu Estudo[1]

João Nunes Vicente [2]

2007/02/04

Operações Baseadas em Efeitos: O Paradigma da Guerra do Século XXI[2]

João Vicente[1]

2005/03/05

Network Centric Warfare

Eduardo Silvestre dos Santos