A Guerra Centrada em Rede: um breve balanço, dez anos depois

Tenente-coronel
António Luís Beja Eugénio

Quando, em Agosto de 2000, publicámos nesta prestigiada Revista o primeiro artigo sobre Guerra Centrada em Rede[1] (GCR) em Portugal, estávamos longe de imaginar os desenvolvimentos posteriores. Continuámos, em Novembro de 2002, também nestas páginas, apresentando em português o essencial da nova teoria de guerra. Mesmo nessa altura, quando os sinais de desenvolvimento do novo corpo de ideias que enformava a Teoria Militar eram por demais evidentes, não sonhávamos a prolixidade associada a este novo filão, ao ponto de hoje ser considerado um "conceito dominante". Novos conceitos são sempre mal recebidos nas estruturas concebidas exactamente para conservar a ordem existente e, se necessário, combater para a sua manutenção. Pode muito bem ser esse o caso da Guerra Centrada em Rede e das forças armadas, em geral. Será então nossa intenção fazer agora uma breve recapitulação, em jeito de balanço, da evolução do conceito de GCR, desde que surgiu, nos interstícios do Pentágono, até aos dias de hoje e a sua aceitação por parte das forças armadas, especialmente as ocidentais.

Em primeiro lugar, abordaremos o essencial da teoria da GCR, para depois darmos voz aos críticos. Passaremos os olhos pelos teatros de operações modernos para verificar se existe alguma aplicabilidade das premissas da GCR, para concluirmos que o grande problema reside a nível estratégico e ou político, pelo que a GCR se tornou num "*master concept*" (Mitchell, 2006) apontando a direcção para onde os Estados Unidos estão a transformar as suas forças armadas. Como tal, está no centro das atenções ao mais alto nível, uma vez que no plano táctico e operacional as soluções técnicas existem e são aplicadas. Daí a importância da discussão que propomos fazer.

A primeira menção ao termo *Network Cenrtric Warfare* surge numa obscura publicação, o *Federal Computer Week*[2], num artigo de Brewin (1997), em que é feito o resumo da gestão das redes de informação de cada ramo das forças armadas americanas, começando por notar que elas foram surgindo sem serem planeadas. Porém, o artigo seminal sobre o assunto surgiu pouco tempo depois, em Janeiro de 1998, na revista *Proceedings of the United States Naval Institute*, da autoria do Vice-Almirante Arthur

Cebrowski[3] e de John Garstka[4], com o título *Network-Centric Warfare: Its Origin and Future*. Mitchell (2006) num *Adelphi Paper*[5] atribui a origem da ideia da necessidade de interligação em rede à época da Segunda Guerra Mundial, mais precisamente à necessidade de coordenar plataformas aéreas a partir de plataformas navais. Daí que não seja de estranhar a publicação, em 1996, de um artigo da autoria do Almirante William A. Owens, com o título "*The Emerging Systems of Systems*"[6] que descreve a concatenação de sensores, sistemas de comando e controle e armamento de precisão que conduziria ao "*dominant battlespace knowledge*". No mesmo ano surge o documento visionário *Joint Vision 2010*[7] que é a referência conceptual para alcançar o domínio em todas as áreas das operações militares, através da aplicação de novos conceitos (Mitchell, 2006).

O artigo de Cebrowski e Garstka (1998) parte do princípio que a economia e a sociedade norte-americanas mudaram, especialmente devido às tecnologias base em que se apoiam, para propor um modelo que seria o equivalente militar ao comércio electrónico. Foi proposto um modelo lógico em que sensores e atiradores eram interligados com as outras entidades relevantes do espaço de batalha[8] (órgãos de comando e controle) por uma rede de elevada performance que fornecesse a espinha dorsal das comunicações. O contraponto em termos de pensamento era feito com a operação centrada nas plataformas, típica da Era Industrial, e eram avançados três requisitos fundamentais para alcançar a GCR: capital intelectual, capital financeiro e um processo de transformação. Era assumida uma Revolução nos Assuntos Militares (que continua a gerar polémica e da qual nos afastaremos neste nosso esforço de síntese) baseada na tecnologia de informação, porque agora vivíamos na Era da Informação.

Ainda em 1998, surge outro artigo da autoria de Stein (1998), onde é feita a relação entre o JV2010 e a GCR, em que a superioridade informacional (tal como antes as outras superioridades…terrestres, navais, aéreas) permitia alcançar os novos desideratos, nomeadamente, a Manobra Dominante, o Envolvimento Preciso, a Logística Focada e a Protecção Total[9], que, por sua vez fariam aumentar a capacidade de combate. Ao mesmo tempo decorre, pelo menos desde 1996, um programa de investigação denominado CCRP[10], no Gabinete do Sub-Secretário de Estado da Defesa para as Redes e Integração de Informação, liderado por David Alberts. Este programa centra-se no Comando e Controle e visa, em primeiro lugar, quer o estado da arte, quer o estado da prática do comando e controle e, em segundo lugar, melhorar o entendimento que o Departamento da Defesa tem das implicações da Era da Informação na segurança nacional na Era da Informação[11].

Sob a batuta de Alberts, o CCRP deu início a uma prolífica produção de literatura sobre os temas centrais da transformação, avançando conceitos chave inovadores como o da GCR, Operações Baseadas em Efeitos, Agilidade e Experimentação, entre outros. Da imensa literatura, a maior parte disponível online, Mitchell (2006) destaca três obras: "*Network Centric Warfare: Developing and Leveraging Information Superiority*", da autoria de Alberts, Garstka e Stein (1999); "*Understanding Information Age Warfare*" da autoria de Alberts, Garstka, Hayes e Signori (2001); e "*Power to the Edge: Command and Control in the Information Age*", da autoria de Alberts e Hayes (2003). Esta trilogia

constitui o âmago de onde a maior parte das ideias sobre GCR emergiram. A primeira obra, *Network Centric Warfare*, muito ligada à ideia dos futurólogos Alvin e Heidi Toffler que sugeriam no seu *"War and Anti-war: Making Sense of Today's Global Chaos"* de 1993, que o modo de enriquecer é também o modo de guerrear, avança uma quantidade de casos de sucesso do mercado em que as empresas alcançaram superioridade informacional sobre os seus competidores porque comprimiram o espaço e o tempo de decisão, através da interligação automática das cadeias logísticas entre fornecedores e clientes. Estas ideias eram transponíveis para o ambiente militar, onde métricas como "velocidade de comando" e "consciencialização do espaço de batalha" podiam ser verificadas através do desenvolvimento e co-evolução de pacotes de capacidades de missão[12], indo desde o desenvolvimento do conceito até à implementação final, num processo de desenvolvimento em espiral, tal como ilustrado na Figura 1.

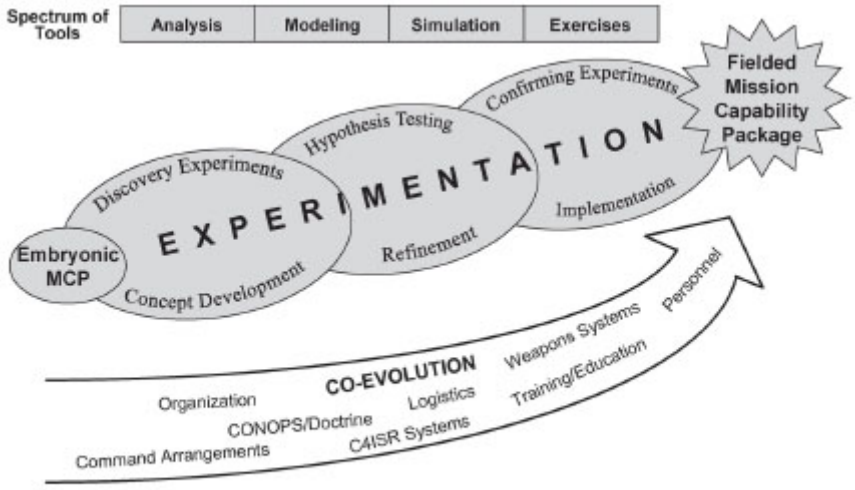

Figura 1 – A Co-evolução dos Pacotes de Capacidades de Missão

É postulado que mudanças isoladas em qualquer dos elementos constitutivos dos Pacotes de Capacidades de Missão podem ter resultados disfuncionais e que mudanças coordenadas podem ter resultados sinérgicos. É garantido que o nevoeiro e o atrito da batalha de que falava Clausewitz, senão eliminados, serão seguramente reduzidos, levando a uma maior eficácia no cumprimento da missão, pela "simples" partilha de informação entre as entidades relevantes do espaço de batalha.

A segunda obra, *Understanding Information Age Warfare*, baseada na anterior, desenvolve uma autêntica teoria de operações em ambientes interligados em rede. É criada uma nova linguagem que inclui os termos "sentir" (directa e indirectamente), "observações" (dados), "informação", "conhecimento", "consciência", "compreensão", "partilha da informação", "partilha do conhecimento", "partilha da consciência", "colaboração", "decisões", "acções" e "sincronização" e são definidos três domínios, a saber: o domínio físico, o domínio informacional e o domínio cognitivo, que se encontram ilustrados na Figura 2.

Figura 2 – Os Domínios da GCR

Existe uma relação entre cada um dos termos da linguagem utilizada e o domínio onde esse termo deve ser entendido. No domínio físico existe a situação que a força militar quer influenciar. É o domínio da realidade. Aí ocorre o ataque, a protecção e a manobra, no ambiente aeroespacial, naval e terrestre. É o domínio onde residem as plataformas físicas e as redes de comunicações que as interligam. Em termos comparativos, os elementos deste domínio são os mais fáceis de medir. Como consequência, o potencial de combate tem sido medido, ao longo do tempo, em termos de letalidade e sobrevivência, principalmente neste domínio.

No domínio informacional reside a informação. É o domínio onde a informação é criada, manipulada e partilhada. É aí que ocorre a comunicação entre elementos de uma força; onde o comando e controlo é transmitido. É através dele que a intenção do comandante é veiculada.

A informação pode reflectir verdadeiramente o que se passa no domínio da realidade ou não. Por exemplo, um sensor observa directamente algo e produz um determinado "output", que existe no domínio da informação. Com excepção da observação sensorial directa, toda a informação que temos acerca do mundo chega-nos através do domínio da informação e é através deste domínio que comunicamos com os outros.

Consequentemente, é cada vez mais o domínio da informação que tende a ser preservado e defendido, para permitir a uma força gerar potencial de combate, quando confrontada com um ataque inimigo. No domínio da informação decorre a batalha pela superioridade informacional. As forças em conflito esgrimem acções, neste domínio, em termos de

relevância, tempestividade, precisão e topologia da informação. A medida dos parâmetros do domínio da informação é mais difícil do que a medida dos parâmetros do domínio físico, pelo que a superioridade informacional pode apenas ser estimada.

O domínio cognitivo existe nas mentes dos participantes. É aí que residem as percepções, a consciência, a compreensão, as crenças e os valores, dos quais resultam decisões, por via do sentido que aqueles fazem nas mentes dos combatentes. É neste domínio que muitas batalhas e guerras são, de facto, ganhas e perdidas. Este é o domínio dos intangíveis: liderança, moral, espírito de corpo, nível de treino e de experiência, consciência situacional e opinião pública. É neste domínio que residem a intenção do comandante, a doutrina, as tácticas, as técnicas e os procedimentos.

Todo o conteúdo do domínio cognitivo passa por um filtro ou uma lente designada por percepção humana. Este filtro é constituído por um conjunto de características pessoais tais como: mundividência, conhecimento pessoal, experiência, treino, valores, inteligência, etc. Dado esta lente ser pessoal, sabe-se que a cognição pessoal é única.

A obtenção de superioridade neste domínio é extremamente difícil de medir, pelo que só é possível inferir, a partir da análise comportamental e das perguntas aos militares envolvidos nas operações, a sua consciência situacional, a consciência partilhada, o conhecimento partilhado e a colaboração.

Só existe uma realidade ou domínio físico. Esta realidade é convertida em dados, informação e conhecimento por sistemas no domínio da informação. Através do treino e da experiência partilhada, tenta-se que as actividades cognitivas dos decisores militares sejam similares, mas, apesar disso, elas continuam a ser únicas. As diferenças na tomada de decisão variam significativamente com o ramo, com a geração e com o país a que pertence o decisor. A maior semelhança de decisões acontece entre indivíduos da mesma unidade ou do mesmo ramo.

A última obra da trilogia, *Power to the Edge*, acrescenta um domínio aos anteriores, designadamente, o Domínio Social, que medeia as avaliações, os julgamentos e as decisões desenvolvidas no Domínio Cognitivo. Nesta obra, os autores defendem que, para tirar partido de todas as oportunidades oferecidas pela GCR, as forças armadas devem focar-se no comando e controle, onde a informação é traduzida em conhecimento accionável. Nos teatros modernos, face à sua complexidade, é fundamental que as modernas organizações militares sejam capazes de partilhar a sua consciência situacional própria com outras. Uma vez que essas organizações não sabem com quem vão trabalhar, à partida, é requerido um elevado grau de partilha.

Daqui decorre que a centralização do comando e controle está a tornar-se cada vez mais impraticável. Em vez dessa centralização é proposta a devolução de poder para as entidades situadas na orla (sítio onde uma organização interage com o seu ambiente de operação), o que envolve acesso a informação e a remoção das restrições desnecessárias. Esta visão é potencialmente revolucionária (Mitchell, 2006), já que ataca as estruturas militares hierarquizadas que tradicionalmente utilizaram o comando e controle para

veicular informação. Apesar disso, o desenvolvimento da designada *Global Information Grid* (GIG), como um exemplo de integração de comunicações e sistemas de computadores numa infoestrutura segura e sem costuras, que fornece acesso a variadíssimas fontes de informação e a recursos de gestão de informação. As capacidades principais da GIG[13], uma rede mundial privada (*private world wide web*) estarão activas em 2010 por um preço de 21 mil milhões de dólares. O desenvolvimento completo não é esperado antes de 2020.

Os críticos da GCR não se fizeram esperar. Um ano após o artigo original, surgia a primeira crítica, veiculada por Thomas Barnett[14] (1999) na mesma publicação onde tinha surgido o artigo de Cebrowski e Garstka, que acusava a GCR de ter sete pecados mortais: Luxúria - a GCR procura um adversário que merece a sua riqueza tecnológica; Preguiça - a GCR atrasa a adaptação das forças armadas americanas a um mundo em que prevalecem as operações militares que não de guerra[15]; Avareza - a GCR prefere os muitos e baratos, enquanto as forças armadas americanas preferem os poucos e caros; Orgulho - a estratégia de paralisia do inimigo ressuscitam velhos mitos como o do bombardeamento estratégico; Ira - a filosofia da velocidade de comando pode provocar uma situação de atirar primeiro e fazer as perguntas depois; Inveja - a GCR cobiça a auto-sincronização do mundo dos negócios; Gula - a imagem comum partilhada pode conduzir a uma situação de excesso de infor-mação.

Se este tipo de discussão se passa dentro de um único país, que dizer dos seus aliados, ou ainda dos seus potenciais inimigos? Na Europa, apenas um país parece ter compreendido o impacte da Era da Informação nas Operações militares: a Suécia, que desenvolveu o seu próprio sistema, denominado *Network Based Defense*. Este país é o único que participa num fórum bilateral com os Estados Unidos sobre estas matérias, constituindo um caso de estudo[16], dada a sua dimensão, mas sublinhando a sua tradicional neutralidade. Quanto aos aliados e começando pelo mais chegado, o Reino Unido limitou-se a retirar as arestas revolucionárias (tipicamente alérgicas ao sentir britânico) do conceito de GCR para desenvolver a sua Capacidade Permitida pela Rede (*Network Enabled Capability*[17]), não tão ambiciosa quanto a GCR, mais pragmática, no sentido de visionar imediatamente programas e aplicabilidade, mas sem nenhuma novidade. Os outros anglófonos, Canadá, Austrália e Nova Zelândia seguem os conceitos americanos, mas quando participam em coligações com os seus aliados sobressaem os problemas de interoperabilidade e de (falta de) confiança, o que conduz à deriva norte-americana para o unipolarismo de actuação e à frustração dos aliados por falta de reconhecimento do esforço dispendido.

Mitchell (2006) observa que a interoperabilidade e a confiança podem ser vistos em círculos concêntricos à volta dos Estados Unidos. Assim, o mais próximo seria o Reino Unido, com o qual seriam possíveis coligações e existiria uma verdadeira partilha de informação. Seguem-se os países anglófonos já mencionados, tradicionais aliados dos Estados Unidos nas suas operações. Depois, numa lógica bilateral e regional, o Japão e a Coreia do Sul. Por fim, a OTAN, que adoptou o conceito de NEC inglês, transformando-o em *Nato Network Enabled Capability* (NNEC), mas que visa exactamente os mesmos

propósitos americanos, conduzindo à criação de um comando de nível estratégico para a transformação, o *Strategic Allied Command Transformation* (SACT). Este comando conduz, desde 2004, Conferências abertas[18] sobre NNEC[19]. Foi efectuado um estudo de adequabilidade da NNEC pela Nato Consultation, Command and Control Agency (NC3A), sedeada em solo europeu, que conclui que será muito difícil à OTAN alcançar a NNEC sem grandes mudanças nas estruturas de implementação de *Communication and Information Systems* (CIS), nas políticas e nos processos. São propostas uma Estratégia para a Transformação e uma arquitectura para a integração.

Do lado dos potenciais opositores chegam-nos críticas vigorosas. Um documento doutrinário chinês, traduzido pela CIA, com o título inglês *Unrestricted Warfare*, afirma peremptoriamente que os americanos se deixaram cair na sua própria armadilha tecnológica, criando aquilo que os coronéis chineses designam por Linha Maginot Electrónica. Este modo chinês de analisar os desenvolvimentos nas operações militares americanas não passou despercebido e já provocou três *simposia* na Johns Hopkins University[20].

Entretanto, dos espaços de batalha não chegam boas notícias, especialmente porque o sistema ainda é conduzido por homens e estes têm as suas próprias idiossincrasias relacionadas com a organização que servem ou com a sua proveniência. Uma análise efectuada pelo CENTCOM, relativa às operações no Afeganistão, no ano de 2003, concluía que os planeadores americanos tinham que lidar com nada menos que 84 redes da coligação. Por outro lado, as questões relacionadas com a confiança causavam brechas mesmo entre os aliados mais próximos, pelo que será ilusória a partilha de informação proveniente directamente dos sensores. Aquilo que será partilhado será *track information*. A última palavra residirá na política e na estratégia dos contribuintes para as coligações de vontade.

Aquilo que começou por serem aplicações tácticas de troca de informação evoluiu para um conceito operacional que já está em prática por forças dos Estados Unidos, do Reino Unido e da Suécia. Os aliados destes países só podem aspirar a ser interoperáveis com eles, o que faz despoletar o nível estratégico e político, ou seja, que informação estará cada país apto para fornecer a uma coligação ou aliança, quando tenta maximizar o seu interesse e remediar as suas limitações, uma vez que é esse o fim de uma coligação.

Por aquilo que foi dito, não será pelo plano da tecnologia que a GCR vingará como conceito operacional que já é, mas sim pela vontade política dos actores internacionais, como sempre foi.

Bibliografia

Alberts, David S., Garstka, John J., Stein, Frederick P. (1999), *Network Centric Warfare: Developing and Leveraging Information Superiority*, disponível online em http://www.dodccrp.org/files/Alberts_NCW.pdf [acedido a 15 de Abril de 1998]

Washington: CCRP.
ALBERTS, David S. et al. (2001), *Understanding Information Age Warfare***,** disponível online em http://www.dodccrp.org/files/Alberts_UIAW.pdf [acedido a 15 de Abril de 2008], Washington: Assistant Secretary of Defense C3I CIO.
Alberts, David S. e Hayes, Richard E. (2003), *Power to the Edge*, disponível online em http://www.dodccrp.org/files/Alberts_Power.pdf [acedido a 15 de Abril de 2008], Washington: CCRP.
Barnet, Thomas P. M., The Seven Deadly Sins of Network-Centric Warfare, *Proceedings of the U. S. Naval Institute*, 125, 1.
Barnet, Thomas P. M. (2004), *The Pentagon's New Map: War and Peace in The Twenty-First Century*, New York: Berkley Books, ISBN 0-425-20239-9.
Brewin, Bob (1997), DOD lays groundwork for network-centric warfare, *Federal Computer Week*, 31 de Outubro de 1997, disponível online em http://www.fcw.com/print/3_50/news/65507-1.html [acedido a 15 de Abril de 2008].
Cebrowski, Arthur K. e Garstka, John J. (1998), Network-Centric Warfare: Its Origin and Futures, *Proceedings of the U. S. Naval Institute*, 125, 1.
Mitchell, Paul T., (2006), Network Centric Warfare, Coalition Operations in the Age of US Military Primacy, *Adelphi Paper 385*, ISSN: 1478-5145.
Owens, William A., The Emerging Systems of Systems (1996), *Strategic Forum*, 63, disponível online em http://www.ndu.edu/inss/Strforum/SF_63/forum63.html [acedido a 15 de Abril de 2008].
Stein, Fred P. (1998), *Observations on the Emergence of Network Centric Warfare*, artigo não publicado, disponível online em http://www.dodccrp.org/files/stein_observations/steinncw.htm [acedido a 15 de Abril de 2008].
Toffler, Alvin e Toffler, Heidi (1995), *War and Anti-War***,** New York: Warner Books. ISBN 0-446-60259-0.

_____

* Sócio Efectivo da Revista Militar.

_____

1 Tradução nossa de *Network Centric Warfare*.
2 Pertencente a um grupo designado *1105 Government Information Group* que fornece informação e *media* em geral para o mercado de tecnologia de informação oficial. Cf. http://www.1105govinfo.com/ [acedido a 14 de Abril de 2008].
3 Falecido a 12 de Novembro de 2005. Foi o primeiro chefe do *Office of Force Transformation*, um *think tank* composto por cerca de 30 pessoas e integrado no Gabinete do Secretário da Defesa Norte-americano. De notar que enquanto o esforço de transformação das forças armadas americanas era uma das bandeiras do então Secretário Donald Rumsfeld, o gabinete continua activo mesmo com a sua substituição, o

que indicia uma constância no rumo de mudança, talvez agora menos propagandeada. Cf. http://www.oft.osd.mil/ [acedido a 14 de Abril de 2008].

4 Um civil ligado aos sistemas de Comando, Controle, Comunicações e Computadores, Informações, Vigilância e Reconhecimento (C4ISR).

5 Publicado pelo *International Institute for Strategic Studies*, que reclama para si o papel de liderança em assuntos políticos. Cf. http://www.iiss.org/ [acedido a 15 de Abril de 2008].

6 Publicado na Revista da *National Defense University*, a *Strategic Forum*. Disponível online em http://www.ndu.edu/inss/Strforum/SF_63/forum63.html [acedido a 15 de Abril de 2008].

7 Disponível em http://www.dtic.mil/jv2010/jv2010.pdf [acedido a 15 de Abril de 2008].

8 Que substitui o velho "Campo de Batalha", no léxico próprio da GCR.

9 Tradução nossa de *Dominant Maneuver*, *Precision Engagement*, *Focused Logistics* e *Full-Dimensional Protection*, respectivamente.

10 *C4ISR Cooperative Research Program*.

11 De acordo com http://www.dodccrp.org/html4/about_main.html [acedido a 15 de Abril de 2008].

12 Estes são constituídos *ad hoc* e integram um Conceito de Operações, Aproximações de Comando/ Liderança, Organização, Doutrina, Sistemas C4ISR, Sistemas de Forças e de Armas, Logística, Treino/ Formação e Pessoal.

13 O embrião da GIG já existe. Tem o nome de SIPRNET *(Secret Internet Protocol Router Network)* e só é acedida pelas forças armadas americanas.

14 Autor do influente "*The Pentagon's New Map: War and Peace in The Twenty-First Century*", onde é desenvolvida a ideia que o mundo tem um centro que funciona, designado por *core* (especialmente o Oeste e os seus aliados) e outra região, que o autor designa por *gap*. Os principais conflitos estão situados ao longo da fronteira entre o *core* e o *gap.* Cf. http://www.thomaspmbarnett.com/published/pentagonsnewmap.htm [acedido a 15 de Abril de 2008].

15 *Military Operations Other Than War* (MOOTW), no léxico americano.

16 Cf. Network-Based Operations for the Swedish Defence Forces - An Assessment Methodology, disponível em http://www.rand.org/pubs/technical_reports/2005/RAND_TR119.pdf [acedido a 15 de Abril de 2008].

17 Disponível online em http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/ScienceandTechnologyPublications/NEC/Jsp777NetworkEnabledCapability.htm [acedido a 15 de Abril de 2008].

18 Tão abertas que inclui palestrantes de Singapura e observadores russos.

19 Cf. http://transnet.act.nato.int/WISE/Informatio/Conference [acedido a 15 de Abril de 2008].

20 Cf. http://www.jhuapl.edu/urw_symposium/ [acedido a 15 de Abril de 2008].