

O ATAQUE AO SÍTIO WEB DA AL-JAZEERA OU O ANUNCIADO SALTO DAS NOTÍCIAS DA RETAGUARDA PARA A LINHA DA FRENTE

Introdução

Procuramos neste artigo sustentar que a guerra do Iraque (19/3 – 1/5/2003) foi a ocasião em que, mercê de um conjunto de factores combinados, as notícias fizeram a sua entrada em cena no teatro da *guerra informática*.

As notícias assumiram desde sempre um papel fulcral na chamada guerra da informação, a guerra paralela à convencional que tem lugar no campo da comunicação e na qual as normas deontológicas do jornalismo são frequentemente preteridas em favor de um «imperativo» de «unidade nacional». A partir do momento em que passam a estar *online*, além de continuarem a sua cruzada no âmbito da guerra da informação, as notícias incorrem num terreno novo, onde se encontram investidas de um valor diferente a diversos níveis e de um valor particularmente importante a nível militar.

Efectivamente, trata-se de um terreno que conhece novas formas de destruição, próprias de um tempo histórico em que a informação e as suas tecnologias assumem uma importância crescente à medida que se tornam cada vez mais necessárias ao funcionamento dos sistemas em que repousa o dia-a-dia das nações e que se substituem a formas de energia enquanto principal motor do desenvolvimento económico; próprias, enfim, de um tempo histórico em que a vivência do espaço físico é progressivamente reconfigurada em função da *sociedade em rede* em que estaremos a ingressar (Castells, 2002, Van Dijk, 1999).

Neste contexto, as notícias *online*, como de resto muitos outros produtos culturais, passam a ser parte integrante do que os americanos

chamam *information warfare*, *cyberwarfare*, *infowars* ou *cyberwars*);¹ passam para a linha da frente da «guerra da Terceira Vaga», para usar o conceito de Alvin Toffler (1993).

Antes de analisarmos o ataque à Al-Jazeera, parece-nos importante, a título de advertência, referir algumas questões metodológicas a ter em atenção na abordagem científica da Internet, sob pena de se incorrer em caminhos epistemologicamente equívocos.

Nesta fase inicial de desenvolvimento da Internet, o seu estudo implica ter que lidar com uma série de lugares-comuns nascidos das ideias utopistas e libertárias que acompanharam a génese do novo medium e que foram entretanto contrariadas, por exemplo, por sociólogos que se dedicaram ao estudo mais aprofundado das interações *online*, na sua relação com as estruturas e dinâmicas *offline* em que se inserem. São os casos de James Slevin (2002), Steve Jones (1999) ou Manuel Castells (2002). Damos apenas dois exemplos desses lugares-comuns que, como outros, não devemos ignorar.

Desde logo, a ideia de que o ciberespaço constitui um «espaço social independente», cara aos estudiosos das «comunidades virtuais» (como Howard Rheingold) e veementemente defendida por entusiastas como John Barlow, que proclamou em 1996, na sequência da promulgação de uma lei ameaçando impor restrições à liberdade de publicação de conteúdos *online*, a então célebre «Declaração da Independência do Ciberespaço», um espaço igualitário, libertário, democrático, totalmente alheio aos poderes estabelecidos e à ordem social *offline*, uma «civilização da mente» imune às limitações do corpo. À medida que o uso da Internet se generaliza e a realidade *online* se confronta com as estruturas económicas, sociais e políticas pré-existentes, que também influencia, estas ideias perdem o seu sentido.

Outro exemplo importante são as visões nihilistas que vêm na nova era de comunicação *online* um «não-lugar» (Clifford Stoll), o «fim do espaço» ou mesmo o «fim do sentido da realidade» e dos sentimentos que nos prendem às outras pessoas e objectos materiais, uma «desrealização do mundo físico» baseada na intensificação da cor e no bombardeamento de imagens (Virilio, 1998). Como vários autores têm demonstrado, a Internet redimensiona as noções de espaço e de tempo, e todas as outras que delas dependem, como a de distância, de vizinhança, a temporalidade dos actos de comunicação, etc., mas está longe de as suprimir ou de lhes atribuir menos importância.

A retórica de substituição

São diversos e de difícil resolução os escolhos metodológicos da abordagem científica da Internet. O mais sério será talvez a dificuldade de produzir teoria, face à rápida mutação da realidade que advém do aparecimento quase contínuo (e também, por vezes, do desaparecimento) de dispositivos tecnológicos, como os *grupos de discussão*, os *blogs*, o *chat*, o *instant messaging*, que tanto são resultado de novas necessidades sociais como vêm introduzir continuamente alterações no sentido da interacção social e da transmissão cultural (Slevin, 2002). A validade das conclusões

¹ Optámos por traduzir estes termos, banalizados na língua inglesa, por «guerra informática». Se optássemos por «guerra da informação» – solução muitas vezes adoptada –, o âmbito do artigo encarrega-se-ia de introduzir uma possível confusão com o conceito homónimo, atrás referido, bem conhecido no jornalismo. A optar por «ciberguerra», estaríamos a cometer uma daquelas ousadias que pela nossa terra são liminarmente catalogadas como «erros de ortografia». Vamos então, pacificamente (passe a expressão), chamar-lhe «guerra informática».

está muito limitada no tempo e só modelos teóricos eles próprios profundamente dinâmicos poderão responder satisfatoriamente a estas problemáticas.

Mas estudar a Internet implica, também, ter consciência de que o seu aparecimento desencadeou, em muitas áreas da actividade humana, uma *retórica de substituição*, segundo a qual o novo meio iria fazer desaparecer uma série de práticas culturais e comunicacionais que existiam «antes». Esta retórica, praticada pelos visionários e os utopistas, por um lado não é exclusiva da Internet, tendo acompanhado o nascimento de todos os meios de telecomunicação, como o telefone, a rádio e a televisão e de outras inovações científicas (Hacker, Van Dijk, 2000; Fidler, 1997); por outro lado, as expectativas de substituição acabam quase sempre goradas por uma realidade em que os novos meios, em vez de os suprimem, complementam os antigos com novas vivências sociais.

A era da informática e a redefinição do conceito de guerra

Albert Einstein, nos anos 50, quando o computador dava os seus primeiros passos e quase ninguém no mundo sabia que raio de utilidade iria ter, disse que à bomba atómica, capaz de destruir a realidade, sucederia uma bomba igualmente terrível, a *bomba informática*, que seria capaz de destruir o *sentido da realidade*. À luz do que hoje começamos a saber acerca das possibilidades infinitas da informática no domínio da realidade virtual e da alienação causada por media tendencialmente menos *mass* e mais *self*, não podemos deixar de nos extasiar com a capacidade de antecipação de Einstein em relação a esse carácter infinito das possibilidades da informática.

A ideia de Einstein entusiasmou Paul Virilio ao ponto de o fazer escrever *A bomba informática* (1998), obra a nosso ver afectada pelo clima de euforia – social e económica – que marcou os dois ou três últimos anos do milénio em torno da Internet e portadora da retórica de substituição predominante nesse tempo; Virilio anuncia o fim não da História mas do espaço, o fim dos sentidos e dos sentimentos, o aparecimento de exércitos de clones geneticamente forjados, num futuro quase presente marcado pela indiferença e os mais extremos individualismo e hedonismo.

Está a guerra a mudar de palco, como dizem Alvin Toffler, com a sua noção de «guerra da Terceira Vaga», aprofundada em *War and anti-war* (1993), Virilio (1998) ou James Adams em *The next World War* (2001)? Estará a transformar-se naquilo a que Arquilla e Ronfeldt (1993) chamam «cyberwar», com exércitos convencionais, visando a destruição física, fortemente assistidos pelas tecnologias da informação e da comunicação? Ou tenderá a transformar-se naquilo a que os mesmos autores chamam «netwar», ou seja, a guerra informática a que se refere este artigo?

Ou devemos ter em relação esta matéria a atitude céptica de Graham Ingram, director de uma agência de segurança para a Internet, quando afirma acerca do *ciberterrorismo*: «A ideia do terrorismo é fazer algo que crie terror. Ora isso implica a realização da violência: há muito pouco terror nos bits e nos bytes»? E será que Ingram, ao usar a expressão «realização da violência», não pensou que o seu valor semântico sofre uma lenta mutação?

Numa crítica ao livro de James Adams publicada no Wall Street Journal, George Smith desmonta uma série de falsas ameaças e faits-divers da informática, dramatizados pelos teóricos da era da informação. Apelidando-os de «histórias de fantasmas da era da informação» e «contos a que muitos pontos foram acrescentados por quem os foi contando», para traduzir com base no nosso provérbio, Smith menospreza o seu real valor. Em muitos casos, como o «bug do ano 2000»

– que nos últimos anos do milénio assumia o valor de uma espécie apocalipse informático «que todos adorámos temer», como diriam os americanos – não podemos deixar de lhe dar razão.

No entanto, a Guerra do Iraque, como de resto também a I Guerra do Golfo, revelaram efectivamente possuir múltiplas características de «Terceira Vaga». As várias etapas da tática norte-americana revelam uma maximização do potencial da informação: primeiro, passar a scanner, durante meses, todo o território iraquiano, através dos voos de altitude dos AWACS e dos J-STARS (aviões Boeing equipados com sensores, radares e equipamento de teledeteção), de modo a construir um mapa minucioso e uma visibilidade total sobre ele; depois, programar as armas para todos os alvos seleccionados; iniciar as hostilidades destruindo toda a estrutura de comunicações inimiga com bombardeamentos selectivos, de modo a provocar uma cegueira total no exército iraquiano em relação aos invasores; só então destruir os alvos terrestres seleccionados e invadir (Virilio, 1991).

Os muitos que foram levados a crer, através deste impressionante «écran do deserto» descrito por Virilio e das imagens de visão nocturna que as televisões transmitiam em abundância, principalmente na I Guerra do Golfo, de bombardeamentos «inteligentes», que a guerra-carnificina tinha acabado para dar lugar a uma guerra «limpa» e «cirúrgica» enganaram-se. As duas guerras do Golfo saldaram-se em mais de 200 mil mortos, correspondentes a outros tantos corpos mutilados cujas imagens não invadiram as televisões.

A importância crescente da informação no desenrolar das guerras

O papel da informação no desfecho das guerras e das batalhas foi *sempre* decisivo (Arquilla e Ronfeldt, 1993; Toffler, 1993): não podemos afirmar de modo algum que foram as TIC que consagraram esse carácter. Não só a informação tática e estratégica acerca do inimigo, mas também a difundida a toda a população através dos mass-media – não houve guerra ou golpe militar da segunda metade do século XX em que o controlo das estações de televisão e de rádio, particularmente as públicas, não fossem objectivos militares prioritários.

Contudo, as duas guerras do Golfo mostram que, à medida que se desenvolvem as TIC e se constrói uma sociedade cada vez mais dependente delas, o papel da informação e da cibernética² no desfecho dos conflitos militares, em particular aqueles que envolvem nações desenvolvidas, é cada vez maior.

A partir do momento em que a informação e as suas tecnologias se tornam um bem essencial ao bom funcionamento dos sistemas não só militar como económico e social dos países, acções como a espionagem, o bloqueio, desactivação ou destruição lógica de sistemas informáticos passam, potencialmente, a caber na categoria de actos de guerra, na medida em que se tornem passíveis de causar danos avultados ao inimigo e de, em última instância, destituir regimes políticos.

A Internet reflecte e aumenta essa dependência e a sua chegada teve efeitos imediatos no campo político e militar: ela constituiu, desde o nascimento, um reduto de visibilidade social, de

² Arquilla e Ronfeldt sustentam que as quatro funções cibernéticas «C3I» (*command, control, communications and intelligence*) são decisivas no desfecho dos conflitos da «cyberwar» (1993).

comunicação e de organização, um verdadeiro «balão de oxigénio» para organizações militares como os zapatistas de Chiapas em 1996, a Falun Gong, na China, em 1999 (Castells, 2002), a que podemos acrescentar outros, como o grupo armado Tupac Amaru, do Perú. Povos politicamente subjugados, como os Curdos ou os Palestínianos, encontram na Internet uma forma de resisténcia³.

A relação filial entre guerra e Internet

A importância crescente da informação no desenrolar das guerras é visível, em primeiro lugar, na génese da Internet. É escusado descrever de novo (tal descrição já faz parte de um sem número de livros e artigos) o nascimento da Internet, o funcionamento engenhoso do seu protocolo de comunicação, o TCP/IP, etc. Mas é muito significativo o facto de a Internet ter sido criada pela instituição militar, durante a guerra fria, enquanto estrutura de comunicações descentralizada, qualidade que lhe permitiria manter a actividade em caso de um ataque nuclear que destruísse as principais cidades do país.

O método de divisão das mensagens em múltiplos *pacotes* que são enviados por múltiplos caminhos e que voltam para trás para seguir um caminho alternativo caso encontrem um servidor desactivado pelo meio, constitui um sistema tão perfeito que assegura hoje a comunicação instantânea e quase sem falhas de milhões de computadores. Mas este método é efectivamente uma tática militar: a sua virtude máxima está talvez em conseguir evitar ou «driblar» a guerra convencional (baseada na destruição física). A sua fraqueza está, como se viu no caso do ataque ao sítio web da Al-Jazeera, no próprio terreno a que pertence: o da guerra informática.

O potencial bélico das redes informáticas

O advento das redes informáticas introduziu um incremento exponencial no potencial de agressão e de conflito das acções hostis baseadas na informação, uma vez que, tecnicamente, a comunicação em rede coloca em contacto directo, instantâneo, permanente, fácil, adversários e inimigos que antes tinham praticamente vedado o acesso ao território inimigo.

A vulnerabilidade das redes nem precisava de ser tipificada por teóricos da comunicação como Van Dijk (1999) ou informáticos como Andreas Borchert, que desenvolve uma análise impressionante da *nossa* «guerra diária na Internet» (2002). Basta abrir um manual técnico de redes informáticas e observar o lugar de grande destaque que nele ocupam as questões da segurança. Ou ver o *e-mail*, diariamente, sem as devidas protecções (software anti-virus, *firewall*).

Se as outras telecomunicações já haviam viabilizado o contacto directo entre os inimigos, as redes informáticas – que desde os anos 80 trouxeram extraordinários ganhos de produtividade resultantes da partilha de recursos – dão-lhes agora a possibilidade de exercitar, de muitas, imaginativas e frutuosas maneiras, essa inimizade.

³ Recolhemos duas notícias de entre centenas relativas à guerra informática entre Israelitas e Palestínianos (Wired News, 8 e 20/11/2000).

Como, concretamente? Destruindo dispositivos informáticos que controlam sistemas vitais para a vida do país inimigo, como os de tipo financeiro, de transportes ou mesmo militar, apagando ou falseando informação de bases de dados, roubando-a, violando a sua confidencialidade, bloqueando comunicações, fechando serviços, lançando campanhas psicológicas sobre a população por *e-mail*, difundindo vírus informáticos altamente destrutivos, em acções simultâneas e em massa.

Como potenciais armas de guerra, as redes informáticas dispõem de uma terminologia rica em metáforas da guerra, que inclui conceitos como *firewall*, *zona desmilitarizada*, *vírus* ou *cavalos de tróia*.

A relevância das notícias *online*

O nosso objecto de análise, a ligação entre as notícias *online* e a guerra informática, levam-nos a procurar compreender o lugar e a importância daquelas no panorama do mercado de notícias e em particular durante a Guerra do Iraque. Essa importância condiciona o alcance dos ataques aos sítios web emissores de notícias e em particular a um sítio tão significativo como o da estação de televisão Al-Jazeera. A ser pouca, então a guerra informática envolvendo o campo das notícias e do jornalismo situa-se num terreno ainda mais marginal em relação à guerra convencional.

Poucos anos volvidos sobre o aparecimento da World Wide Web, em 1993, podemos afirmar que a generalidade da sociedade e das suas instituições socialmente reconhecidas adoptaram a Internet, como um novo meio, complementar dos tradicionais, de interacção com os seus membros ou utentes. O mesmo aconteceu com as empresas jornalísticas, com um sucesso que as audiências dos media *online* comprovam.

Mas além desta «migração» dos media tradicionais, a Internet viu nascer uma grande quantidade de entidades emissoras, muitas vezes produtoras, de notícias. Damos apenas os exemplos dos portais como o Yahoo, o Sapo, o Clix ou o IOL; ou de sítios web institucionais, que nas suas *homepages* apresentam as notícias mais recentes das instituições: universidades, empresas, clubes desportivos, partidos políticos e muitas outras associações.

A Internet comporta ainda outros dispositivos sociotécnicos (Bijker, citado por Jones, 1999) onde são produzidas e circulam notícias, como os *grupos de e-mail* temáticos ou institucionais ou as *notícias por e-mail* personalizadas, ou os (agora) famosos *blogs*, fenómeno generalizado em 2003 que tem menos a ver com notícias do que com outras formas de acção social, mas onde também encontramos produtos noticiosos.

Algumas características distinguem as notícias *online* das veiculadas por outros media, no sentido de uma comunicação menos baseada na alocação e mais na interacção.

São os casos da *variedade de escolha* – na Internet é muito mais fácil contactar com correntes de opinião diferentes das preponderantes do que nos outros media; da *personalização* – surgem inúmeras modalidades de personalização da informação, numa transferência da figura do *gatekeeper* para o leitor; da *interactividade e do hipertexto* – alguns sítios web disponibilizam o *e-mail* do jornalista, alguns possibilitam a resposta ou o comentário do leitor, alguns permitem o acesso imediato a um repositório de artigos desse jornalista; as notícias *online* introduzem muitas vezes *links* ao longo da narrativa, facultando ao leitor um percurso de leitura que ele próprio produz

(Bastos, 2000); da *flexibilidade espacial e temporal* – elemento que distingue decisivamente as notícias *online* das dos jornais (limitadas espacialmente) e da televisão (limitadas no tempo segundo um alinhamento único) (Bastos, 2000).

Mas a característica que popularizou, mais do que qualquer outra, as notícias *online*, é a actualização permanente a que podem estar sujeitas. Nos sítios web dos media tradicionais sabemos que vamos encontrar os acontecimentos mais importantes que ocorreram no mundo nas últimas horas ou minutos.

Seja qual for o uso que se faz ou não de todo este potencial – questão central na investigação das notícias *online* – a relevância destas na formação da opinião pública é hoje indiscutível, num mercado potencial de 720 milhões de pessoas (ver www.InternetWorldStats.com), correspondendo a 11% da população mundial, percentagem que sobe muito nas regiões do mundo mais influentes (63% na América do Norte, 28% em toda a Europa, por exemplo) e nos grupos sociais mais influentes em cada país.

Primazia da televisão e das versões online dos grandes media

Um estudo da Pew Internet & American Life Project (Lee, Fox, Fallows, 2003) acerca do modo como os Norte-americanos usaram a Internet para se esclarecerem e trocarem ideias sobre a Guerra do Iraque revela que a televisão permanece largamente preponderante como principal fonte de notícias: 89% de todos os Norte-americanos (não apenas aqueles com acesso à Internet, o alvo principal do estudo) afirmaram ter sido a televisão a sua principal fonte de informação sobre a guerra e tanto os jornais como a rádio permaneciam como fonte mais usada do que a Internet.

No entanto, segundo este estudo, a quantidade de Norte-americanos com acesso à Internet a considerar as notícias *online* como primeira fonte de informação aumentou de 3% para 17% no ano e meio que passou entre o 11 de Setembro de 2001 e a Guerra do Iraque, valor que chegou aos 26% nos dias anteriores ao início da guerra.

Segundo o estudo anteriormente referido, os principais motivos de recurso à World Wide Web pelos Norte-americanos durante a guerra estiveram relacionados com notícias: procurar notícias sobre a guerra (44%), obter reacções dos mercados financeiros à guerra (23%) e obter informação acerca do Iraque enquanto país (15%) foram os motivos mais evocados.

Outro facto relevante deve ser destacado do estudo precedente: os sítios web dos principais jornais e televisões quase monopolizam a audiência das notícias *online* (tabela 1). Este dado contraria brutalmente algumas visões alarmistas dos primórdios da Internet: Koch (1996, cit. por Bastos, 2000) argumentava que os jornalistas deixariam de ser necessários, porque passaríamos a ter um acesso directo às fontes; Shaffer (1998, cit. por Bastos, 2000) assegurava que «qualquer pessoa ligada à Internet e com uma ideia original poderia chegar a uma audiência mundial», para citar duas de entre as muitas promessas que a euforia da Internet produziu, com alguma ajuda da cultura libertária que esteve na sua origem.

Mais uma vez os factos contrariaram a retórica de substituição: a Internet não só não ameaçou a profissão de jornalista como tudo leva a crer que a reforçou. A tabela 1 mostra como no campo

das notícias *online*, e com toda a proliferação de sítios web produtores de notícias, os jornalistas não deixam os seus créditos por mãos alheias:

Tabela 1
Sítios web acedidos pelos Norte-americanos para obter informação sobre a guerra

| <i>Sítios web</i> | <i>Percent. de utilizadores da Internet que visitaram</i> |
|---|---|
| Sítios web de estações de TV americanas | 32% |
| Sítios web de jornais americanos | 29% |
| Sítios web do governo americano | 15% |
| Sítios web de notícias estrangeiros | 10% |
| Sítios web de notícias alternativas | 8% |
| Sítios web de grupos anti-guerra | 6% |
| Sítios web de grupos pró-guerra | 5% |
| Web logs (blogs) | 4% |

Fonte: *Pew Internet & American Life Project Iraq war survey*, 20 a 25 de Março de 2003. N.º dos utilizadores da Internet = 999. Margem de erro: $\pm 3\%$.

Estes dados, relativos à população dos EUA, sugerem que o sítio web da Al-Jazeera, enquanto mais prestigiada estação de televisão do Mundo Árabe, terá tido uma grande importância durante a Guerra do Iraque.⁴

Comunicação multicanal

Dez anos depois do boom da World Wide Web, podemos afirmar com propriedade que a retórica de substituição relacionada com a Internet tem pouca validade no campo dos media. Diversos estudos (Finberg, Stone, Lynch, 2002; Vector21, 2003; Lee, Fox, Fallows, 2003) demonstram que vivemos num mundo em que múltiplos canais (*e-mail*, *WWW*, *chat*, televisão, jornais, rádio, telefone, etc.) se complementam, se publicitam mutuamente e são socialmente preservados, pelas suas valências insubstituíveis. Mais uma vez, a novidade tecnológica veio alargar o leque e complementar, não substituir.

Cada *medium* existe em espaços sociais próprios e possui um valor social e cultural em grande medida exclusivo (Castells, 2002). A Internet está associada a determinados espaços físicos e sociais, determinados contextos *offline*, ao passo que a rádio, os jornais, a televisão, o telefone, pelas suas características físicas, técnicas e culturais, estão associados a outros.

Notícias *online* na linha da frente

Com «linha da frente» não estamos a recorrer à metáfora tantas vezes usada para proclamar a importância ou primazia dum objecto. Referimo-nos mesmo aos lugares do teatro de guerra em que

⁴ A estação afirma que o seu sítio web recebeu 161 milhões de visitas só em 2002, das quais 54% originárias do Médio Oriente e 39% da Europa e América do Norte (<http://www.aljazeera.net/e-marketing-eng/2002/5/5-5-1.htm>).

os inimigos se enfrentam cara a cara e onde decorrem os combates. James Adams (2001) dizia que, agora, «a linha da frente está em toda a parte». No contexto da guerra informática, compreende-se que os sítios web mais importantes de notícias *online* constituam um alvo privilegiado, pela sua vulnerabilidade.

Para bloquear, por exemplo, uma emissão de televisão da RTP é preciso uma intervenção militar convencional. Todos recordamos, nem que seja pelos documentários, a célebre emissão de 25 de Novembro de 1975 em que o ex-capitão Duran Clemente foi retirado do ar. No caso da Internet, como se viu no caso do ataque à Al-Jazeera, o mesmo tipo de bloqueio pode ser levado a cabo por qualquer pessoa que leia um ou dois capítulos dum livro de *hacking* e que aceda à Internet algures no mundo.

Acresce, a esta vulnerabilidade, que as infraestruturas de comunicação baseadas na Internet, hoje, dependem de uma combinação de serviços cuja localização física obedece a uma lógica efectivamente global. Tomemos uma qualquer instituição, de um país A. A empresa que registou o domínio do seu sítio web pode estar no país B; a empresa que presta o serviço de *DNS* pode ser do país C e a empresa onde está alojado o sítio web propriamente dito estar no país D. O bloqueio de *qualquer um* destes serviços é suficiente para retirar a visibilidade do sítio web em questão na Internet.

Guerra do Iraque na Internet

A expressão «Guerra do Iraque na Internet» é susceptível de uma multiplicidade de entendimentos, que se prendem quer com a ambiguidade da expressão «guerra na Internet» (guerra informática via Internet ou reflexos da guerra nos dispositivos sociais da Internet?), quer com o carácter multidisciplinar da própria ideia de Internet. De facto, existem tantos conceitos de Internet como ciências sociais que a elegem como objecto de estudo. Diferenças relativas aos centros de interesse, dispositivos teóricos e conceptuais e problemáticas conduzem ao desenvolvimento de conceitos de Internet mais centrados na sua vertente de acção social (a sociologia), de sistema económico (a economia), de dispositivo de transmissão cultural (a antropologia) ou nos novos desafios que traz à justiça (o direito). Juntamente com a história, a linguística e a psicologia, estas ciências coincidem no carácter inovador e dinâmico do novo meio, na singularidade das suas vivências, mas também na profunda interdependência entre as realidades *online* e os contextos *offline* em que elas se integram (Jones 1999, Slevin 2002), produzindo-se assim realidades duais.

No caso da guerra informática, que encontra na Internet, pela sua vulnerabilidade, um campo de batalha apetecível, o conflito que abordamos trouxe algumas novidades, que apresentamos como forma de contextualizar o ataque à Al-Jazeera.

Aumento exponencial dos ataques de hackers

Vários sítios web, que monitorizam diariamente a actividade de *hacking* na Internet (casos da Keynote Systems, o Internet Storm Center ou empresas de segurança como a F-Secure ou a iDefense), registaram, nas semanas anteriores ao início da guerra, um fortíssimo aumento dos

ataques a nível mundial, muito por força de sítios web relativos às temáticas da guerra. Os *defacings* (sítios web cujo tráfego é desviado para outros sítios onde aparecem mensagens satíricas ou contestatárias), relacionados com a guerra aumentaram em flecha, tendo afectado milhares de sítios, como por exemplo o de Tony Blair (www.number-10.gov.uk), quatro dias depois do início da guerra.

Segundo a iDefense, uma novidade introduzida nos *defacings* durante a guerra do Iraque, praticado centenas de vezes, consistiu em mostrar as *homepages* dos sítios com grafittis sobrepostos em que se liam frases na maior parte dos casos anti-guerra (BBC Online, 21/3/2003).

Numerosos sítios web de entidades militares norte-americanas estiveram sob intenso ataque de *hackers* pacifistas ou mesmo, segundo a iDefense, de grupos de *hackers* islâmicos organizados.⁵

O governo de Saddam Hussein também dispunha de um sítio web oficial, o Uruklink.net, que foi atacado por *hackers* através dos seus servidores de DNS e sete dias depois do início da guerra já não estava disponível, sendo os seus visitantes redireccionados para uma página onde se lia: «Hacked, tracked, and NOW owned by the USA.» (Internet Security News, 26/3/2003)

Guerra psicológica por e-mail

As tecnologias de comunicação desenvolvidas ao longo do século XX permitiram desencadear a chamada «guerra psicológica», ou seja, a difusão de mensagens de desencorajamento, de intimidação tanto de civis como das tropas inimigas, de apelos à deserção e à rendição, a divulgação de instruções sobre como levar a cabo a deserção. Assim, nas guerras do século XX, esta «guerra psicológica» baseou-se em técnicas como a largada de milhares de panfletos sobre território inimigo, a rádio ou, na frente de batalha, os altifalantes. Na Guerra do Iraque, um novo meio de guerra psicológica foi usado pelos militares norte-americanos: o *e-mail*.

Num país em que toda ou quase toda a população use a Internet, um meio como a largada de panfletos por avião sobre território inimigo torna-se totalmente obsoleto: a Internet, com a massificação da capacidade de emissão e difusão que trouxe, permite levar mensagens de *e-mail* a uma população inteira e a um exército inteiro.

Segundo artigo da CNN.com (12/1/2003), agências ligadas ao Departamento de Defesa tinham iniciado, em Janeiro de 2003, uma campanha por *e-mail* junto de um conjunto de líderes iraquianos de incentivo à revolta contra Saddam Hussein. O artigo baseia-se numa fonte militar que afirmou tratar-se da primeira vez que os Estados Unidos usavam o novo meio de guerra psicológica. Segundo a fonte, a mensagem de *e-mail* procurava convencer o destinatário de que o Iraque não tinha qualquer possibilidade de sucesso numa guerra contra «os Estados Unidos e os seus aliados». Incluía também um conjunto de informações e endereços de *e-mail* das Nações Unidas, com o intuito de facilitar o trabalho aos potenciais desertores. A fonte refere ainda que o remetente destas mensagens foi «disfarçado», de modo a que os destinatários não percebessem que tinham origem no Pentágono.

⁵ Uma notícia da BBC Online (19/6/2002) identifica diversos grupos de hackers islâmicos, particularmente atraídos por servidores americanos, israelitas e indianos, que estariam a unir esforços e competências: o USG (Unix Security Guards), o WFD (World's Fantabulous Defacers) e o AIC (Anti-India Crew).

Esta campanha de *e-mail* terá sido curta e limitada no seu alcance. Seguiu-se-lhe a continuação da guerra psicológica através de emissões de rádio a partir de aviões que sobrevoavam o território iraquiano e de bases militares em terra.

Se parte considerável da população do Iraque tivesse acesso à Internet, o que não era o caso, se a guerra opusesse dois países «wired» (para usar o termo de gíria anglo-saxónico que adjectiva a conectividade à Internet), então seria de prever uma actividade frenética deste novo tipo de guerra psicológica.

O ataque ao sítio web da Al-Jazeera

A guerra informática atravessou o campo do jornalismo por via do ataque à única entidade do campo das TIC simbolicamente associada ao Mundo Árabe e apostada em rivalizar com as instituições ocidentais no âmbito global da sua visibilidade social, porque dotada dos requisitos tecnológicos, financeiros, éticos e simbólicos adequados: o sítio web da estação de televisão Al-Jazeera.

Algumas características estruturais desta estação conferiam-lhe um estatuto ameaçador para a hegemonia dos grandes media ocidentais (como a BBC ou a CNN) face à opinião pública internacional e aos próprios públicos dos países ocidentais. A ameaça é tanto maior quanto, segundo Pierre Bourdieu, é o próprio poder político que está em jogo quando tem lugar uma luta pela imposição de determinada visão do mundo e das suas categorias de percepção do real. Ora a Al-Jazeera dispunha de um conjunto de meios que lhe permitiam desafiar a visão do mundo dominante, nomeadamente acerca da Guerra do Iraque:

- apoio político e meios financeiros e técnicos suficientes para concorrer com os mass-media de âmbito global;
- pertença ao «Mundo Muçulmano», enquanto realidade civilizacional divergente da ocidental e enquanto campo simbólico, facilmente associável, perante um vasto público menos informado, ao regime de Saddam Hussein;
- recurso a normas deontológicas, práticas e padrões de qualidade jornalísticos comparáveis às das grandes estações de televisão mundiais;
- uma presença forte e ganhadora num campo social associado ao progresso e à modernidade: a Internet.

Este dispositivo constituía e constitui por si só uma afronta para algumas pretensões de hegemonia ideológica no Ocidente. Mas naquele fim de Março de 2003, que coincidiu com o início da guerra, a Al-Jazeera serviu de bandeja duas novas afrontas:

Por um lado, a 24 de Março, pôs no ar uma versão improvisada de língua inglesa do seu sítio web. Ao usurpar a arma simbólica por excelência, a língua inglesa, numa tentativa deliberada de disputa do mercado mundial das ideias e da visão, senão mesmo de conquista do universo (hipótese plausível se considerarmos o facto de ser a língua inglesa a língua universal), o <http://english.aljazeera.net> passava das marcas e tinha que ser posto na ordem.

Por outro, apresentou imagens de corpos de soldados norte-americanos mortos em combate e de soldados norte-americanos prisioneiros acorrentados pelos pés. Esta última imagem, embora

familiar junto da opinião pública norte-americana por via das reportagens acerca dos seus próprios estabelecimentos prisionais, não se enquadra nos padrões éticos do jornalismo. O vídeo que incluía essas imagens foi publicado no sítio web da Al-Jazeera em Árabe.

Esta atitude da Al-Jazeera provocou reacções de ira das autoridades norte-americanas; Colin Powell, na ocasião, completou a acusação afirmando que a estação estava a exagerar os pequenos sucessos do exército iraquiano nos primeiros dias de guerra (BBC Online, 27/3/2003). E levou a um ataque impiedoso, desencadeado por *hackers* durante mais de uma semana, a partir de 23 de Março.

A «declaração de guerra informática», para cujo perigo Virilio nos advertia em 1998, aí estava, à margem dos poderes político e militar instituídos, mas não tão à margem de poderes políticos, militares e simbólicos não instituídos e porventura emergentes na nossa sociedade em rede.

Descrição técnica

Como acabámos de ver, o ataque à Al-Jazeera não constituiu um acto isolado: podemos enquadrá-lo no enorme incremento da actividade de *hacking* registado nas semanas anteriores e subsequentes ao início da guerra, a 19 de Março. No entanto, como acabámos também de assinalar, reveste-se de uma importância superlativa. Uma abordagem técnica suscita, como veremos, novas questões.

A descrição técnica do ataque baseia-se em várias fontes, devidamente identificadas, mas principalmente nos relatórios da Keynote Systems, uma empresa sediada na Califórnia que monitorizou hora a hora – através de *browsers* automatizados que, a partir de cerca de 50 cidades espalhadas pelo mundo, efectuem pedidos de página e de ligações *streaming* – o desempenho de dezenas de sítios web importantes no contexto da guerra.

O ataque ao sítio da Al-Jazeera começou no dia 23/3 pelas 3:00 (EST) e revestiu-se de duas formas diferentes.

Numa primeira fase, os *hackers* provocaram o que tecnicamente se chama um *ataque DDOS* (Distributed Denial Of Service). Segundo o Keynote Systems Report de 26 de Março, os servidores de DNS⁶ em que o sítio web da Al-Jazeera se baseava para converter os nomes www.aljazeera.net e english.aljazeera.net nos respectivos endereços IP deixaram de estar acessíveis. Mesmo quem tentasse aceder directamente, pelo endereço IP numérico, aos servidores web da Al-Jazeera, encontrava-os inacessíveis. O que os *hackers* fizeram foi sobrecarregar o sítio web e os servidores de *e-mail* da estação com milhares de mensagens e pedidos, de modo a bloquear o servidor por sobrecarga ou incapacidade de resposta. Este «bombardeamento» de mensagens foi automaticamente accionado por software e de forma constante. Na prática, os DDOS fazem com que qualquer utilizador que aceda ao sítio atacado receba a mensagem de que não encontra o servidor ou que ele se encontra desactivado.

⁶ DNS significa «Domain Name System» e é um serviço que permite converter endereços nominais da Internet (por exemplo, www.clix.pt) em endereços IP – cada computador ligado à Internet possui um endereço IP, um conjunto de quatro bytes único e irrepetível a nível mundial (por exemplo, 156.12.134.78). O processo é o seguinte: um utilizador tenta abrir uma determinada página no seu browser (por exemplo, <http://www.aljazeera.net>); esse pedido não vai directamente ao servidor que aloja o sítio web da Al-Jazeera, mas antes a um servidor DNS onde está registado o endereço IP numérico, universal, a que corresponde esse nome; o servidor DNS converte o nome no endereço IP numérico e efectua então o pedido de página ao servidor web, que responde enviando-a ao cliente.

«Let Freedom Ring...»

Uma outra técnica, também recorrente na Internet, foi usada no ataque: o *defacing* ou *DNS poisoning*. A técnica é rudimentar: no servidor de DNS usado pela Al-Jazeera, troca-se o endereço IP para onde devem ser direccionados os pedidos do nome www.aljazeera.net. Os hackers desviaram assim o tráfego para uma página onde se exibia a bandeira dos EUA, a frase «Let Freedom Ring» e a assinatura «Freedom Cyber Force Militia».

Esta página estava alojada numa empresa de Salt Lake City (EUA), a NetWorld Connections, especializada no alojamento de sítios web, que negou qualquer envolvimento no ataque – de facto, estas empresas não podem controlar os milhares de páginas que alojam. O desvio não se dirigiu apenas para esta página mas também para outros sítios que nada tinham a ver com a guerra.

Tabela 2

Disponibilidade do sítio web da Al-Jazeera (Língua Árabe)

| Dias | Hora do dia (EST) | | |
|------|-------------------|------------|-------------|
| | 0-8 horas | 8-16 horas | 16-24 horas |
| 21/3 | 100% | 100% | 100% |
| 22/3 | 100% | 100% | 100% |
| 23/3 | 100% | 46% | 46% |
| 24/3 | 33% | 66% | 71% |
| 25/3 | 20% | 18% | 10% |
| 26/3 | 0% | 0% | 0% |
| 27/3 | 0% | 0% | 0% |
| 28/3 | 7% | 44% | 39% |
| 29/3 | 83% | 79% | 24% |
| 30/3 | 93% | 90% | 80% |
| 31/3 | 90% | 55% | 78% |
| 1/4 | 59% | 98% | |

Fonte: Tabela construída com base em dados da Keynote Systems, recolhidos hora a hora.

Estes dados mostram a importância que a difusão das imagens de prisioneiros norte-americanos – e a sua disponibilização *online* – terá tido na decisão dos *hackers*. Efectivamente, a guerra começou no dia 19/3, e nos três dias seguintes a disponibilidade (o inverso da taxa de erro) do sítio web da Al-Jazeera manteve-se total. A difusão de imagens de soldados americanos prisioneiros e abatidos, no dia 23/3 (ver tabela 2), a par de notícias de feroz resistência por parte das forças iraquianas, levaram aparentemente a uma « reacção » por parte dos *hackers*, como contributo voluntarioso para o esforço de guerra americano, no campo da comunicação.

Os responsáveis da estação retiraram os seus sítios web e serviço de DNS dos servidores onde se encontravam, nos Estados Unidos, para servidores europeus e conseguiram restabelecer o serviço a partir de 1 de Abril.

Não se pode de modo algum sustentar que este acto de guerra informática não teve consequências nem impacto ao nível das representações sociais acerca da guerra. Por um lado, o silêncio forçado de um sítio web tão influente durante vários dias, impediu os milhões de actos de comunicação que normalmente se teriam estabelecido entre a Al-Jazeera Online e a sua audiência por todo o mundo e a respectiva transmissão de uma determinada visão dos acontecimentos.

Por outro lado, o acto em si, pelo seu peso simbólico, suscitou reacções generalizadas e poderá ter contribuído para a reestruturação das representações acerca do conflito, o que importaria, evidentemente, testar através de estudos empíricos. Ele foi formalmente condenado por todas as autoridades, amaldiçoado pelos movimentos anti-guerra e aclamado pelos movimentos pró-guerra. E permite aos cientistas o levantamento de questões interessantes acerca da natureza das relações de poder, das fontes de legitimidade e dos conflitos militares na sociedade em rede.

As autoridades americanas opuseram-se publicamente, e ao que leva a crer nas acções concretas, ao chamado «*patriotic hacking*», ou seja, o ataque por parte de civis a sítios web ou outros servidores iraquianos de Internet.

Em Fevereiro de 2003, o FBI, através do National Infrastructure Protection Center (NIPC), advertiu os Americanos de que o «*patriotic hacking*» seria considerado crime e o próprio FBI ripostaria a tais actos (BBC Online, 14/2/2003). Na mesma linha, os autores do ataque à Al-Jazeera viriam a ser processados criminalmente pelas autoridades norte-americanas e John William Racine II, um *web-designer* da localidade de Norco, na Califórnia, viria mesmo a assumir-se como culpado em Junho de 2003.

Conclusões

Não tendo constituído um acto bélico no sentido estrito do termo, uma vez que os seus protagonistas (o grupo «Freedom Militia» e a estação de TV Al-Jazeera) não faziam parte dos exércitos em confronto, o ataque assume um significado profundo no contexto de uma sociedade contemporânea em evolução acelerada, crescentemente interdependente das TIC.

As notícias *online*, pelo seu carácter multimedia, interactivo e universal, viram consagrada a sua enorme relevância em tempo de guerra: elas trouxeram a visibilidade universal sobre os horrores da guerra, com imagens e relatos dilacerantes publicados não apenas em *blogs* de pessoas directamente envolvidas no terreno de batalha, mas também em sítios web de agências noticiosas, relativamente dispensados do trabalho de *gatekeeping* que, nos media tradicionais em tempo de guerra, evita imagens desmoralizadoras e desmobilizadoras e em sítios de informação «alternativa»⁷. O ataque ao sítio web da Al-Jazeera deve ser interpretado à luz desta nova relevância.

As conclusões que se poderão tirar deste episódio pioneiro são múltiplas e terão origem em todas as áreas do saber no seio das quais ele assuma um valor teórico importante, o que a nosso ver inclui todas as ciências sociais e algumas ciências ditas exactas. Neste trabalho, cingir-nos-emos ao âmbito da guerra informática e à relação desta com o sistema político.

O «regresso» do espaço físico

O episódio da Al-Jazeera, a par de outros da guerra do Iraque, como a desactivação da Uruklink.net (o sítio oficial do governo iraquiano), mostra que a ideia de Internet como um espaço «sem fronteiras» ou um «não-lugar» cai pela base a partir do momento em que é declarada uma

⁷ A expressão «informação alternativa» não deixa de encerrar uma ironia gritante, quando usada tão recorrentemente por sociedades democráticas.

guerra. Efectivamente, se num contexto legal de economia de mercado a localização física das infraestruturas que suportam a Internet – nomeadamente os ISP (Internet Service Providers), os DNS (Domain Name Servers), os web hosts – é irrelevante, num contexto de conflito internacional deixa imediatamente de o ser.

No estado actual da tecnologia, um Estado que participe numa guerra tem meios para, dentro das suas fronteiras físicas e das dos países seus aliados, bloquear ou sabotar serviços de Internet que considere servirem, directa ou indirectamente, o inimigo.

Acresce, no caso em análise, que à hegemonia política dos EUA a nível mundial corresponde uma hegemonia talvez ainda mais acentuada no que se refere à prestação de serviços globais de Internet, incluindo as vendas online, os motores de pesquisa e os serviços básicos referidos no parágrafo anterior.

Afinal, a Internet é essa entidade livre, impoluta, descentralizada, ou a filiação nacional, ideológica, «civilizacional» das instituições que a controlam a nível técnico é decisiva em casos de guerra? Os episódios verificados na Guerra do Iraque vieram, sem surpresa, confirmar a segunda hipótese.

O ataque à Al-Jazeera e a crise do Estado moderno

A atitude das autoridades dos EUA de proibir e penalizar o chamado «*patriotic hacking*» não é apenas eticamente razoável: reflecte também a preocupação de manter todas as actividades militares sob estrito controlo estatal. Estado que abraze mão do monopólio do uso da violência física legítima (segundo a fórmula de Max Weber) abriria também um precedente gravíssimo para a sua futura integridade, numa sociedade em que os meios técnicos para fazer a guerra informática estão ao alcance de qualquer cidadão comum.

O ataque à Al-Jazeera, o facto de ter tido como protagonistas entidades «não políticas» e este possível questionamento do monopólio estatal não devem ser isolados das recentes tendências de descentralização política: nas últimas décadas, o Estado central perdeu poder para as autarquias locais, para as grandes empresas multinacionais, para organizações internacionais como a União Europeia ou o Banco Mundial, para as próprias burocracia e infocracia que desenvolveu no seu interior e que entretanto se autonomizaram.

Não nos esqueçamos que à crise da participação das populações ocidentais nos seus foruns políticos tradicionais da democracia representativa – as eleições, o Parlamento, os partidos políticos –, visível no crescimento regular da abstenção eleitoral e nas representações sociais negativas acerca dos políticos, corresponde um movimento que parece ser intenso de participação em matérias políticas através da Internet, em inúmeros foruns, petições, sondagens, discussões, manifestações, grupos de *e-mail* de informação política.

São formas de intervenção não institucionalizadas e por isso com fracos reflexos na vida política institucional, mas não é de excluir que haja uma verdadeira *vontade de intervenção política* em todos estes foruns *online* que, a tornar-se pública e socialmente (re)conhecida, pode obrigar o sistema político a mudanças estruturais profundas.

Uma nova fonte de legitimidade?

Em jeito de desafio, podemos terminar lendo nestes novos foruns (em que os desejos ainda não ascenderam ao estatuto de exigências políticas) e, no caso em análise, na simpatia com que o ataque foi recebido junto de largas camadas da população norte-americana, não só um sinal da crise do Estado moderno e da sua prerrogativa de monopólio da violência física legítima (pelo menos no campo da guerra informática), mas também o embrião de uma nova fonte de legitimidade, característica do tipo de organização social mais descentralizada e dependente das TIC a que diversos autores chamam sociedade em rede e que Weber não chegou a conhecer. Uma fonte de legitimidade reforçada pela erosão, nas sociedades mais desenvolvidas, das tipificadas por aquele autor e características das formas de dominação tradicional, carismática e racional-legal.

Bibliografia

- Adams, James (2001), *The Next World War*, New York, Simon and Schuster.
- Arquilla, John, Ronfeldt, David (1993), «Cyberwar is coming!», *Journal of Comparative Strategy*, Volume 12, n.º 2, Bristol, Taylor & Francis.
- Bastos, Hélder (2000), *Jornalismo Electrónico, Internet e Reconfiguração de Práticas nas Redacções*, Coimbra, MinervaCoimbra.
- Borchert, Andreas F. (2002), *The daily war on the Internet*, Ulm University.
- Castells, Manuel (2002), *A sociedade em rede, volume 1, A Era da Informação: economia, sociedade e cultura*, Lisboa, FCG.
- Fidler, Roger (1997), *Mediamorphosis: Understanding New Media: Journalism and Communications for a New Century*, Thousand Oaks, Pine Forge Press.
- Finberg, Howard; Stone, Martha; Lynch, Diane (2002), *Digital Journalism Credibility Study*, Online News Association.
- Geller, Daniel S., Singer, J. David (1998), *Nations at War: A Scientific Study of International Conflict*, Cambridge University Press.
- Hacker, Kenneth, Van Dijk, Jan (2000), *Digital democracy*, Sage.
- Hafner, Katie, Markoff, John (1992), *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, New York, Simon and Schuster.
- Jones, Steve (org.) (1999), *Doing Internet Research*, Sage.
- Keegan, John (1996), *Histoire de la Guerre: Du néolithique à la guerre du Golfe*, Ed. Dagorno.
- Kura, Alexandra, John V. Blane (2001), *Cyberwarfare: Terror at a Click*, Ed. Novinka Books.
- McLuhan, M., Powers, B. R. (1986), *The global village: Transformations in the world life and media in the 21st century*, New York, Oxford University Press.
- Lee, Rainie; Fox, Susannah; Fallows, Deborah (2003), *The Internet And The Iraq War: How Online Americans Have Used The Internet To Learn War News, Understand Events, And Promote Their Views*, Pew Internet & American Life Project.
- Rheingold, Howard (1991), *Virtual Reality*, New York, Summit Books.
- Rheingold, Howard (1993), *The Virtual Community: Homesteading on the Electronic Frontier*, Reading, MA, Addison-Wesley.
- Slevin, James (2002), *Internet e sociedade*, Lisboa, Temas e debates.
- Toffler, Alvin (1984), *A Terceira Vaga*, Lisboa, Livros do Brasil.
- Toffler, Alvin, Toffler, Heidi (1993), *War and Anti-War*, New York, Warner Books.
- Van Dijk, Jan (1999), *The Network Society, Social Aspects of New Media*, London, Sage.
- Virilio, Paul (1991), *L'Ecran du désert – chroniques de guerre*, Paris, Editions Galilée.
- Virilio, Paul (1998), *La bombe informatique*, Paris, Editions Galilée.
- Wellman, Barry (org.) (1999), *Networks in the Global Village*, Boulder, CO, Westview Press.

Outras fontes

(ordenação cronológica)

Wired News (8/11/2000), *Hacker War Rages in Holy Land*

Wired News (20/11/2000), *Israeli-Arab Warfare, Web-Style*

BBC Online (19/6/2002), *Pro-Islamic hackers join forces*

CNN.com (12/1/2003), *U.S. e-mail attack targets key Iraqis*

BBC Online (14/2/2003), *US hackers told to leave Iraq alone*

BBC Online (21/3/2003), *Anti-war hackers target websites*

Keynote Systems (24/3/2003), *Keynote Systems Reports: Iraq War*

Wired News (25/3/2003), *English Al-Jazeera Website Hacked*

Keynote Systems (26/3/2003), *Keynote Systems Reports: Iraq War*

ABC Online (26/3/2003), *Headaches as Al Jazeera launches English website*

Internet Security News (26/3/2003), *Iraq's Uruklink «Owned» By Hackers*

Reuters (26/3/2003), *Al Jazeera hacked after showing US POWs*

Keynote Systems (28/3/2003), *Keynote Systems Reports: Iraq War*

Keynote Systems (1/4/2003), *Keynote Systems Reports: Iraq War*

Debra W. Yang, United States Attorney, Central District of California (12/6/2003), Press-release *Southern California Man*

Who Hijacked Al Jazeera Website Agrees to Plead Guilty to Federal Charges (ver <http://www.usdoj.gov/criminal/cybercrime/racinePlea.htm>)

CyberJournalist.net (4/9/2003), *Al-Jazeera Launches English Site*