The International Communication Gazette
COPYRIGHT © SAGE PUBLICATIONS 2008
LOS ANGELES, LONDON, NEW DELHI, SINGAPORE AND WASHINGTON DC 1748-0485 VOL. 70(6): 419–441
DOI: 10.1177/1748048508096141
http://gaz.sagepub.com

INFORMATION OPERATIONS 'BLOWBACK'

Communication, Propaganda and Surveillance in the Global War on Terrorism

Dwayne Winseck

Abstract / The US's adoption of the broad doctrine of 'information operations' (IO) in 2003 put information and media strategies on a par with conventional means of military power and made them pivotal to achieving 'full-spectrum dominance'. This article focuses on the role of IO in shaping the global media ecology and in the battle for hearts and minds, especially in Muslim-majority countries. However, the author also argues that the impact of such operations at home may be their most important legacy. IO 'blowback' occurs as surveillance and propaganda campaigns targeting foreign audiences spill back into the US because of the nature of the global media and information flows. The all-encompassing doctrine also blurs the boundaries between 'normal' media spin and public affairs, on the one hand, and propaganda and covert media operations, on the other. The convergence of commercial media and the military and government in such operations is also yielding what some call the military–information–media–entertainment (MIME) complex. Lastly, the US military's heavy reliance on the Internet and other public communication networks means that cyberspace is being retooled to meet national security, surveillance, propaganda and cyberwarfare needs.

Keywords / information warfare / military–information–media–entertainment (MIME) complex / networks / propaganda / surveillance

Introduction

The beginning of the global war on terrorism (GWOT) immediately after the 11 September 2001 attacks on the World Trade Center and the Pentagon launched the US onto a path of conflict that knows no bounds in time or territory. Just as the National Security Act of 1947 put the US on a permanent wartime footing for the Cold War, the country has again been put on such a path through three initiatives: the Authorization of the Use of Military Force (AUMF) granted by Congress to the Bush administration three days after 11 September, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (commonly known as the Patriot Act) and the adoption of information operations (IO) as a new and fundamental doctrine of US military and foreign policy (DBS, 2004: 33).

IO encompasses the surveillance, control and destruction of communications networks, psychological warfare and propaganda, and more routine methods of

public affairs and media relations. The pivotal role of such operations in the war on terrorism has sparked a revival of the study of propaganda (Brown, 2003; Knightly, 2004; Snow and Taylor, 2006). Such studies are valuable, but here I want to focus on how IO changes the architecture of cyberspace (Lessig, 2001). Civilian communication networks, including the Internet, are now fully intertwined with military communications, a situation that has led to networks being retooled for surveillance, control and information warfare. These pressures are also eroding formerly distinct elements of media–public diplomacy–military relations, and they are tightening the nexus between the military, state and commercial media, giving rise to a military–industrial–media–entertainment (MIME) complex (Burston, 2003; Der Derian, 2002).

The seamless nature of the global media system also means that the impact of media spin, propaganda and surveillance activities may fall just as heavily upon the media and people in the US and other liberal democracies as they do elsewhere. While Americans in the past could take some comfort in domestic laws that prevented them from being the targets of US government electronic surveillance, covert media operations and propaganda, this is no longer certain (CRS, 2004, 2006). These concerns, moreover, are not abstract and hypothetical. They are concrete and specific. According to the definitive US court ruling on these issues, a broad arc of journalistic, citizen and professional rights as well as the constitutional foundations of presidential authority and American democracy have already been damaged badly (*ACLU* [*American Civil Liberties Union*] *et al*. v. (*NSA*) *National Security Agency et al*., 2006). This 'blowback' from IO is a crucial theme of this article.

A Brief History on the Origins and Structure of C3I

Things were not supposed to be this way. The work of renegade scholars from the late 1960s into the 1980s on the nexus of state–military–communications media power, which was dubbed the structure of C3I (Command, Control, Communications and Intelligence), have been pushed to the margins ever since. Writing at the apex of the Cold War, Dallas Smythe (1981) and Herbert Schiller (1969), for example, were alarmed by the fusion of electronics, communications and military spending. The pivotal role of the military could already be seen just after the Second World War, when Navy Secretary James Forrestal boasted before a seemingly startled Congress that the military's global communications grid was larger than that of 'all the private industries combined' (US Congress, 1945: 12). This was because:

> *. . . diplomatic and military affairs are so vitally dependent upon the comprehensiveness, efficiency, reliability, and security of international communications that the continuation of private competition in such communications can no more be rationalized than could the administration by private enterprise of the diplomatic and military affairs themselves. In other words, they are so closely intertwined it is impossible to separate them.* Senator Reed*: You do not really mean that, do you?* Mr. Forrestal*: Yes sir. I have reached that conclusion reluctantly. (US Congress, 1945: 10)*

Added to this, by the late 1970s, the Pentagon had financed two-thirds of all computer research and development. The marriage of computing and telecommunications gained momentum in the mid-1960s as the Defense Advanced Research

Project Administration (DARPA) pioneered an alternative to the telephone system: the Internet. In 1948, Britain, US, Australia, New Zealand and Canada signed an agreement (which continues to this day) to create Echelon, 'a global surveillance system . . . targeting . . . most of the world's . . . phone calls, internet, email, faxes and telexes' (Wright, 1998: 18). The mass media at the time were centralized and heavily regulated. National telecom monopolies saw electronic databases and computer communications as new markets. Within the context of hierarchically organized and centrally controlled communications, it was not surprising that a 1965 proposal in the US to create a National Data Centre conjured up fears of Big Brother, while blueprints for wired nations sparked anxiety about civil liberties and people's privacy. George Orwell's *1984*, Aldous Huxley's *Brave New World* and the movies *Blade Runner* and *Brazil* anchored dystopian images even deeper in the public mind. Amid all of this, the information and cultural arm of the national security state was fortified. In the past, the US had hastily cobbled together the Committee on Public Information and the Office of War Information in the crises-ridden contexts of the First and Second World Wars, respectively. That changed forever in 1953 as permanent tools of persuasion and propaganda were created: the Voice of America (VOA), the United States Information Agency (USIA), Radio Free Europe and a slew of newspapers, books and magazines, journalists and intellectuals financed by the CIA in a bid to cultivate a global milieu of opinion favourably disposed to the US view of the world (Boyd-Barrett, 2004: 38–9; Gerecht, 2006: A15).

Technologies of Freedom and the Death Knell of Dystopian Worlds?

By the late 1980s and early 1990s, however, technological changes, the demise of the Cold War and shifts in academic fashion made such views appear anachronistic. Indeed, where Schiller railed against 'technologies of domination', Ithiel de Sola Pool (1983) heralded a new generation of 'technologies of freedom'. Telephone monopolies and mass media oligopolies were being dismantled, privatized and facing more competition than ever. In addition, when AT&T was invited to take over the Internet in the 1970s, it refused. Moreover, military technology developers at DARPA designed the Internet as an open system, with its functionality and power placed at the ends of the network (Lessig, 2001: 33). All in all, declining telecom costs, powerful desktop computers, the proliferation of new media outlets and 'Net'-based applications appeared to be anything but the menacing colossus outlined by Schiller and Smythe, or the dystopian visions of *Blade Runner* and *Brave New World*.

Privacy and surveillance studies also shifted course, especially under the influence of postmodernism and cultural studies. As David Lyon (2003: 18) observes, 'surveillance now appears much less sinister. The older metaphors of Big Brother or the panopticon, redolent of heavy-handed social control, seems somehow less relevant to an everyday world of telephone transactions, Internet surfing, street-level security, work monitoring, and so on'. Even Lawrence Lessig (2001) rounded out his otherwise pessimistic assessment of the future with the observation that privacy, anonymity and openness had been hardwired into the design of the Internet. And

if this was not enough, 'pretty good privacy' could be downloaded online, from firms such as Zero Knowledge. An array of agencies also arose to audit websites and online services, bestowing a seal of 'e-trust' on those that passed muster. In sum, antidotes to surveillance seemed to be hardwired into the Internet, as part of its 'architecture' or 'code', so to speak.

The Return of Netscapes of Surveillance and Control?

Several pressures, however, have steadily chipped away at this picture: copyright laws, media technologies designed for surveillance and control, and the retooling of public communications infrastructures for information warfare. Significant challenges to the media and entertainment industries posed by the ease of information distribution and copying, and the rise of peer-to-peer networks, have sparked a powerful backlash against open media. Lawsuits against Napster, ICraveTV, My.MP3, Kazaa and entertainment fans have targeted the underground media economy, with varying degrees of success. New laws have extended the scope and duration of copyright, while digital rights management technologies limit what people can do with digital media content. The impulse to control information has also furthered vertical integration and cross-media alliances, and thus the consolidation of media markets. While all of these actions aim to conserve the 'old media' in the face of sweeping technological and cultural changes, they are sacrificing the original qualities of the Internet in the process (Lessig, 2001: 134–43; Vaidhyanathan, 2004: 41–61).

Technologies, of course, can also be designed to counter such forces. The emergence of peer-to-peer networks as soon as others are shut down reveals the hydra-headed nature of communications media. The greater availability of privacy enhancing technology (PETs), such as encryption, proxy-servers and anonymizing software demonstrate similar values. The Open Society Institute and Citizen Lab at the University of Toronto, for instance, have created and freely distributed Psiphon, a program that 'turns a home computer into a personal, encrypted server' allowing users to 'access blocked sites in countries where the Internet is censored' (psiphon.civisec.org/faq1.html). Microsoft was also forced to redesign its .Net service in 2002 to meet higher European Union standards of personal privacy.

However, these measures do not offset efforts to embed surveillance and control features ever more deeply into the infrastructure of mediated communication. In response to demands from the telecom and cable industry, for example, Cisco Systems, Nortel and Alcatel – the firms that build much of the equipment upon which the Internet and telecom networks run – have designed networks which, as Cisco Systems (1999) boasts, put 'absolute control, down to the packet, in your hands. . . . You can identify each traffic type – Web, email, voice, video . . . [and] isolate . . . the type of application, even down to *specific brands*, by the *interface used*, by the *user type and individual user identification* or by the *site address*' (Cisco Systems, 1999: 3; emphasis added). As Cisco's marketing material continues:

> *The [network's capabilities] allow you to specify the user access speed of any packet by allocating the bandwidth it receives, depending on its IP address, application, precedence, port or even Media Access Control (MAC) address. For example, if a 'push' information service that*

> *delivers frequent broadcasts to its subscribers is seen as causing a high amount of undesirable network traffic, you can . . . limit subscriber access speed to this service . . . to discourage its use. At the same time, you could promote and offer your own or partners' services with full-speed features to encourage adoption of your services. (Cisco Systems, 1999: 5)*

While these capabilities have been pitched as a critical element in the battle for 'greater mind share' in increasingly competitive markets, they have also become the cornerstones of a powerful architecture of state control, most notoriously in the People's Republic of China (Zittrain and Edelman, 2003). The US Committee on International Relations put the issues under the spotlight in early 2006, with Cisco, Microsoft, Google and Yahoo chastised for tailoring their technologies, search engines and web services to meet the Chinese government's demands. As the committee chair Christopher Smith exclaimed, the Internet offers unprecedented 'access to vast amounts of information for people the world over', but in China, these US firms have helped to turn the Internet into 'a cyber-sledgehammer of repression of the Government' (US Committee on International Relations, 2006: 1). The Chinese example shows that controlling the Internet is possible, even if imperfect. The significance of the Chinese model also lies in the fact that China is promoting it as an international standard, with Yemen, Vietnam, Malaysia, Burma, Tunisia, Egypt and, to a lesser extent, Singapore already emulating its key features. Equally significant, while Cisco may be a leader in creating an Internet of control within China, given that it accounts for 60 percent of the Chinese Internet switching and router market (US Committee on International Relations, 2006: 3), its standards have been hard-wired into the Internet world-wide, for commercial *and* national security reasons (US Committee on International Relations, 2006: 3).

The Hard Reality of Soft Power: Information Operations and the GWOT

The installation of similar capabilities in the US for reasons of state is a crucial example of information operations blowback. The Committee on International Relations hearings just discussed offered glimpses of this (US Committee on International Relations, 2006: 15), but with little insight into the larger issues at stake. The re-tooling of the Internet and infrastructures of public communication in the US is driven by: (1) the convergence of military and civilian networks; (2) Federal Communications Commission rules that require telecom and Internet companies to adopt strong surveillance and national security capabilities; and (3) licensing conditions that require the multinational consortia of US and foreign firms that control the submarine cable networks linking the US telecom system and Internet to the outside world to adopt similar mechanisms. The National Security Agency's secret Terrorist Surveillance Program, the aborted but still instructive cases of the Office of Strategic Influence and the Total Information Awareness Program, as well as the Patriot Act's combination of sticks and carrots designed to gather personal data from libraries to Internet service providers also further the slide towards a system of 'total infosphere control'. In their entirety, these efforts have fortified American military and international communication policies for the 'long war' against terrorism.

According to the US Department of Defense's (2003: 9) recently declassified *Information Operations Roadmap*, IO consists of: cyberwarfare, psychological operations, computer network operations, military deception and operational security. The doctrine stretches from the traditional mass media, to influential websites, cell phones, the Internet, blogs, email and prominent opinion leaders and decision-makers. Leigh Armistead (2004), an advocate of such ideas, argues in *Information Operations: Warfare and the Hard Reality of Soft Power*, that the aim is to 'collect, shape, process, and disseminate an uninterrupted flow of information while exploiting or *destroying* an adversary's ability to do the same' (Armistead, 2004: 19). The ultimate objective, states the *Information Operations Roadmap*, is to achieve full 'domination of the information spectrum', an aim that involves 'transforming IO into a core military competency on a par with air, ground, maritime, and special operations' (Department of Defense, 2003: 4). Information and media power, in sum, have taken on a wholly new degree of prominence in the war on terrorism.

The concept of 'infowar' includes activities that run across the 'soft' and 'hard' end of the power spectrum. The 'hard edge' of information operations was on full display when the US bombed Al-Jazeera offices in Kabul and Baghdad in 2001 and 2003, respectively (Brown, 2003: 92; Collins, 2003: 2; Reporters Without Borders, 2003). During the early stages of the Iraq War, the US military also pondered destroying critical elements of the Iraqi information infrastructure but were reined in by concerns that doing so could cause severe collateral damage to the European banking and financial system. The risk that destroying civilian communication networks could constitute an international war crime also constrained such actions (CRS, 2004: 11–17). Thus, rather than destroy the Iraqi Ministry of Information – the pillar of Iraq's broadcast and telecom system – it was taken over and made into the rebranded Iraqi Media Network (IMN). The IMN remains under Pentagon control, but is operated by a consortium of US defence contractors – Science Applications International Corporation (SAIC) and the Harris Corporation – as well as the Lebanese Broadcasting Company International (Harris Corp., 2005; SAIC, 2004). These are examples of the hard edge of information power and I return to them later.

Soft Power and the Military–Information–Media Complex

The hard edge of information operations is often overlooked by studies of propaganda. Such studies offer valuable insights into media spin, diplomacy and propaganda, but it is essential to recast them in the context of the larger whole being developed in this article. 'Soft power' aims to get others 'to want the same outcomes that you want', through consent rather than coercion, and to promote particular values and policies (Nye, 2002: 5). It focuses on the cultural underpinnings of the global system and strives to reinforce shared values between the US and other democracies, while changing the climate of opinion where such values are unwelcome (Fraser, 2003: 32). The significance of soft power has also grown immensely in tandem with the rise of a 24/7 global commercial media ecology. Seen in this light, the apparent appeal of American culture alongside its bristling military power – indeed, unrivalled superiority with the US military budget of US$400 billion equal

to that of the next 15 countries combined – is crucial to girding the US's dominant position in the world system, despite the relative decline of its economic clout (Fraser, 2003: 18–23; Nye, 2002: 81–96; Rothkopf, 1997).

The end of the Cold War, according to some, however, severely eroded US soft power. The VOA and other broadcasting agencies had their budgets cut and were brought under the authority of the fledgling Board of Broadcasting Governors (in 1996), while the USIA became an under-appreciated section of the State Department in 1999. IO seek to restore these agencies to their prior lustre, expand them, and to prise them away from the State Department so as to put them under the wing of the military and national security agencies (DSB, 2004; GAO, 2006; Snow and Taylor, 2006: 400).

Steps in this direction have followed. Budgets and the number of Arab specialists and language-speakers have been increased at the VOA. Ties to academics and think-tanks with expertise in Muslim media and cultures have been strengthened. More programmes are being disseminated by every kind of medium possible, especially to Muslim audiences. The US and Britain created Coalition Information Centres in Islamabad, London and Washington in 2001 to counter the belief in some quarters that the Taliban had gained an advantage in the 'information wars' by getting their message out while London was still sleeping and Washington going to bed. The centres were subsequently folded into the US Office of Global Communications in 2003 to tighten control over government communications and daily messages from the White House, with the aim of influencing the continuous global news cycle. The US$750 million 'Initiative 9/11' fund created Radio Farda, directed at Iran, and the Mid-East Media Network, consisting of Al-Hurra TV and Radio Sawa. At least US$400 million more have been spent on private contractors, the biggest of which are: the Rendon Group, the Lincoln Group, SAIC, Level-3 Communications and Harris Corporation (Bamford, 2005; DSB, 2004: 21–2; Robertson, 2006; Schulman, 2006: 5).

Through the sweep of these initiatives, several things stand out. First, US state-owned media outlets and propaganda operations have been expanded. In addition, propaganda is being privatized. Crucially, the lines between public affairs and media relations, on the one hand, and propaganda and psychological warfare, on the other, have blurred beyond recognition. As one senior military official states, 'the movement of information has gone from the public affairs world to the psychological operations world' (quoted in Schulman, 2006: 11). Indeed, this is exactly the outcome desired by advocates of IO, who have constantly argued that the separate 'silo' approach to public affairs and diplomacy, propaganda and psychological operations should be eliminated. Yet, this move is strongly criticized even by some public affairs officers in the State Department and the Pentagon, who feel that their credibility, and the news media that rely upon them, is being tarnished badly by their increasingly close ties to propaganda operations (Department of Defense, 2003: 23–5; DSB, 2004: 12, 24; Snow and Taylor, 2006: 400–1).

Report after report also advocates tighter cooperation between the government and military, on the one side, and commercial media outlets, on the other, as well as for the state-owned propaganda agencies to mimic commercial media production values (CRS, 2004: 14; DSB, 2004: 2–4). This, too, has occurred. Thus, weeks after

9/11, the Bush administration sent leading neoconservative Karl Rove and several others to meet media industry power brokers to discuss how they could contribute to the 'war on terrorism'. In one such meeting, they met with 30 executives, including Peter Roth, the president of Warner Brothers TV, Leslie Moonves, president of CBS Television, Sandy Grushow from the Fox Entertainment Group, Jerry Offsay of Showtime, Chris Albrecht and Colin Callender at HBO Films and Bryce Zabel, the chairman of the Television Academy of Arts and Sciences (Bart, 2001). They were ready, willing and able, but some complained that the administration was moving too slowly and that Bush's emissaries were unclear about 'what they're looking for . . . and we need some direction' (Waxman, 2001: C1).

Hollywood and the military have always maintained ties to one another, but those ties have been put on firmer footings. The nexus tightened a year into the GWOT with the Pentagon and Disney/ABC announcing plans to co-develop a 13-part 'reality-TV' series on the life of soldiers in the war on terrorism, to be produced by Jerry Bruckheimer (*Pirates of the Caribbean*, *Black Hawk Down*, *Pearl Harbour* and the *CSI* series) and Bertram van Munster (*Amazing Race* and *Cops*). Bruckheimer and van Munster received daily access to soldiers in Afghanistan, while Disney gave prime-time billing for the series: *Profiles from the Front Line* (ABC, n.d.; Der Derian, 2001). Bruckheimer, in particular, has parlayed his status as a top producer of popular television programmes and blockbuster films into a starring role in the propaganda machine, overseeing the design of the Pentagon media briefing centre in Doha, Qatar and advising its media affairs people how to spin the 'Saving Jessica Lynch' story – which later turned out to be a fabrication of heroic proportions rather than an accurate portrayal of a hero's experience.

Black Hawk Down, *Pearl Harbour* and other media fare also reveal the not-so-subtle hand of the Department of Defense, with its branches maintaining offices in Los Angeles to make it easy to make 'military-friendly' movies and television shows (see, for example, Department of Defense, 1998a; US Army, n.d.). The offices offer access to resources in return for content that supports national interests, recruitment and retention policies, and a favourable image of the US at home and abroad. The Air Force Entertainment Liaison Office touts itself as a 'single contact for . . . assistance to motion pictures and television programs. . . . Whether it's cutting edge technology or historic authenticity you're after, we can help you accomplish your goal!' (US Air Force, n.d.). Script writing and technical assistance are also offered. Such close ties come at a cost, however. And that cost is that scripts must be approved and arrangements made for 'an official DoD screening in Washington, DC, before . . . public release. Preferably this review should be before composite printing to facilitate any changes that may be required' (Department of Defense, 1998b). That is, movie makers should be ready for last-minute demands from military officials in Washington to change their film.

James Der Derian (2001) and Jonathan Burston (2003) summarize these relations as the military–industrial–media complex. They also highlight another of its key pillars: the Institute for Creative Technologies (ICT), a joint venture between the Department of Defense and the University of Southern California, with management drawn from the executive ranks of Disney, Paramount Studios and NBC Universal. ICT's main

goal is to develop cutting-edge computer simulation and animation technologies for entertainment and military purposes. The military gains access to technologies that simulate battlefield and cyberwarfare conditions, which now figure prominently in US and NATO military training exercises. It also gets a gloss of 'Hollywood style'. In return, Hollywood gets top-level special effects equipment, while the video games industry gains access to macho 'toys for boys' concepts around which it can model new games (Burston, 2003: 166; Greenwell, 2006). The result is exemplified in the popular game *America's Army*, where players vicariously experience the adrenalin rush of war, while the US military obtains another marketing tool to recruit soldiers.

The military is also taking on the media 'style' by mimicking the production, marketing and branding values of the entertainment and persuasion industries. Again, report after report, task force after task force and consultants to a name underscore the point that strategic communications must adopt modern media methods that resonate with commerce and youth culture, in particular.[1] To this end, former Secretary of State Colin Powell appeared on MTV to sell the US war on terrorism to a global audience of music video lovers – a hearty mix of politics, pop and the kids. In addition, the ranks of Madison Avenue have been pilfered, with former JWT and Oglivy brand-marketing executive Charlotte Beers appointed as Under-Secretary of State for Public Diplomacy and Public Affairs. Her task? Selling 'brand-America'. During her four-year tenure, Beers spear-headed the 'Shared Values' campaign that used television, a new magazine, *Hi*, books and other media in a bid to cast US values as universal ones. A central theme depicted Muslim Americans enjoying the lifestyle of a religious and racially tolerant America. However, the campaign failed completely to achieve its objectives and Beers stepped aside. She was replaced by George W. Bush's spiritual advisor and long-time friend, Karen Hughes, in 2005 (DSB, 2004: 40–6; Mirrlees, 2006: 3).

Nowhere is the thread tying together privatization, commercialization, propaganda and the control of information infrastructures more evident than in the Iraq Media Network (IMN). As briefly discussed earlier, the IMN was reconstructed out of the remnants of the Iraq Ministry of Information. Its first radio and television broadcasts took place in April 2003, before US troops even entered Baghdad. Since then, the IMN's television network, Al-Iraqiya, a parallel radio network and a national newspaper, *al-Sabah*, have expanded to 30 cities that include 80 percent of the population. Although pitched as an Iraqi state-owned public media service, the IMN is controlled by the Pentagon, but managed on a day-to-day basis by SAIC, Harris Corporation and the Lebanon Broadcasting Company International (LBCI). SAIC and Harris are familiar US military contractors, while LBCI is a commercial broadcaster created in the mid-1990s and which had been partly owned by Lebanon's Prime Minister Rafiq al-Hariri until his assassination in 2005 (Harris Corp., 2005; Miladi, 2003: 152; SAIC, 2004). Together, the group is responsible for rebuilding the Iraqi media infrastructure and replenishing the ranks of media professionals, since all former journalists were fired as part of the 'de-Baathification' policy. To this end, about 1000 employees have been hired and are receiving training from American advisors, such as former executive editor of Time Warner's CNN, Ted Iliff. While day-to-day operations are in the hands of Iraqi journalists, programming and editorial

control rests with SAIC and Harris Corp., and through them, the US government and military (Harris Corp., 2005; SAIC, 2004).

The thorough-going transformation of the media in Iraq has led to some 100–200 new newspapers and a burgeoning market in satellite dishes means that many other Arab and global television channels are widely available (Miladi, 2003: 152; Mirrlees, 2006: 6). While the tumultuous media environment is undoubtedly an improvement on the state of affairs under Saddam Hussein, it is hardly a model of the free media and democracy promoted by the US. The shadow of psychological operations hangs over the Iraqi media, with private contractors paid to run the hardware and others similarly placed paying the media to carry 'content' of suspect origins and questionable veracity (Mazzetti and Daragahi, 2005). In short, the lines between 'white' and 'black' propaganda have been crossed.[2] 'It's all cloak-and-dagger stuff', states Kevin McCauley, editor of *O'Dwyer's PR Daily*, but at the front of this private 'Ministry of Propaganda' stands the Rendon and Lincoln groups and L-3 Communications. Rendon appears in these matters time and time again. It played a key role in creating the fictitious 'weapons of mass destruction' claim that served as pretext for war to begin with. It also cultivated the pseudo-nationalist Iraqi National Congress, with the equally odious Ahmad Chalabi at its head. Rendon's share of the private propaganda budget since 9/11 has been US$50–$100 million (Bamford, 2005).

Beyond swamping the Iraqi media with content of dubious origins, the occupation of Iraq has led to censorship, press closures and revocation of broadcast licences. The popular *Al-Awaza* newspaper linked to Iraqi cleric Muqtada al-Sadr and another opposed to the US hand-picked Iraqi Governing Council were shut down under instructions from the Coalition Provisional Authority. Following a path blazed by other governments in the region, the Iraq Higher Media Council temporarily barred Al-Jazeera and Al-Arabiya from the country (Mirrlees, 2006: 6). In the US, Wall Street banned the first of these two Arab broadcasters from its trading-room floor, while almost every cable and satellite firm has refused to offer its service to US audiences. The Canadian regulator imposed onerous rules that made it all but impossible to receive in Canada. As the Air Force states, 'the US will continue to lose ground in the global media wars until it develops a . . . strategy to counter Al-Jazeera' (CRS, 2004: 4). Using a strategy of carrot and stick, officials from the Bush administration have begun to appear more frequently on Al-Jazeera to put forth their views. As for the stick? Al-Jazeera offices in Baghdad were bombed by US forces in 2003 – similar to events in Kabul two years earlier. Human rights and journalist groups wondered if these acts were intentional, and with good reason given the statement about 'global media wars' mentioned above and the hard edge of information operations. The *Daily Mail*'s (London) disclosure – in the face of threats of prosecution under Britain's Official Secrets Act – that George Bush Jr had pondered blowing up Al-Jazeera's headquarters in Doha during a meeting with Tony Blair, further bolstered such suspicions (Reporters Without Borders, 2003, 2004).

As a result of such actions, the US attempt to spread democracy and freedom throughout the Middle East is in tatters. In fact, the view of the US in Muslim-majority countries is getting worse, not better. Worse, soft opposition is hardening.

Moreover, the decline has yet to hit bottom (DSB, 2004: 44–6). Summing up such views, the Defense Science Board (DSB) (2004) states, 'US policies and actions are increasingly seen by the overwhelming majority of Muslims as a threat to the survival of Islam itself. [There is] an overwhelming conviction that the US seeks to "dominate" and "weaken" the Muslim World' (DSB, 2004: 35). 'There is consensus . . . that US public diplomacy is in crisis' (DSB, 2004: 16).

Yet, that same report, while taking a more nuanced view of the diversity within Muslim-majority countries than previous studies, largely recommends 'staying the course', but with greater resolve. In response to why current efforts are failing so badly, it suggests that propaganda and public diplomacy continue to be underfunded, receiving just one-quarter of 1 percent of a military budget that exceeds US$400 billion. A boost to the budgets of the Board of Broadcasting Governors, thus, may help solve the problem (DSB, 2004: 28). Philip Taylor, a communication professor at Leeds University and propaganda advisor to the administrations of Mssrs Blair and Bush, however, sees the commercialization of propaganda as the culprit. Selling ideas is different than selling brands, he notes (Taylor, as quoted in Robertson, 2006). Still others blame a lack of coordination and presidential direction. The ongoing rift between media and public affairs officers – whether in the Board of Broadcasting Governors, Defense or the State Department – and the cadre of bold IO operatives, according to others, is to blame (Schulman, 2006: 13). As ex-Secretary of Defense Donald Rumsfeld (2006) complained, these turf wars are hobbling efforts badly and they may cause the US to lose the infowar. The neoconservative Heritage Foundation points to people's knee-jerk reaction to just the idea of propaganda as well as to outdated laws, notably the 1948 Smith Mundt Act's prohibition on the use of propaganda against the American people, as the problem (Johnson et al., 2005). Similarly, Simon Worden, a high ranking officer in US Space Command states, 'the American public will need to accept that certain information warfare tactics may not seem, on the surface, to be consistent with a global free press. Clearly, some things . . . will generally be considered "off-limits"' (quoted in Schulman, 2006: 7).

Blowback and the New Normal: Information Operations and Retooling the Domestic Mediasphere for the 'Long War'

With the worldwide 'struggle for hearts and minds' failing – and even having an effect opposite to that intended – and the scope of information operations off limits in the US, perhaps the greatest impact of information operations falls on the communications media and people of the US. What if the real damage is not just in the 'outside world', but the inside world of the US and other liberal democracies? The 'new normal', suggests the *Information Operations Roadmap* bluntly, is one where IO abroad will have a significant impact at home:

> *. . . public diplomacy and PSYOP . . . messages disseminated to any audience except individual decision-makers (and perhaps even then) will often be replayed by the news media for much larger audiences, including the American public. . . . Today,* the distinction between foreign and domestic audiences becomes more a question of USG intent rather than information dissemination practices. *(Department of Defense, 2003: 26; emphasis added)*

If the intention of the Bush administration is the thin reed upon which the issues turn, than there is clear cause for concern. Indeed, Daniel Kuehl, director of the Information Strategies Concentration Program at the National Defense University, for one, strongly believes that the Bush administration does intend to have an impact on the information environment at home (quoted in Schulman, 2006: 8). The troubled existence of three programmes – the Office of Strategic Influence (OSI), the Total Information Awareness Program and the National Security Agency's (NSA) secret Terrorist Surveillance Program – suggests that he is right.

The Pentagon's plans for a new OSI were revealed by *The New York Times* in late 2001. The OSI aimed to influence public opinion by planting stories and influencing journalists and media organizations throughout the world, in friendly, neutral and enemy countries alike. It would use an indiscriminate mix of news stories planted in the media and a host of other methods that ran the gamut, as a senior Pentagon official stated, 'from the blackest of black programs to the whitest of white' (Dao and Schmitt, 2002). And standing in the midst of this flow of influence stood the Rendon and Lincoln groups and SAIC. However, about to be caught in a maelstrom of corrupted information and covert media operations, and likely tipped off by disgruntled public affairs officers in the Pentagon, American and foreign journalists pilloried the OSI (CRS, 2004: 12–13; DSB, 2004: 24; Schulman, 2006: 6). It was killed off less than six months later, or was it?

The *New York Times* exposure of DARPA's Total Information Awareness Program in late 2002, just six months after the OSI had supposedly been closed, is another example of how information operations are spilling over into the US. In this case, the aspect of IO in question was a broad surveillance programme directed at gathering up information from telephone records, Internet users, travel documents and banking transactions, inside the US and worldwide (Markoff, 2002). The Total Information Awareness Program, like the OSI, also relied heavily on the private sector, notably on huge database vendors such as Axciom. Second, the project relied on existing laws that permitted surveillance directed abroad, but ran roughshod over tight restrictions against such methods in the US. And finally, like the OSI, the project was supposedly closed down. Yet, with his classic touch of hubris, ex-Defense Secretary Rumsfeld bluntly told reporters, 'you can have the name, but I'm gonna keep doing every single thing that needs to be done, and I have' (quoted in Schulman, 2006: 7). Although speaking in this instance about the OSI, Rumsfeld's statement undoubtedly reflected his feelings on the surveillance programme as well. Indeed, the *Information Operations Roadmap*, rather than conceding the lessons learned from these debacles, blithely folds their key elements into the new IO doctrine (CRS, 2004: 14).

This cavalier attitude is also visible in the writings of military officials tucked away in specialized publications. Writing in *IOSphere*, a publication of the Joint Information Operations Center, Major James B. Kinniburgh (USAF) and Dorothy Denning (2006), for instance, lay out a strategy for extending information operations to the 'blogosphere' and the Internet. Drawing on the concept of 'full information spectrum dominance', they present the case for using IO across all three layers of the 'global infosphere': the top layer of traditional mass media; the intermediary layer of prominent websites, blogs, opinion leaders and advocacy groups; and a 'micro-layer' of

personal email, cell phones and discussion groups (Kinniburgh and Denning, 2006: 7). While recognizing that media outlets such as CNN, Fox News, *The Washington Post*, *The New York Times*, etc. continue to be the leading sources of news and current affairs even in the online world, they also argue that prominent blogs, websites and newsgroups are beginning to have a much greater impact on public discourse and perceptions. The upshot is that IO needs to map this online discourse, identify prominent blogs and websites and intervene in the online flow of information to shape that discourse. They also recommend that foreign intermediaries with established credibility and authority in their own 'cultural milieu' be identified and used as a conduit of strategic communications whenever possible (Kinniburgh and Denning, 2006: 9).

To some extent, this is already being done by 'electronic media engagement teams' operating under the US Central Command. Its tasks are to scour the Internet and to 'initiate contact with editors of Web sites that cover operations in Iraq and Afghanistan, offering the same news releases and stories written by military officials that are made available to journalists affiliated with the traditional media outlets' ('Centcom Eyes Blogs . . .', 2006). In addition to identifying prominent sites, the group evaluates their accuracy, offers additional information and 'corrections' where they see fit, and tries to push 'good news stories' in ways that 'bypass traditional print and broadcast media' ('Centcom Eyes Blogs . . .', 2006). By inviting these sites to link to 'official' military and government sites, the goal is to piggy-back on prominent websites and blogs. To this end, while only 300 blogs have taken the military up on its offer, the logarithmic scaling effect of Internet links offers connections to an additional 270,000 sites at two steps out from the original source. The biggest problem according to a Centcom spokesperson for the project, however, 'is that most links are run by supporters. . . . It's almost like we're preaching to the choir' ('Centcom Eyes Blogs . . .', 2006). While these operations are, at least according to press releases, run by staff on the media affairs side of things, Kinniburgh and Denning (2006: 10) state clearly that 'there will be times when it is . . . necessary to pass false or erroneous information through . . . all three layers . . . [of] the media'. They also acknowledge that this will violate laws prohibiting the 'US military . . . from conducting information operations against US persons' (Kinniburgh and Denning, 2006: 10). However, instead of retreating from the precipice of a legal blackhole, they charge over it by advising the adoption of 'a well thought-out deception operation that minimizes the risks of exposure' (Kinniburgh and Denning, 2006: 10). Cavalierly tossing caution to the wind, the authors slip effortlessly from nominally acceptable 'white propaganda' into the underworld of 'black propaganda'. It is a prescription for a virile and militaristic form of lawlessness in cyberspace.

Kinniburgh and Denning are not renegade mavericks; they are moving well within the shadows cast by the Bush administration's pronounced tendency to play fast and loose with established law. Thus, at the same time that Kinniburgh and Denning published their blueprint for extending monitoring and propaganda deeper into cyberspace, the Bush administration was being hauled before the court of public opinion and a District Court in Michigan over the National Security Agency's secret Terrorist Surveillance Program. The existence of the NSA's electronic surveillance

programme was disclosed by James Risen and Eric Lichtblau in *The New York Times* in December 2005 (against White House attempts to block publication of the article and amid even more intrigue created by *The New York Time's* decision to delay the article for a year) (Calame, 2006; Risen and Lichtblau, 2005). The NSA's surveillance programme was authorized by President Bush on the pretext that he could do so under the Authorized Use of Military Force legislation that had been hastily passed within days of 9/11 (CRS, 2006: 2–4). Tapping into the telecom networks and switching hubs of AT&T, Verizon and most other big US telecoms firms (except, to its credit, Qwest), the NSA's surveillance programme eavesdrops on telephone, email and Internet communications between people in the US and elsewhere in the world, targeting up to 500 people at any one time and thousands overall. The aim is to monitor the electronic communications of people suspected of having ties to Al-Qaeda and other terrorist groups, and thus to pre-empt terrorist plots. The rub, however, is that the Bush administration approved the surveillance of the US telecoms system and Internet without following the legal course of obtaining warrants through the Foreign Intelligence Review Court (*ACLU et al*. v. *NSA et al*., 2006: 22).

The leading court case is replete with sections of the government's case 'blacked out' for reasons of national security and claims that it was impossible to proceed with the case at all because doing so would reveal the existence of 'state secrets', a claim the court was told it had to give utmost deference to (Keisler et al., 2006: 2). Over and against the administration, stood those representing journalists, academics, writers and lawyers who argued that they had been illegally caught up in the electronic drag-net because of their work involving Muslims living abroad. The president lacked authority, they stated, under the AUMF, the Constitution or any law to create the secret programme (*ACLU et al*. v. *NSA et al*., 2006; CRS, 2006: 34–44). Carolyn Jewel, a writer of futuristic action and romance novels, claimed that the surveillance programme made it impossible for her to talk 'openly about Islam or US foreign policy in emails to a Muslim individual in Indonesia and that she has decided against using the Internet to conduct . . . research' (Keisler et al., 2006: 20). Government lawyers scoffed at the claim, but the judge was not so inclined.

Indeed, Judge Anna Diggs Taylor was blunt in her decision: the Terrorist Surveillance Program was illegal and unconstitutional. She further argued that the claims before the court were not speculative and general, but 'distinct, palpable, and substantial' (*ACLU et al*. v. *NSA et al*., 2006: 22). The Terrorist Surveillance Program crippled plaintiffs' 'ability to report the news and . . . to effectively represent their clients', Taylor stated (*ACLU et al*. v. *NSA et al*., 2006: 20). In exceptionally strong language, she disparaged Bush's claims that his authority stemmed from the 'inherent powers' clause of the Constitution and the AUMF (*ACLU et al*. v. *NSA et al*., 2006: 33–41). To these claims of unfettered authority, Taylor sharply retorted: 'There are no hereditary Kings in America' (*ACLU et al*. v. *NSA et al*., 2006: 40). The administration withdrew for the next six months, but in January 2007 it announced that the surveillance project would continue, but only after warrants were obtained according to the rules of the Foreign Intelligence Surveillance Act and the Foreign Intelligence Review Court. In other words, the administration would follow the law.[3]

Creating Network Infrastructures for an Age of Cyberwar

While the Terrorist Surveillance Program will apparently proceed in accordance with the law, it will continue to be superimposed on top of the public Internet and telecoms grid. And those networks are being, correspondingly, retooled to meet the needs of national security and cyberwarfare, through changes adopted by the Federal Communications Commission (FCC) in 2005 and the long-standing practice of presidential control over the intercontinental submarine cables that link the US to the rest of the world. With an estimated 70–85 percent of all military communications depending on civilian communication networks, and submarine cables accounting for a similar volume of all intercontinental information flows, these are crucial areas in which security, surveillance and control demands are embedded into the infrastructure of public communication networks (CRS, 2004: 15). With an estimated 30 countries engaged in cyberwar preparations, this also means that these countries are probing the networks of others for vulnerabilities and potential military advantages. Russia and a few others have pushed for a global legal framework to restrict the 'weaponization' of cyberspace, but such efforts have gained little traction, with the US objective of 'full information spectrum dominance' actually pushing developments in the opposing direction. Global laws, in this setting, are derided as merely the means by which the weak seek to curtail the power and influence of the strong. The dependence of military communications on civilian networks reveals the extent to which such networks constitute the battleground of information warfare, but that, conversely, also raises the issue of whether attacking the networks upon which the public depends constitutes an international war crime (CRS, 2004: 11–12).

In the face of all of these factors, it is probably not surprising that gold-plated public networks are being built to military specifications, with citizens effectively subsidizing the infrastructure of infowar. Networks have always been designed to facilitate such ends, but contemporary conditions have been dramatically altered. Steps along this path began in earnest with a host of new 'critical infrastructure protection' initiatives launched under the Clinton administration. Those initiatives have drawn the private sector, military and government closer together and have been continued under the Bush administration's National Strategy to Secure Cyberspace (United States, 2003). However, such efforts are widely seen as ineffective, leading some to believe that regulation is 'needed to supplement, or replace market forces' (CRS, 2004: 16). While the companies that run the public telecoms networks and the Internet sometimes chafe about having to shoulder the costs of national security, the FCC imposed new rules in 2005 that required them to do just that, albeit with other commercially beneficial trade-offs that, for instance, allowed them to offer broadband Internet services on a non-common carrier basis, effectively preempting debates that continue to this day over 'network neutrality' (FCC, 2005: sec. VI). Yet, in this context, the idea of network neutrality had largely been rendered mute by the increased national security obligations placed on the telecoms and Internet providers – so it was a short step from there to the sacrifice of 'open network' principles in the commercial realm. In short, open networks have been traded off for national security and greater commercial control, precisely the forces

that have been mounting in a more piecemeal fashion over the last decade, as this article observed earlier.

While there has been a fundamental change in the character of surveillance and control, it is also true that nations have always used control over networks as part of their security and military strategies. Throughout the late 19th and early 20th centuries, Britain strongly encouraged the British, European and American companies that ran the world's network of submarine cables to use London as the hub of their operations, both because this was good business and because it afforded it a great deal of control. The US claimed similar powers and the president has had concentrated authority over these matters since the first trans-Atlantic cables connected the US to Europe in 1866. Several companies challenged the basis of that authority just after the First World War, but any doubts as to the president's powers in this regard were put to rest with passage of the Cable Landing Licenses Act in 1921. And whether in London, Washington or Paris, those measures were put to good effect in the massive bout of cable censorship and the cutting of privately owned German cables during the First World War (Winseck and Pike, 2007). These powers are still the basis of presidential authority today, and they are used to implant national security interests into global communication networks, as a tool using the lure of US markets as a lever to gain entry for American firms into foreign markets, and to allow the US military, NSA and other security agencies to review the ownership, control, technical design and landing points of submarine cables landing on US soil (FCC, 2003).

Despite the massive changes in global communication between now and the distant past, the geography of the cable system still follows the paths set down in the 19th century. While the number of cables connecting the US to the rest of the world is slightly larger today, the differences in speed and capacity are incomparable – although, up to 90 percent of current capacity is defined as 'dark-fibre', bandwidth held back to avoid a glut on the global telecoms market. And now, as then, the world's communications – around 80 percent – depend on the global cable system for intercontinental communications. Just as the number of cables and cable landing centres in the late 19th and early 20th centuries were comparatively small, they are surprisingly few still. Indeed, 45 cables link the US to the rest of the world: 17 across the northern Atlantic to Europe, 15 more to South America and another 13 to Asia (FCC, 2003: 32–3). Cables running to the Middle East and Africa are scarcer yet. As usual, weak states in zones of conflict and coveted by imperial powers, if for nothing other than military bases, remain among the least connected, most poorly served places on the planet. Manuel Castells (1996) refers to them as 'electronic black holes'.

The concentration of cables is rendered tighter yet by the fact that they are clustered in a handful of metropolitan centres: Sacramento, Los Angeles, Palo Alto, Seattle and San Francisco on the west coast and New York, Boston, Washington and Miami on the east coast (Cybergeography, n.d.). Moreover, these cables intersect with the domestic system in tightly clustered and shared 'telecom hotels'. On the one hand, as US military planners note, this greatly increases network vulnerability. The sense of vulnerability is magnified still further by the fact that all of the world's undersea cables are owned by a small number of multinational consortia consisting of the largest privately and state-owned telecoms companies from the US and other

nations. On the other hand, however, the relatively small number of ownership groups and cable landing points constitute the choke points at which the nation-state imposes its authority and control over the global communications system.

In the US, that control still rests solidly in the president's hands. Access to US markets is determined by an open 'market test' and a secret national security assessment. In the first, the FCC and the Departments of Justice and Commerce pass judgement on grounds of market power, ownership, price and the existence of equivalent access to foreign markets of the interests involved in the consortia – the cornerstone of the US's long-standing reciprocity policy and its obligations under the telecoms agreement of the WTO. The other review is a convoluted process that is conducted entirely in secret, with the only public disclosure being a curt press release, at the discretion of the president, at the end of the process approving or denying the application. As personal correspondence with an official intimately involved in the review of cable landing licenses indicated:

> *. . . it is against the law for any member of the government to provide any information about a transaction, including even confirming whether we reviewed a transaction. No information is put out on any reviews unless the President makes a decision and then the White House issues a press release with the President's decision. . . . In many telecom cases the members of the Committee of Foreign Investment in the United States negotiate network security agreements to mitigate the national security concerns.*[4]

While the national security review is shrouded in the cloak of 'state secrets', the FCC's review at least indicates who the parties to this review are and, in broad brush strokes, the outlines of what is at stake. Those insights can be gained in the fascinating recent case of Global Crossing, which occurred between the collapse of the speculative telecom bubble in 2000 and the final decision in the case taken by the FCC and the president in 2003. The collapse of the telecom bubble is relevant insofar as it was that matter which had led to the bankruptcy of Global Crossing and an attempt to rescue it through a transfer of control to a new group of international investors, including the Hong Kong-based multi-billionaire and close confidante of the Chinese Communist government in Beijing, Li Kashing. When the matter went to review before the Committee of Foreign Investment in the United States (CFIUS), it was disclosed that the group had hired Richard Perle, one of the neoconservative architects of the Project for a New American Century, which many see as having defined the direction of the Bush presidency, and who continued to chair the Pentagon's Defense Science Board concurrent to his new role as lobbyist for Global Crossing. Given that the Pentagon, alongside the NSA, the FBI, CIA, Department of Homeland Security and, as just mentioned, the CFIUS, constitute the 'secret' national security review committee for cable landing licences, Perle was in an obvious position of conflict of interest. The case was redolent with 'star chamber'-like qualities and smacked of crony capitalism, an odour that eventually led Perle to resign from the DSB and a reshuffling of the ownership group so as to lose the ties to Li Kashing and, thus, indirectly to the government of the People's Republic of China.

With Li Kashing gone, the majority of ownership in Global Crossing fell to companies 'indirectly controlled by the Government of Singapore' (FCC, 2003: 41): Singapore Telecom and ST Telemedia. With a faithful and long-standing ally from

the Asia-Pacific region now in control, the remaining issues fell within the scope of the national security review. And while only the general outcomes of that review are known for all the reasons stated, enough insight can be gleaned to get a sense of its main features. Referring to the secret agreement between the Executive Branch and Global Crossing, the FCC notes that it covers 'provisions for information storage, access to facilities and data' and that all of its equipment on American soil must be 'directed, controlled, supervised and managed by a domestic communications company' (FCC, 2003: 40). Moreover, '50 percent of the members of the new GX Board must be . . . US citizens, [who] have or acquire US security clearances', with the FBI, Pentagon and director of Homeland Security all having a veto over such appointments. Global Crossing was, thus, firmly grounded on US territory and its operations calibrated so as to place it within the reach of the national security state. In sum, surveillance, control and data-gathering capacities are hardwired into the organizational and technological structure of Global Crossing. Consequently, it has been transformed from a commercial entity providing open channels of global communication into a tool of the state. Lastly, outside of a few of its specificities, these are common features of communications media built to operationalize the requirements of information operations in the long war against terrorism, a sprawling notion that reduces all of us to the level of those set up as threats to democracy and a whole way of life as we know it.

Conclusion: Blowback, American Empire and the Consequences of IO

The US has an undeniable imperial past, given its turn-of-the-20th-century forays into the Philippines and Caribbean. Whether or not that status is being restored today is still an open question. Some argue that its declining economic clout makes it all but impossible to speak of an imperial America, others that the magnitude of its influence across the spectrum of 'hard' and 'soft' power make it so, while still others claim that it is an empire in denial, an imperial power in all but name. At the same time, historically there has been a current in American political culture opposed to imperial and military forays abroad because of their corrosive impact on the character of the American people and its brand of republican democracy. Thus, it was Mark Twain who poignantly exclaimed at the height of early 20th-century US imperialism 'that it was a lot easier to get in, then it was to get out'.

While the jury is still out on the ultimate question of US imperial power, this article has shown that concerns about the corrosive impact of militarism and foreign misadventures are well placed. As Immanuel Wallerstein (2002: 68) states, 'over the last 200 years, the United States acquired a considerable amount of ideological credit. But these days, the United States is running through this credit even faster than it ran through its gold surplus in the 1960s'. And while its international legitimacy is in free-fall, even US courts and others have condemned the Bush administration for acting beyond the law and at the lowest ebb of presidential authority (*ACLU et al*. v. *NSA et al*., 2006; CRS, 2006). These are the costs, the 'blowback', from the long war on terrorism and the pivotal role of IO in that project.

Among the casualties thus far lies the increasing, but uncomfortable, tendency for the 'rule of men' to replace the 'rule of law', as Judge Anna Diggs Taylor illuminated in her pointed rebuke, 'there are no hereditary Kings in America' and 'when structure fails, liberty is in peril' (*ACLU et al*. v. *NSA et al*., 2006). While Taylor was speaking of the Terrorist Surveillance Program, a cast of characters closely tied to the Bush administration have implemented a range of programmes that fit within the remit of information operations, all operating on the margins of the law and whose outcomes even on their own terms have been, at best, questionable. Arrayed around the roundtable of information warriors sit George Bush Jr's spiritual advisor Karen Hughes, as Under-Secretary of State for Public Diplomacy and Public Affairs; Richard Perle, who served simultaneously as the head of the Pentagon's Defense Science Board and as chief lobbyist for Global Crossing before being forced to resign from both; John Poindexter, of Iran-contra infamy, who led the Total Information Awareness Program; and Bush's chief strategist until resigning in August of 2007, Karl Rove, who had met with an all too eager cadre of entertainment and media power brokers shortly after 9/11. And of course, it was ex-Defense Secretary Rumsfeld who spear-headed the creation of the nominally defunct Office of Strategic Influence and the formalization of IO. But more than this, it is the elevated status of the military in IO and the structure of American democracy, and the long-term and universal scope of the GWOT, that have a strong whiff of militarism and authoritarianism about them. As we have seen, 'normal' practices and laws have been cavalierly tossed to the wind, resulting in a communications and media environment in which media affairs and nominally acceptable 'white propaganda' slip into covert media operations and the murky underworld of 'black propaganda'.

The machinery of democracy is certainly out of kilter, although the culture of democracy offers more than a residue of hope. To their credit, a few American journalists and media organizations and people have clued into the problems at hand. In this, the unprecedented 'mea culpas' of *The New York Times* and *The Washington Post* for their slavish dependence on 'official' and 'anonymous' sources in the run-up to the Iraq War stand as a hopeful sign. Those apologies may be 'too little, too late', but they suggest that the tide may be turning, as do recent elections and George Bush Jr's incredibly low ratings in domestic opinion polls. The courts have also been surprisingly blunt, condemning the administration's surveillance programme and other aspects of the 'long war' that run foul of domestic and international laws. The ongoing rift between media and public affairs staff, on the one hand, and the cadre of bold IO operatives, on the other, is another sign of a mounting backlash. The former, standing in a long and respectable line of media professionalism, fear that the indiscriminate mix of 'white' and 'black' propaganda is tarring the entire framework of government communications, and the commercial media that rely upon 'well-placed officials', with the dirty brush of IO. That, in turn, could erode the legitimacy of government, the media and democracy itself even further. With questionable results abroad, the greatest consequences of IO may just be on the communications media and people of the US and other democracies.

Yet, while it is crucial to highlight the forces arrayed against militarism and imperial adventures, it is also necessary to candidly recognize that much of what is

taking place occurs beneath the threshold of perception. Tears in the veil here and there do not reveal the whole cloth from which current trends are cut. In this case, cyberspace has been retooled for surveillance, control, propaganda and information warfare. This has largely occurred with a compliant private sector and under the initial press of copyright laws and the seemingly quixotic attempts of far-off authoritarian states to impose order on the anarchic Internet. However, as another example of blowback from IO, a new citadel of power is arising in cyberspace, and the pressure to drive surveillance deeper yet continues unabated, with Internet service providers and electronic databases, including those used heavily by academics, journalists and the public, such as LexisNexis and Factiva, under relentless pressure to retain more detailed records of their users, to hold that data longer and to cooperate further with national security agencies. Seen in that light, the 'long war' is far from over and the culture of democracy will have to draw on even deeper resources to turn back the tide.

Notes

1. Here and throughout this article I draw heavily on the Defense Science Board Task Force Report (DSB, 2004). The document also contains an appendix that lists around 20 other studies by government agencies, task forces and think-tanks. Many of those are drawn on for background for this article, but for reasons of space are not cited here unless it is critical to do so.
2. White propaganda involves a 'deliberate, systematic attempt to shape perceptions, manipulate cognitions and direct behaviour' in an intended direction through the use of truthful, but incomplete information from known sources. Black propaganda involves the same strategic intent, but uses information from unknown origins and of dubious veracity, often intentionally based on lies and deception (Jowett and O'Donnell 2005: 6, 17–18).
3. More importantly, however, the Bush administration continues to push for new legislation to this day that would free the president from even this minimal level of oversight by secret tribunal and grant telecom and Internet companies immunity from prosecution when acting as proxies for national security agencies.
4. I have kept the name of this source anonymous out of appreciation for the potential negative professional consequences that naming them in an article of this kind might have for them. A copy of the correspondence, however, is on record with the author.

References

ABC (n.d.) 'Profiles from the Front Lines'; at: abc.go.com/primetime/profiles/ (accessed 29 January 2007).

ACLU (*American Civil Liberties Union*) *et al*. v. *NSA (National Security Agency) et al*. (2006) 'Memorandum Opinion', Case No. 06-CV-10204. Judge Anna Diggs Taylor, US District Court Eastern District of Michigan, 17 August.

Armistead, L. (2004) *Information Operations: War and the Hard Reality of Soft Power*. Washington, DC: Brassey, Inc.

Bamford, J. (2005) 'The Man Who Sold the War', *Rolling Stone* 17 November; at: www.rollingstone.com/politics/story/8798997/the_man_who_sold_the_war

Bart, P. (2001) 'H'wood Enlists in War Nets, Studios Answer Call to Arms in Fight against Terrorism', *Variety* 17 October; at: www.variety.com/article/VR1117854476?categoryid=1064&cs=1&s=h&p=0

Boyd-Barrett, O. (2004) 'Understanding: The Second Casualty', pp. 25–42 in S. Allen and S.B. Zelizer (eds) *Reporting War*: *Journalism in Wartime*. New York: Routledge.

Brown, R. (2003) 'Spinning the War', pp. 187–100 in D.K. Thussu and D. Freeman (eds) *War and the Media*. Thousand Oaks, CA: Sage.

Burston, J. (2003) 'War and the Entertainment Industries', pp. 163–75 in D.K. Thussu and D. Freeman (eds) *War and the Media*. Thousand Oaks, CA: Sage.

Calame, B. (2006) 'Behind the Eavesdropping Story, a Loud Silence', *The New York Times* 1 January; at: www.nytimes.com/2006/01/01/opinion/o1publiceditor.html
Castells, M. (1996) *The Network Society*. New York: Basic Books.
'Centcom Eyes Blogs to Shape Opinion', (2006) *Military.com* 3 March; at: www.military.com
Cisco Systems (1999) *Controlling your Network – a Must for Cable Operators*. San Jose, CA: Cisco Systems.
Collins, S. Lieutenant-Colonel (2003) 'Mind Games', *NATO Review*; reprinted at IWS: the Information Warfare Site; at www.iwar.org.uk
CRS (Congressional Research Service) (2004) *Information Warfare and Cyberwarfare: Capabilities and Related Policy Issues*. Washington, DC: CRS.
CRS (Congressional Research Service) (2006) *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*. Washington, DC: CRS.
Cybergeography (n.d.) 'Network Map'; at: www.cybergeography.org
Dao, J. and E. Schmitt (2002) 'Pentagon Readies Efforts to Sway Sentiment Abroad', *The New York Times* 19 February; at: www.commondreams.org/headlines02/0219–01.htm
Department of Defense (1998a) 'US Military Assistance in Producing Motion Pictures, Television Shows, Documentaries, Music Videos, Advertisements, CD-ROM's, etc.'; at: www.defenselink.mil/faq/pis/PC12FILM.html
Department of Defense (1998b) 'Instructions: DoD Assistance to Non-Government, Entertainment-Oriented Motion Picture, Television, and Video Productions (No. 5410.16)', 26 January; at: www.dtic.mil/whs/directives/corres/pdf/i541016_012688/i541016p.pdf
Department of Defense (2003) *Information Operations Roadmap*. Washington, DC: US Dept of Defense.
Der Derian, J. (2001) *Virtuous War: Mapping the Military–Industrial–Media–Entertainment Complex*. Boulder, CO: Westview Press.
Der Derian, J. (2002) 'The Rise and Fall of the Office of Strategic Influence', *Infointerventions* 4 March www.watsoninstitute.org/infopeace/911/article.cfm?id=42
DSB (Defense Science Board) (2004) *Report of the Defense Science Board Task Force on Strategic Communications*. Washington, DC: DSB.
FCC (Federal Communications Commission) (2003) 'Global Crossing Cable Landing License Decision' (DA 03–3121); at: www.fcc.gov
FCC (Federal Communications Commission) (2005) 'Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, etc. (Report and Order and Notice of Proposed Rulemaking)' (FCC 05–150); at: www.fcc.gov
Fraser, M. (2003) *Weapons of Mass Distraction: Soft Power and American Empire*. Toronto: Key Porter Books.
GAO (Government Accountability Office) (2006) 'US Public Diplomacy Interagency Coordination Efforts Hampered by the Lack of a National Communication Strategy', April; at: web.ebscohost.com.proxy.library.carleton.ca/isc/pdf?vid=14&hid=115&sid=0899ed2b-be74–4247-b2fb-2bbcf3910efe%40sessionmgr102
Gerecht, R.C. (2006) '"Hearts and Minds" in Iraq: As History Shows, Ideas Matter More Than Who Pays to Promote Them', *The Washington Post* 10 January: A15.
Greenwell, M. (2006) '"Operation Hollywood" and "Hollywood and the Pentagon"', *Spinwatch* 28 October; at: www.spinwatch.org/
Harris Corporation (2005) 'Iraqi Media Network Awards Harris Corporation $22 million Contract for Network Integration and Development', 20 January; at: www.govcomm.harris.com
Johnson, S., H.C. Dale and P. Cronin (2005) 'Strenghtening Public Diplomacy Requires Organization, Coordination, and Strategy', *Heritage Foundation Backgrounder* No. 1875; at: www.heritage.org/Research/National/Security/bg1875.cfm
Jowett, G.S. and V. O'Donnell (2006) *Propaganda and Persuasion*, 4th edn. Thousand Oaks, CA: Sage.
Keisler, P.D., C.J. Nichols, D.N. Letter, J.H. Hunt, A.J. Coppolino and A.H. Tannenbaum (2006) 'Notice of Motion and Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America in the case of *Tash Hepting, et. al*., v. *AT&T, et. al*.' (Case No. C06–0672-vrw); at www.eff.org/files/filenode/att/GovMotiontoDismiss.pdf
Kinniburgh, J.B. and D.E. Denning (2006) 'Blogs and Information Strategy', *IOSphere* Summer; at: www.au.af.mil/info-ops/iosphere/iosphere_summer06_kinniburgh.pdf

Knightly, P. (2004) *The First Casualty*. Baltimore, MD: Johns Hopkins University Press.
Lessig, L. (2001) *The Future of Ideas*. Toronto: Random House.
Lyon, D. (ed.) (2003) *Surveillance as Social Sorting*. New York: Routledge.
Markoff, J. (2002) 'Pentagon Plans a Computer System That Would Peek at Personal Data of Americans', *The New York Times* 9 November; at: www.nytimes.com/2002/11/09/politics09COMP.html?ex=1170824400&en=3c391fde4069f9f7&ei=5070
Mazzetti, M. and B. Daragahi (2005) 'US Military Pays to Run Iraqi Press', *Los Angeles Times* 30 November.
Miladi, N. (2003) 'Mapping the Al-Jazeera Phenomenon', pp. 149–60 in D. Thussu and D. Freedman (eds) *War and the Media*. London: Sage.
Mirrlees, T. (2006) 'Imperial Communication and Culture Wars', *State of Nature* Spring; at: www.stateofnature.org/imperialistCommunication.html
Nye, J. (2002) *Power in the Global Information Age*. New York: Routledge.
Pool, I. de Sola (1983) *Technologies of Freedom*. Cambridge, MA: Belknap Press.
Reporters Without Borders (2003) 'Reporters Without Borders Outraged at Bombing of Al Jazeera Offices in Baghdad', 8 April; at: www.rsf.org/article.php3?id_article=5945
Reporters Without Borders (2004) 'Government Shuts Down Al Jazeera Offices in Baghdad', 8 August; www.rsf.org/article.php3?id_article=11115
Risen, J. and E. Lichtblau (2005) 'Bush Lets US Spy on Callers without Courts', *The New York Times* 16 December.
Robertson, D. (2006) 'PR Joins Fight for Hearts and Minds', *Times Online* 18 September; at: business.timesonline.co.uk/tol/business/industry_sectors/media/article642219.ece
Rothkopf, D. (1997) 'In Praise of Cultural Imperialism?', *Foreign Policy* 107 (Summer): 38–53.
Rumsfeld, D.H. (2006) 'War in the Information Age: In a 24/7 World, the US Isn't Keeping up with its Enemies in the Communication Battle', *Los Angeles Times* 23 February.
SAIC (Science Applications International Limited) (2004) 'SAIC and News Coverage of the Iraqi Media Network', 26 January; at: www.saic.com
Schiller, H. (1969) *Mass Communications and American Empire*. New York: A.M. Kelley.
Schulman, D. (2006) 'Mind Games', *Columbia Journalism Review* May/June; at: www.cjr.org/issues/2006/3/schulman.asp
Smythe, D. (1981) *Dependency Road*. Norwood, NJ: Ablex.
Snow, N. and P. Taylor (2006) 'The Revival of the Propaganda State', *The International Communication Gazette* 68(5–6): 389–407.
United States (2003) *National Strategy to Secure Cyberspace*; at: www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
US Air Force (n.d.) 'Wings over Hollywood'; US Air Force Entertainment Liaison Office; at: airforce-hollywood.af.mil/index2.html
US Army (n.d.) 'Making Movies Guide'; at: www4.army.mil/outreach/documents/guide.pdf
US Committee on International Relations (2006) 'The Internet in China: A Tool for Freedom or Suppression?', Serial No. 109–157, 16 February; at: www.foreignaffairs.house.gov/archives/109/26075.pdf
US Congress (1945) *Hearings on Senate Resolution 187: A Resolution Directing a Study of International Communications by Wire and Radio*, 78th Congress. Washington, DC: GPO.
Vaidhyanathan, S. (2004) *The Anarchist in the Library*. New York: Basic Books.
Wallerstein, I. (2002) 'The Eagle has Crash Landed', *Foreign Policy* July–August: 60–8.
Waxman, S. (2001) 'White House Looking to Enlist Hollywood in Terrorism War', *Washington Post Staff* 20 October: C01; at: www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A23635–2001Oct19&notFound=true
Winseck, D. and R. Pike (2007) *Communication and Empire: Media, Markets, and Globalization, 1860–1930*. Durham, NC: Duke University Press.
Wright, S. (1998) 'An Appraisal of Technologies of Political Control', Working Document, Consultation Version PE 166 499, European Parliament, Director General for Research, Directorate B, Science and Technology Options Assessment.
Zittrain, J. and B. Edelman (2003) 'Empirical Analysis of Internet Filtering in China', Berkman Center for Internet and Society Research Publication Series; at: cyber.law.harvard.edu/home/uploads/203/2003–02.pdf

Dwayne Winseck is associate professor at the School of Journalism and Communication, Carleton University, Ottawa, Canada. His research focuses on the political economy of communication, new media, media history and global communication. He has published extensively in academic journals and the press and is the author, co-author or co-editor of four books, most recently, with Robert M. Pike *Communication and Empire: Media, Markets and Globalization, 1860–1930* (Duke University Press, 2007).

Address *School of Journalism and Communication, Carleton University, Ottawa, ON, Canada K1S 5B6. [email: dwayne_winseck@carleton.ca]*