MILITARY DISINFORMATION

A bodyguard of lies

Kevin Foster

Disinformation and propaganda

On 30 April 1943, Spanish fishermen off the coast of Huelva plucked a uniformed corpse from the waters of the Atlantic. Identity discs and miscellaneous papers identified the body as Major William Martin of the Royal Marines, who had apparently perished in an air crash. Chained to Martin’s waist was a black attaché case which contained a sealed military envelope. Over the following days, British authorities urgently sought the return of the briefcase. When the Spaniards copied and passed on the contents of the envelope to German intelligence, they caused a sensation. Martin had been carrying a personal letter from the vice chief of the Imperial General Staff, General Archibald Nye, to General Harold Alexander, commander of the 15th Army Group in Tunisia, detailing plans for the allies’ forthcoming landings in Southern Europe. The letter confirmed that the allies would come ashore in the Balkans, German-held Greece, and Sardinia. In response, significant Axis personnel and materiel were redeployed from Western and Southern Europe to the Balkan flank:

In March 1943, there were eight German divisions in the Balkans; by July there were eighteen, with the number in Greece having increased from a single division to eight; two divisions were sent to reinforce Sardinia and Corsica. That left just two for Sicily. (Fennell 2019, 340)

When the allies landed 160,000 troops in Sicily in early July, they overran the island’s depleted defences in less than six weeks.

The allies had had no intention of invading the Balkans. The letter carried by Major Martin was a hoax – as was the major himself. The body was that of a mentally ill itinerant, Glyndwr Michael, who had been found dead in London. Military intelligence claimed the body, provided it with a new identity, and armed it with disinformation specifically targeted to mislead the Germans as to allied invasion plans for Southern Europe. Operation Mincemeat, described here, offers an exemplar of military disinformation: that is to say, the ‘dissemination of deliberately false information, esp. when supplied by a government or its agent to a foreign power or the media with the intention of influencing the policies or opinions of those who receive it’ (Simpson and Weiner 1991, 448).1 Ironically, it would not have been possible to have described...
it as a disinformation operation at the time as the first use of the term in English was not recorded until 1955. The Oxford English Dictionary traces the etymology of ‘disinformation’ to the Russian _dezinformatsiya_, first used in 1949. By contrast, misinformation, the ‘action of misinforming or condition of being misinformed’, without any hint of calculation or purpose, has a far more venerable pedigree, with its first use recorded in 1547 (Simpson and Weiner 1991, 1092).

Misinformation and disinformation are entirely different in their purposes, if not their effects. What distinguishes disinformation is its emphasis on deliberation and intent – it is purposefully misleading towards specific ends. This lays bare its close relationship with propaganda, which Philip Taylor defines as

> the _deliberate_ attempt to persuade people to think and behave in a _desired way_ . . .
> the conscious, methodical and planned decision to employ techniques of persuasion designed to achieve specific goals that are _intended to benefit those organising the process_.

(Taylor 2003, 6, emphasis in original)

The changed nature of conflict during the twentieth century, the introduction of conscription, the development of the long-range bomber, the targeting of civilian populations, and the total wars these brought meant that ‘men, women and children formed the new armies and their morale, their will to fight and resist on a mass scale, accordingly became a significant military asset’ (Taylor 2003, 173). In this context, propaganda and the disinformation it entailed became key weapons of war as nations set out to undermine their enemy’s morale while shoring up their own. During the Tehran conference in late 1943, Churchill is reputed to have told Stalin that in wartime, truth is so precious that it should always be attended by ‘a bodyguard of lies’ (Gilbert 1988, 586). In what follows I will detail why this bodyguard has grown into a mass, organised force and how (dis)information has become both an increasingly important weapon in and the dominant domain of modern conflict.

_‘This will not be another Vietnam’_

By March 1973, when US forces formally withdrew from Vietnam, the conviction that the nation’s defeat was attributable to a sophisticated disinformation campaign, organised in Hanoi but executed by the Western media, was widespread. Communist North Vietnam had ‘bombed our domestic opinion with continuing propaganda’ until the American public, wearied by the media’s focus on blood and carnage, balked at further sacrifice, turned against its political proponents, and demanded peace (Tiffen 1983, 186). This oppositional media thesis regarded the free press as an active fifth column, ‘instinctively “agin the Government” – and, at least reflexively, for Saigon’s enemies’. As a result of their coverage, disinformation triumphed over force of arms, and ‘For the first time in modern history the outcome of a war was determined not on the battlefield, but on the printed page and, above all, on the television screen’ (Elegant 1981, 73). Many scholars, Daniel Hallin among them, have demonstrated the conviction that ‘the media were adversaries to American policy in Vietnam or a decisive factor in the outcome of the war’ to be false (Hallin 1989, x). Indeed, many reporters regarded their coverage as a corrective to the Joint US Public Affairs Office (JUSPAO) briefings, whose cheery summaries of body counts, kill ratios, and pacified villages misrepresented the true state of the war. JUSPAO, Michael Herr observed, ‘had been created to handle press relations and psychological warfare, and I never met anyone there who seemed to realize that there was a difference’ (Herr 1977, 174).
Despite its demonstrable falsehood, the conviction that media coverage had lost the war in Vietnam bred a hostility to the fourth estate that ‘soaked deep into the military’s cultural tissue’ (Rid 2007, 62). In response, in the conflicts that followed, militaries and their political masters set out to corral the media, control the flow of information, and so shape the message. During Britain’s re-conquest of the Falkland Islands (1982) and the US assaults on Grenada (1983) and Panama (1989), the military strictly regulated media access to, freedom of movement in, and content and transmission of copy from the area of operations. In each case, the military assault was coordinated with an official information offensive, which ensured positive coverage and promoted popular support for the operation. The inaccessibility of the Falklands and the monopoly this afforded the Ministry of Defence (MoD) over transportation to and information provision from the islands meant that ‘hardly ever have circumstances been more propitious for a censor than they were for the British in the Falklands’ (Mercer et al. 1987, 39). The task force included a number of MoD public affairs ‘minders’, whose role was to review reporters’ copy at the source (Harris 1983, 27). Not that much censorship was required. A number of the correspondents ‘decided before landing that our role was simply to report as sympathetically as possible what the British forces are doing here today’ (Hastings 1982, 1). The military campaign may have been a close-run thing, but the information offensive was a walkover.

Though Grenada was more proximate, it was no more accessible to the US media. Excluded from the invasion, the few resourceful reporters who reached the islands independently were detained by US troops. Only when the shooting finished was a handpicked pool from the major broadcasters escorted around the conflict’s key sites by a team of public affairs (PA) personnel. Once their material had been vetted, the reporters were cleared to travel to Barbados to transmit their copy, thus formally ending the news blackout. However, while they waited for their flight, the networks carried President Reagan’s live broadcast from the Oval Office announcing victory in Grenada and the safe evacuation of all US citizens. Succeeding bulletins illustrated the story with the only visuals available, US Army footage of ‘young American students making the “V” sign and smiling at the cameras as they walked up the ramp of the rescue aircraft’ (Young and Jesser 1997, 132). A humiliation for the media, Grenada ‘was a lovely war from the public information point of view’ (Young and Jesser 1997, 133). The Sidle Commission, established in its wake to review future conflict reporting arrangements, made eight recommendations, among them the creation of a national media pool. Yet its insistence that ‘The American people must be informed about United States military operations and this information can best be provided through both the news media and the government’ ensured that information would continue to be released at the behest of and in the interests of the authorities and that the media would remain shackled (Young and Jesser 1997, 134).

This was clearly demonstrated in the first Gulf War when the military’s strategy to positively shape public responses to the liberation of Kuwait centred on two of the Sidle Report’s proposals: the creation of media pools for a few select reporters, which radically constrained the fourth estate’s access to the war zone, and the live broadcast of military briefings to furnish the bulk of reporters and the public with a steady flow of upbeat, official information. Not that the military needed to worry about the media’s loyalty. Its patriotic purpose recharged by the celebratory nationalism of the Reagan years, the media clamoured to cover the war and became ‘a vital conduit for mobilizing support for US policy’. During the build-up, ‘hardly any dissenting voices were heard in the mainstream media’, which became ‘little more than public relations outlets for the White House and the Pentagon’ (Kellner 1991).

If the principal purpose of US information was to underpin domestic support, the Iraqis also targeted US public opinion. The two countries’ leaders were obsessed with Vietnam, each
Kevin Foster

convinced that US public support for the war had buckled under graphic coverage of its costs. Where Bush reassured the American public that ‘this will not be another Vietnam’, Hussein did his utmost to ensure that it would (Bush 1991). Iraq’s Ministry of Information helped Western reporters who had remained in Baghdad during the coalition bombardment of January and February of 1991 cover stories where there was evidence of coalition mistargeting and Iraqi civilian casualties, most notably the coalition airstrike on the Amiriyah bomb shelter, which incinerated 400 Iraqi civilians. However, Hussein not only overrated the media’s power in Vietnam, (as did Bush), he also failed to see that public distaste for him framed US responses to Iraqi information. Unlike Ho Chi Minh, whose determined pursuit of national self-determination had been grudgingly respected, Hussein ‘had no constituency in the US’ (Cumings 1992, 104). Though his information policies failed to dent US public support for the war, they persistently wrong-footed the coalition militaries and accelerated debate about the role and purpose of information on the battlefield.

‘The fifth dimension of war’

In the 30 years since the first Gulf War, the nature of war has radically transformed. The conflicts in Somalia (1993), Kosovo (1999), Afghanistan (2001–present) and Iraq (2003–2011) laid bare the limits of conventional military force. In each of these conflicts, the overwhelming advantage in firepower enjoyed by the US and its allies failed to subdue their adversaries, who took the fight to the information domain and triumphed. As a result, information moved from the periphery to the centre of military strategy.

Policy development on information as a strategic asset began with the collapse of the Soviet Union. In 1992, planners at the Joint Chiefs of Staff produced DOD Directive TS3600.1 ‘Information Warfare’, a policy on the use of information as a war-fighting tool. The secretary of defense at the time, Les Aspin, defined information warfare as

the actions taken to preserve the integrity of one’s own information systems from exploitation, corruption or destruction, whilst at the same time exploiting, corrupting, or destroying an adversary’s information systems and, in the process, achieving an information advantage in the application of force.

(Department of Defense 1994, 244)

From its outset, information warfare’s focus on the corruption and destruction of adversary systems established disinformation as a perennial, shadow presence in all discussions about information operations. That is to say, information operations are, by nature, disinformation operations.

In early 1993 Arquilla and Ronfeldt endorsed the new centrality of information when they proposed that ‘Warfare is no longer primarily a function of who puts the most capital, labor and technology on the battlefield, but of who has the best information about the battlefield. What distinguishes the victors is their grasp of information’ (Arquilla and Ronfeldt 1993, 141–142). Two years later, General Ronald Fogelman of the US Air Force formally identified information as ‘the fifth dimension of war’ while acknowledging that ‘Dominating this information spectrum is going to be critical to military success in the future’ (Fogelman 1995).

Just how critical was driven home during Operation Allied Force, the 1999 air force mission to halt Serb ethnic cleansing of Kosovo. NATO recognised that without boots on the ground
Military disinformation

and the information they could supply, it needed a convincing explanation for why it was bombing targets in the Balkans. To furnish this it organised

dedicated IO [information operations] cells . . . at the command and joint task force levels, tasked to integrate – and employ – such diverse tools as civil affairs, electronic warfare, intelligence, and public information in an effort to control and dominate the ‘information battle space’.

(Pounder 2000, 58)

Yet their efforts were undermined by the Pentagon’s refusal to release ‘specific information on friendly force troop movements, tactical deployments, and dispositions’ because they ‘could jeopardize operations and endanger lives’ (Pounder 2000, 66).

In the absence of information from the battlefront, NATO Public Affairs promoted its cause by launching an aggressive ‘media saturation strategy’ through which it controlled the news cycle by permanently occupying it (Combelles Siegel 2002, 191):

[O]ur credo at NATO was just to be on the air the whole time, crowd out the opposition, give every interview, do every briefing. . . . We occupied the whole day with our information. And the more we did, the less the media put on talking heads and others who could nullify our briefings.

(Shea 2002, 167–168)14

Thus, NATO’s (dis)information crowded out the enemy’s.

Yet despite the omnipresence of its spokesmen, NATO lost the information war. The Serbs controlled the ground, where they gathered and promoted, through their antagonists’ own media channels, information tailored to advance their narrative of innocent victimhood. Their information campaign was a masterwork of strategic disinformation. The commander of allied forces in Southern Europe conceded that

the enemy was much better at this than we were . . . and far more nimble. The enemy deliberately and criminally killed innocents by the thousands, but no one saw it. . . . We accidentally killed innocents, sometimes by the dozens, and the world watched on the evening news.

(Pounder 2000, 58)

NATO’s defeat in the information domain was not just due to a lack of news and images from the field. It was also attributable to its own organisational shortcomings, its failure to track how the weaponisation of information required adaptations in its own internal systems to optimise information effects. The conventional military’s existing organisational structures produced ‘a detailed institutional division of labor’ between public affairs (PA) and information operations (IO) personnel. This underpinned the ‘firewall’ that notionally existed between information provision and influence operations: ‘PA officers and IO officers receive separate educations and training, they follow diverging career paths, they work for specialized sub-organizations, they think in contrasting mindsets and philosophies of war, and they do not read the same publications and doctrines’ (Rid 2007, 115). NATO’s efforts ‘to integrate public information into IO planning . . . came to naught’ because military public affairs (PA) officers were reluctant to involve themselves in an information operations campaign (Pounder 2000, 58).
258

2000, 60). They believed that putting public information at the service of information operations would damage the reputation for trustworthiness on which PA operations depended. As a result, the military’s own organisational systems militated against ‘the implementation of IO initiatives based on public information’ (Pounder 2000, 60). The deputy director of the USAF’s Public Affairs Center of Excellence believed that this fine distinction between public information and information effects was an ethical luxury that militaries could no longer afford: ‘Everyone – commanders, IO specialists, and public affairs officers – needs to understand public information is a battlespace that must be contested and controlled like any other’ (Pounder 2000, 60). To exercise one’s scruples and vacate the field was to surrender it to the enemy.

**The digital battlefield**

The principal lesson that Jamie Shea took from Operation Allied Force was that ‘Winning the media campaign is just as important as winning the military campaign’ (Shea 2002, 167). The experience in Afghanistan and Iraq demonstrated that militaries could not do one without the other. Yet the democratisation of the means of media production and distribution in the mid-2000s advantaged non-state actors and made the media campaign that bit more challenging for conventional militaries. If, in the 1960s and 70s, those seeking the liberation of Palestine needed to hijack an airliner or attack an OPEC meeting to attract the attention of the world’s media, by the mid-2000s, the digital revolution in communications meant that Iraqi insurgents and the Taliban needed nothing more than a mobile phone and an internet connection to promote their causes: ‘Never before in history have terrorists had such easy access to the minds and eyeballs of millions’ (Koerner 2016).

When the US and its allies pursued the enemy leadership or their production and broadcasting facilities, they found that their targets had evaporated. Abandoning military hierarchy and disengaged from studios, transmission towers, and satellite dishes, their non-state adversaries communicated with, motivated, and directed their followers and the public via a decentralised network of semi-autonomous nodes: ‘a collection of remote hubs, which are themselves points of centralized “transmission”’. (Jones and Holmes 2011, 161). The futility of bombing a virtual target that was concurrently everywhere and nowhere laid bare the extent to which the conduct of war had undergone a paradigm shift that brought (dis)information to its heart.

As they struggled to suppress the insurgencies in Afghanistan and Iraq, the US and its allies reappraised what force of arms could achieve, the weapons they needed to deploy, and the battlespaces they had to contest. Rid and Hecker describe this transformation in terms of a shift from War 1.0 to War 2.0: ‘a predominantly military exercise’, War 1.0

focuses on enemy formations, aims to interrupt decision cycles, has short duration, progresses quickly, ends in clear victory, uses destructive methods . . . and is run by top-down initiatives with a clear chain of command. The media and the public in War 1.0, are a side problem, to be ignored. Information is protected, secret, and used primarily for internal purposes.

By contrast, War 2.0, is as much a political, social, and cultural exercise as it is a military venture:

Its focus is on the population, its aims to establish alternative decision cycles, its duration long, its progress slow, its end a diffuse success at best, its methods productive (such as nation-building). . . . Its initiatives often come from the bottom up, with
Military disinformation

decentralized structures of authority. The media and the public, in War 2.0, are the central battleground and they have the highest priority. Information is predominantly public, open-source, and intended for external consumption.

(Rid and Hecker 2009, 10)

As the conflicts in Afghanistan and Iraq settled into their insurgent phase and the struggle for the trust and loyalty of local and dispersed publics, it became clear to the US and its allies that the terrain they were contesting was human and cognitive, not topographical and inert. In their efforts to win the peoples’ trust, the militaries increasingly turned to the strategies and tactics of War 2.0, in which the core battlefield and the key weapons in the struggle were information, disinformation, and influence activities. As a consequence, Maltby (2012) notes, the media not only played a more prominent role in conflict, but, increasingly, militaries also designed their presentation of war through and for the media.

Military disinformation in Afghanistan and Iraq was driven by close cooperation between the US and British governments. Together they maintained top-down control over the war’s strategic narratives and the micro-messaging that supported them to ensure that information from the front lines both reflected and could be accommodated within the larger frames of disinformation through which the allies advanced their cause. The information arrangements for the second Gulf War offer a model disinformation campaign. Coordination began with the White House press secretary, Ari Fleischer, who ‘set the day’s message with an early-morning conference call to British counterpart Alastair Campbell, White House communications director Dan Bartlett, State Department spokesman Richard Boucher, Pentagon spokesperson Torie Clarke, and White House Office of Global Communication [OGC] director Tucker Eskew’ (Quenqua 2003, 1).16 Thus, the message ‘cascaded down to the rest of the propaganda apparatus’ from the White House (Miller 2004, 81).

The OGC’s role was to keep ‘all US spokespeople on message. Each night, US Embassies around the world, along with all federal departments in DC, will receive a “Global Messenger” email containing talking-points and ready-to-use quotes’. As a consequence, wherever they were in the world, US, British, and global publics received a consistent set of messages about the war, reinforced by saturation coverage throughout the news cycle:

When Americans wake up in the morning they will first hear from the (Persian Gulf) region, maybe from General Tommy Franks. . . . Then later in the day, they’ll hear from the Pentagon, then the State Department, then later on the White House will brief.

(Quenqua 2003, 1)17

David Miller notes that this apparatus provided a constant flow of disinformation. The OGC, and through it, government departments across the US ‘fed out the lies about the threat posed by the Hussein regime including the faked and spun intelligence information supplied by the UK and by the secret Pentagon intelligence operation, the Office of Special Plans’. In the UK, the Coalition Information Centre (CIC), led by the prime minister’s press secretary, Alistair Campbell, directed the campaign to mislead the media about the existence of weapons of mass destruction (WMD). . . . In particular it oversaw the September [2002] dossier on WMD and the second “dodgy” dossier of February 2003 which was quickly exposed as plagiarised and spun.
Beneath this upper-level coordination of messaging, Miller notes, the disinformation apparatus comprised four integrated elements that reached from the Cabinet and the foreign office right down to psychological operations (PsyOps) teams out in the field in Iraq:

First was the external system of propaganda run by the Foreign Office and coordinated by the Public Diplomacy Policy Department. Second was internal propaganda focused on the alleged ‘terrorist threat’ coordinated out of the Cabinet Office by the newly established Civil Contingencies Secretariat. Third and very much subordinate to the command and control propaganda systems in Washington and London was the operation ‘in theatre’ – the stage for the crushing of Iraq. This was Centcom in Doha, Qatar; the Forward Press Information Centre in Kuwait; and the embedded reporters with their military minders. Lastly, there were the US and UK military psychological operations teams undertaking overt and covert operations in Iraq, which were said only to target enemy opinion to break resistance.

(Miller 2004, 82)

Despite this top-down regulation, disinformation flows were increasingly deregulated as the capacity to isolate domestic consumers from foreign news sources, and vice versa, collapsed in the face of the digital communications revolution. By early 2003, just as defensive public information targeted at a domestic audience could be picked up by and influence foreign audiences, so information effects operations intended to manage the perceptions of adversary and foreign audiences could loop back to influence domestic audiences. Disinformation flowed in both directions.

‘Psy-oping the home team’

Over this period, militaries struggled to ensure that doctrine kept abreast of technological advances, the new capabilities they made available, and their effects on the contemporary battlefield. When the USAF’s Basic Doctrine (2003 [1997]) was revised in 2003, it reflected the air force’s developing grasp of the battlespaces specific to information operations and the assets that had to be controlled to ensure information dominance. The revised doctrine proposed that the ‘action taken to affect adversary information and information systems while defending one’s own information and information systems’ was not a single entity but the product of three integrated non-kinetic actions: ‘Electronic Warfare Operations’, ‘Network Operations’, and ‘Influence Operations’ (USAF 2003, 31). While the first two focus on control over radio frequencies, ‘satellite links . . . telemetry . . . telecommunications; and wireless communications network systems’, influence operations take place in the ‘cognitive battlespace’. Here, ‘Influence operations . . . capabilities’ are deployed to affect behaviors, protect operations, communicate commander’s intent, and project accurate information to achieve desired effects across the cognitive battlespace. These effects should result in differing behaviors or a change in the adversary decision process, which aligns with the commander’s objectives.

(USAF 2003, 31)

Efforts to target enemy decision-making and influence foreign and domestic audiences were evident in an array of information operations undertaken in Afghanistan and Iraq. The Taliban’s only radio transmitter in Kabul was destroyed by cruise missiles in October 2001
when US forces invaded, ‘and the frequency was taken over by U.S. PSYOP’. Its broadcasts sought to ‘explain to Afghans what happened in the United States on September 11, 2001, and why our government had decided to invade their country’. To maximise the audience and the information effect, the air force dropped ‘thousands of hand-cranked radios locked to U.S. PSYOP frequencies’ (King 2011, 8). In an effort to bolster its ‘source credibility’ in Iraq, the US planted ghost-written, pro-US messages in local newspapers, falsely attributed to Iraqi authors (Marx 2006, 51–59). On the home front, the Department of Defense Digital Video Imagery Distribution System (DVIDS) supplied ‘pre-packaged video, audio news stories, and images of U.S. military activity’, gathered by military public affairs personnel, ‘without charge, to any broadcast news organization in the world, including U.S. domestic channels’. Its ‘up-to-the-minute images and broadcast-quality video of military activity’ was supplemented by ‘a huge, accessible electronic library of previously produced images, video, and stories’. Sara King notes that while ‘all major U.S. networks, both over-the-air and cable, use DVIDS material’, their viewers would have had no idea which material had been gathered by professional journalists and which by uniformed servants of the military, as ‘Information provided by DVIDS is identified as “public” and users are not required to credit DVIDS when using the products that it provides’ (King 2011, 11). Thus, military propaganda and the disinformation it entails is transformed into news.

British efforts to ensure an equivalent pipeline of military-sourced information coincided with and grew out of the drawdown in Afghanistan in 2014, which instigated ‘the biggest shake-up to military reporting in a generation’. As the traffic of British reporters through Camp Bastion dwindled to near zero, news management teams in the MoD were thinned out, and their remaining staff were redeployed to the media operations group (MOG) to work on ‘direct to audience communication’. Under these new arrangements, the gaps in information provision would be filled by uniformed ‘media operators . . . filming and photographing [the army’s] own operations, before posting the edited material online’ (Hill 2014). These reforms were led by Stephen Jolly, a former instructor with 15 (UK) Psychological Operations Group (15 PsyOps). Jolly was ‘keen to see a greater emphasis on this kind of in-house news-gathering, in which material is channelled through the open gateway of digital communication and social media’, free from oversight by the fourth estate. In 2014, when MOG and 15 PsyOps moved into neighbouring buildings at Denison Barracks in Berkshire to form the new security assistance group (SAG), their cohabitation laid bare the MoD’s determination to lower the firewall between news provision and information operations:

Traditionally, the two worlds of the MOG and Psyops have existed in separate universes, the former being expected to deal in the honest-to-goodness truth, the latter being more closely associated – fairly or unfairly – with the “dark arts”, usually directing its material at an enemy’s audience.

(Hill 2014)

Two years earlier, 15 PsyOps had been awarded the Firmin Sword of Peace for setting up and supporting seven local radio stations across Helmand. Research had revealed that, given the low rates of literacy among Afghans and negligible internet coverage, the most effective channel for psy-ops was radio. The unit’s CO, Commander Steve Tatham, insisted that the stations were committed to information provision, not covert influence:

Psy-ops is all about communicating with people around and on the battlefield, who ordinarily might not hear what’s going on. . . . Most of our work in Helmand is about
talking to Afghans, and explaining and encouraging them to engage in the debate about what’s happening in their country.

(Wyatt 2012)21

Captain Kieron Lyons, who ran one of the stations and had previously ‘spent a lot of time planning the “information effect” for large-scale military operations’ in Afghanistan, acknowledged that while the broadcast material had to be truthful and attributable, its purpose was ‘to create behavioural change’ (Wyatt 2012).

To ensure that sufficient numbers of Afghans could tune in to the broadcasts from 15 Psy-Ops–sponsored Radio Tamadoun (‘all the Afghans I ever met called it what it was, Radio ISAF’), psy-ops personnel handed out thousands of wind-up radios to locals. Chris Green, who monitored coalition influence effects in Helmand, claimed he ‘never saw any of the locals actually using the radios or listening to Radio ISAF’. Despite claims that some DJs were attracting audiences of up to 50,000 for their shows, signal reception beyond the towns was ‘patchy at best and non-existent in many areas’. Further, phone-in reports revealed that most of the calls to the station’s much-vaunted talkback sessions ‘came from the same half-dozen callers’. In Green’s view, ‘by overstating the role and value’ of radio in the counter-insurgency, 15 Psy-Ops had been ‘psy-oping the home team’ (Green 2016).

Just a few months after its formation, SAG was absorbed into the newly formed 77th Brigade, where Tatham’s view that information, disinformation, and influence were indistinguishable was a basic operating premise.22 ‘Inspired by the successes of Israel and the USA’, the establishment of 77th Brigade was also a ‘response to Russia’s propaganda activities in the Crimea and the effective use of social media by the Islamic State’ (Merrin 2019, 122). Named in honour of Orde Wingate’s Chindit guerrilla force, 77th Brigade was tasked with bringing the same ‘spirit of innovation’ to the unorthodox environment of the online battlespace, where ‘the actions of others . . . can be affected in ways that are not necessarily violent’ (Beale 2015).

In July 2016, 77th Brigade established the organisation and command structure for both an overt online presence and its non-attributable covert systems. This resulted in the establishment of the digital operations group (Digi Ops), which is divided into two teams. Members of the production team ‘design and create video, audio print and digital products that aim to influence behaviours for both Army and external audience. Additionally, they advise on campaign strategy and propose innovative behavioural change methods’, while the Web Ops team ‘collects information and understands audience sentiment in the virtual domain. Within the extant OSINT policy framework, they may engage with audiences in order to influence perceptions to support operational outcomes’ (British Army 2020).23 The COVID–19 crisis revealed that one of the key targets for perception and behaviour influence was the British public. In April 2020, the chief of the defence staff, General Sir Nick Carter, disclosed that members of 77th Brigade were ‘helping to quash rumours about misinformation, but also to counter disinformation’. The information effects staff had been ‘tackling a range of harmful narratives online – from purported “experts” issuing dangerous misinformation to criminal fraudsters running phishing scams’ (D’Urso 2020).

While the Digi Ops team engaged in the open source environment with a range of actors, the delivery of covert strategic and tactical fires had passed to the task group, which provided ‘the deployable framework to deliver Information Activity and Outreach (IA&O)’ through one of its cells or teams (British Army 2020).24 Carl Miller suggested that the work of GCHQ’s Joint Threat Research Intelligence Group (JTRIG) provides a model for the sort of covert work
Military disinformation

undertaken by 77th Brigade. Our knowledge of JTRIG’s work comes from a series of slides Edward Snowden passed on to Wikileaks in 2013:

According to the slides, JTRIG was in the business of discrediting companies by passing ‘confidential information to the press through blogs etc.’ and by posting negative information on internet forums. They could change someone’s social media photos (‘can take “paranoia” to a whole new level’, a slide read). They could use masquerade-type techniques – that is, placing ‘secret’ information on a compromised computer. They could bombard someone’s phone with text messages or calls. JTRIG also boasted an arsenal of 200 info-weapons, ranging from in development to fully operational. A tool dubbed ‘Badger’ allowed the mass delivery of email. Another, called ‘Burlesque’, spoofed SMS messages. ‘Clean Sweep’ would impersonate Facebook wall posts for individuals or entire countries. ‘Gateway’ gave the ability to ‘artificially increase traffic to a website’. ‘Underpass’ was a way to change the outcome of online polls.

(Miller 2018)

Yet conventional militaries are still playing catch-up when it comes to the sophisticated deployment of disinformation. When ISIS forces seized Mosul in June 2014, their assault was spearheaded by a potent disinformation campaign. Employing Twitter, Snapchat, and other social media platforms, it publicised the gory fate that awaited those who defended Mosul. Over one 24-hour period, it issued almost 40,000 tweets, its output peaking at almost 200 per minute (Berger 2014). As a result, an attacking force of scarcely 1,500 ISIS fighters seized Iraq’s second city, whose 60,000-strong military and police detachment fled, their morale shattered by a precisely targeted disinformation offensive. This triumph brought home to conventional militaries around the world that they could not hope to match the enemy’s speed, agility, or virtual firepower. They lacked the tools, the personnel, and above all else the organisational systems they needed to optimise and deploy the information assets they possessed.

Disinformation has become a key weapon on the information battlefields of modern conflict. For today’s militaries and the governments that direct them, the question is not whether to deploy disinformation against their adversaries but how to do so to best effect while retaining their credibility with domestic audiences. Truth was never more precious than it is now, so much so that the bodyguard of lies that once protected it has grown to become an army.

Notes
1 For more on Operation Mincemeat, see MacIntyre 2010.
2 It appears to have arrived in English from the French désinformation, whose first use was in 1954 (see Simpson and Weiner, 448).
3 UNESCO defines disinformation as ‘Information that is false and deliberately created to harm a person, social group, organisation or country’, whereas misinformation describes ‘Information that is false but not created with the intention of causing harm’ (Ireton and Posetti 2018). Given that I am focused on the purposeful use of information to establish advantage over one’s adversary, what follows will be focused on disinformation.
4 In their overview of its history and evolution, Jowett and O’Donnell define propaganda as ‘the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behaviour to achieve a response that furthers the desired intent of the propagandist’ (Jowett and O’Donnell 2015, 7). It has since accrued a diverse array of often highly specialised definitions, focused variously on its function as behaviour control, psychological manipulation, corporate persuasion, pleading and convincing, a
participatory co-production, the transmission of messages, and more. See Doob 1948; Qualter 1962; Ellul 1965; Bogart 1995; Pratkanis and Turner 1996; Carey 1997; Taithe and Thornton 2000; Parry-Giles 2002; O’Shaughnessy 2004.

5 Stalin would have approved. The Soviets ran a highly sophisticated deception operation, integrated into operations and strategy throughout World War II. See Glantz 1989.

6 There is a wealth of material on information warfare; for a useful overview see Taylor 2003; Rid and Heckern 2009; Merrin 2019.

7 For more on this, see Mandelbaum 1982; Braestrup 1986; Kimball 1988; Hammond 1989.

8 See also Trainor 1990; Shotwell 1991; Gole 1996.

9 For more details on these arrangements, see Rid 2007, 77–82; Carruthers 2011, 131–138; Taylor 2003, 290–291.


12 See Armistead 2010, 47. The US administration’s first official definition of information warfare was contained in Department of Defense 1994, in a section on ‘C4I Cross-Functional Integration’.

13 The Department of Defense Dictionary of Military Terms defines information operations as ‘The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own’ (Department of Defense 2016, 110).

14 NATO’s briefings offer an exemplary illustration of mediation in which the media assume ‘an active performative involvement and constitutive role’ in the conduct of war (Cottle 2006, 9).

15 Sergeant Marilee Philen, a former USAF Europe PAO, claimed that IO planners ‘were more interested in “media manipulation” than dissemination of factual information’ (quoted in Pounder 2000, 64).

16 Quenqua notes that this routine ‘mirrors procedure during the conflict in Afghanistan’ (Quenqua 2003, 1).

17 Robin Brown notes that the OGC in Washington was essentially a reincarnation of the Office of Strategic Influence (OSI), which had been established in the Department of Defense in the autumn of 2001 to ‘“roll up all the instruments within DoD to influence foreign audiences” including those in neutral and allied countries’ (Brown 2003, 167). News of the OSI’s existence and purposes was leaked to the press in February 2002 by DoD public affairs staff concerned about potential damage to their credibility and that of the information they disseminated. This resulted in ‘a storm of criticism from the press, who feared that they were going to be the targets of false information. This, in turn, drew in the presidential communications staff who were concerned about the risk to their own credibility if the US was seen to be in the business of deceiving media organizations’ (Brown 2003, 167). Disinformation was not only toxic; it was contagious. Within a week, Rumsfeld had closed the OSI, shifting its responsibilities and its influence activities to the OGC.

18 Alberts et al. define the cognitive domain as the ‘domain of the mind of the warfighter and the warfighter’s supporting populace’ (Allen and Gilbert 2009, 135) while Kelton et al. describe it as ‘a unified threat environment where both state and non-state actors’ pursue ‘a continual arms race to influence – and protect from influence – large groups of users online’ (Kelton et al. 2019, 860).

19 This is an annual award presented to a unit of the British armed forces deemed to have made an outstanding contribution to improving civil-military relations in the UK or overseas.


21 The radio stations were set up using radio-in-a-box (RIAB), tape and CD decks, and recording and broadcasting equipment, all contained in a single, cumbersome box, which required only the addition of electricity, an antenna, and a DJ to set up a working radio station.

22 For more on 77th Brigade, see British Army 2020.

23 OSINT refers to open-source intelligence.

24 The two cells and four teams are Division IA&O (Information Activity and Outreach) Cell, Brigade IA&O Cell, IA&O Teams, Information Warfare Team (IWT), Tactical Engagement Team (TET), and IA Training and Advisory Team (TAT).

25 For more on this, see Brooking and Singer 2016.

References


Military disinformation


Harris, Robert, *Gotcha! The Media, the Government and the Falklands Crisis*, London: Faber and Faber, 1983.

Hastings, Max, ‘Why None of Us Can Be Neutral in This War’, *Daily Express*, 8 June 1982.


Military disinformation


