Australian Army
Research Centre

Social Media as a Force Multiplier

Kevin Foster

Australian Army Occasional Paper No. 6

Australian Army
Research Centre

Social Media as a Force Multiplier

Australian Army Occasional Paper No. 6

Serving our Nation

ISSN (Online) 2653-0406
ISSN (Print) 2653-0414

This research was produced as part of the contracted Army Research Scheme in the 2016/2017 Financial Year.

All enquiries regarding this publication should be forwarded to the Director of the Australian Army Research Centre.

To learn about the work of the Australian Army Research Centre visit researchcentre.army.gov.au.

Contents

Recommendations

1. **Accept failure:** Army must develop a healthy culture of tolerance around early and useful failure. Experimentation and innovation on young or new platforms bring inevitable risk, but without ownership of that risk and a tolerance of the missteps that will inevitably occur, personnel will be driven to conformity, to following SOPs, thereby stifling opportunities for creativity. The British Army provides a model approach with respect to failure:

   > *The Army needs to take the behavioural leap and start to accept that failure is acceptable in an era of continuous improvement. We should be prepared to try novel approaches and technology on the understanding that failing fast, safe and at a relatively low cost is a success in its own right.*[1]

2. **Mission command:** Army must move to mission command arrangements for social media operators and extend to them the trust that they extend to junior commanders in the field. Working under effective top-down direction, given clear arcs of fire—messages to push, amplify and avoid—operators must be trusted to do their work. This marriage of top-down direction with bottom-up speed and spontaneity will ensure that Army's messaging will be accurate, plentiful and timely.

3. **Recruitment and training:** Army must move to ensure more and smoother two-way flow between civilian and military expertise in social media via an enhanced Reserve presence and more two-way secondment opportunities. Greater porousness between civil and military organisations will assist more rapid take-up of the latest innovations in the field and keep Army at the cutting edge of development and practice. This closer working relationship should be underpinned by a bespoke training regime in which industry expertise is married with the specific needs of Army and best practice in civil society is combined with Army's purposes and outcomes.
4. **Strong narratives:** Messaging has to be shaped by strong, strategic narratives that speak to our shared experiences, cultures and concerns, that create meanings that reaffirm our sense of who we are and what we are fighting for. This was signally not the case in either Iraq or Afghanistan.
5. **Refocus resources:** In the always-at-war context of grey or hybrid conflict, Army needs to refocus resources from Phase III to Phase 0 of operations to enable active engagement with our information competitors and the shaping of the cognitive terrain for domestic audiences. The Chief of the Defence Force observed that currently across the Western world there is:

   > *a thinning of the combat force, the shooters if you like, and also a thinning of the logistic supply force, and the thickening up of this middle space, the enablers, of which, in many different meanings, the idea of information operations exist. I think we're going to continue to see that thickening of the enabler, a more effective but thinner spread of the shooters, a more effective, more commercialised sustainment path. And the power in information operations, as one enabler, it's real. It doesn't replace, ultimately, the use of violence for state purposes, but it does exactly what that broader term says, it enables, and it can enable by strengthening and coalition, by isolating the adversary, by informing the public, by so many things.*

   He went on to point out that 'we're not yet good at this'.[2] It is vital that the Army becomes as good at this as it can be in as short a time span as is possible, that it dedicates the necessary resources to upskill in this area and is prepared to take its place on the information battlefield.

Introduction: The Changed Face of War

This report examines how the Australian Army's engagement with and use of social media compares to that of a selection of its allied and comparator militaries. It finds that, despite the welcome establishment of the Information Warfare Division (IWD) in July 2017, Army continues to trail its allies and is a long way behind best practice in its adoption of, adaptation to and use of social media as a capability in the contest for information advantage against its conventional competitors and non-state actors. It finds that Army's cultural norms and organisational structures are ill-fitted to the architectures of participation that social media and the digital landscape rest on. Unless Army is willing and able to adapt its organisation, operations and practices to the flatter, networked systems of the digital environment, it will continue to underperform in the information domain.

A preliminary report that I submitted to the Australian Army Research Centre in March 2017 identified a number of larger questions that my analysis had raised, which I would like to return to and briefly address again.[3] In *War 2.0*, Rid and Hecker proposed that insurgent groups have been advantaged by the emergence of Web 2.0 and the social media platforms it supports, 'that Web 2.0 … initially benefits insurgents more than counterinsurgents'.[4] Democratising the means of producing and distributing information has enabled fringe groups, terrorists and other non-state actors to broadcast their views, their violence and their vindications of them to a potentially global audience, garnering international attention, funds and followers. These views were echoed by Harvard's Yascha Mounk, who proposed that social media:

> *weakens the power of insiders and strengthens the power of outsiders. As a result it favours change over stability—and constitutes a big, new threat to political systems that have long seemed immutable.*[5]

It is now axiomatic that social media operates, in all contexts, as a disruptive force on established forms of organisation, communication, expression, and more.[6] But is this actually the case? What have been its effects on war? How do its disruptive forces play out in the context of a hierarchical, socially conservative organisation like the military with a cautious approach to innovation, especially in the sphere of communications technology? What happens when the irresistible forces of cultural and technological change run into the immovable object of established military systems?

Summarising the 'new wars' debate in the work of Van Creveld, Münkler and Kaldor, among others, Thomas Elkjer Nissen notes that over the last three decades the character of war has changed irrevocably:

> *War is no longer about states against states (in the conventional sense), but about identity and identity claims, and about cosmopolitanism (inclusion) versus particularism (exclusion/ nationalism). Contemporary wars are therefore more about control of the population and the political decision-making process than about control over territory. Contemporary wars are therefore not to be understood as an empirical category but rather as a logical framework in which to make sense of contemporary conflicts and their characteristics.*[7]

More significantly, as social media has instigated and accelerated a number of these key changes so it has become an increasingly central actor in its conduct:

> *[A]s most conflicts and wars for western liberal democracies today are what is called 'wars of choice', requiring a high degree of legitimacy, and multiple non-state actors are struggling to mobilize support and find new ways of fighting asymmetrically, social network media seems to have become the weapon of choice. This is the case both because it is easy for nearly every actor to access and use, due to the democratisation of technology that the Information and Communication Technology revolution is facilitating, and because you can create effects that are disproportionate in relation to the investment. Effects that support the goals and objectives of the multiple actors 'fighting' in the social network media sphere, including influencing perceptions of what is going on, can, in turn, inform decision-making and behaviours of relevant actors.*

> *Due to the global connectivity that social network media provides, the actors are no longer just direct participants to conflict. They can be whoever, civilians and activists included desires to create effects. This is also why terms such as 'remote warfare' and 'social warfare' play an increasing role in contemporary conflicts, where social network media is now used for military activities … The increasing strategic use of social network media and the effects achievable in and through the use of them, empower a multitude of actors and have a re-distributive effect on international power relations. This also affects the character of contemporary conflicts.*[8]

Given the changed nature of war, its differing goals, diffuse actors, shifted battlefields and expanded weapons systems, and given the centrality of social media as a weapon, combat zone and centre of gravity in the struggle for this new, disputed terrain, it is clear that for militaries: 'The question is no longer *whether* to be on social media, but *how* to be there.'[9] Where their organisational systems and cultural norms are ill-disposed or hostile to the accommodation or optimal use of social media, militaries have to adapt or change these systems and cultures. Those who do not risk exclusion from or impotence in the information environment.[10]

This study examines how militaries in the United States, Britain, Israel and Australia have met, or have yet to meet, the challenges posed by the changed nature of conflict and the increasingly central role that social media plays in it. It considers how well adapted they are to make the necessary changes, how their doctrinal and policy settings, their organisational systems and their cultures are positioned to accommodate the radical adjustments required by the new battles, new battlefields and new weapons of 21st century conflict. It finds that a number of core factors affect a military's capacity to adapt to change. If necessity is the mother of invention, then credible threat to one's survival is the midwife to rapid adaptation, as such a busy operational tempo provides recurring opportunities to trail, test, adopt or reject innovations. Militaries that empower their junior officers to take risks and do not censure them when they fail, that are positioned and prepared to embrace bottom-up experimentation and innovation, in which bureaucratic levels are thinner, where innovations from civil society are rapidly taken up and absorbed, where resources have been deployed to enable effective action on the information battlefield and where all combatants, military and civilian, are empowered by a deep understanding

of what it is that they are fighting for and why—these militaries are better placed to adapt to the challenges of the information domain and to take up and best use the new capabilities it provides. Where fear of failure and the sanction it will bring overpowers the instinct to experimentation, where top-down control and rigid hierarchies hold firm, where junior officers and other ranks are subject to intrusive oversight in the performance of their missions, where civil society innovations are mistrusted and resisted, where actors are unsure about what is at stake on the battlefield and unmotivated by the struggle—these militaries will labour to adapt themselves to, if not actively resist, the innovations brought by social media. As a result, they will not only misapprehend the capacity of the weapons it makes available; they will struggle to locate or navigate the information battlefield. As information becomes a critical dimension in all contemporary battlefields, militaries without a solid social media capability will find themselves strategically disempowered.

What follows is divided into two parts. In the first I offer an analysis of the development of military–media–public communication from the First Gulf War to Afghanistan. This considers the evolution of information from target to weapon to platform, in the words of Rid and Hecker, and how the US and British militaries in particular recognised and responded to this. It charts the official recognition of information as the fifth dimension of war, and the organisational and policy responses to that. It considers how and why conventional militaries moved more slowly into the information space and the painful lessons they learned in Iraq, Somalia and Kosovo about the power and efficacy of effective messaging. The Second Gulf War provided the US and Britain with an opportunity to showcase the full-spectrum dominance they had been perfecting. However, it became clear in Iraq and in Afghanistan that what conventional militaries took to be the final stage in their gradual journey towards information supremacy was the first step into a new, decentred, networked battlefield where the principal impediment to success was their own structures, systems and cultures. Part II examines, respectively, US, British, Israeli and Australian military endeavours to respond to the challenges of social media, to adapt their structures, systems and cultures to social media so that they might accommodate and weaponise it. It considers the history of their engagement with social media; the policy, organisational, recruiting and training reforms they have undertaken or will need to undertake; the outcomes of their efforts to date; and how these compare with the advances made by non-state actors and other competitors.

Part 1: From Full-Spectrum Dominance to Information Operations

Chapter 1: The First Gulf War

By the end of February 1991, the verdict was in. The executive, legislators from both sides of Congress and senior figures in the national networks and the press all agreed that the media coverage of the First Gulf War had been an unqualified success. Just how much of a success was implied in the concluding remarks to President George HW Bush's address to the American Legislative Exchange Council on 1 March 1991, the day after hostilities ceased in the Gulf, when he triumphantly proclaimed, 'by God, we've kicked the Vietnam Syndrome once and for all'.[11] The spectre of Vietnam had hung heavy over the US's preparations for war in the Gulf. Indeed, the experience of the Vietnam War had haunted every US administration in the years since America's withdrawal from South-East Asia, restraining foreign intervention, fracturing domestic unity and undermining national self-confidence. As early as 1979, Robert Schultzinger notes, there was a growing sense among neoconservatives that 'a "Vietnam Syndrome" had overtaken the Carter administration, causing American officials to believe that any threat to use force would sink the United States deeply into a conflict from which it could not extricate itself'.[12] When in August 1980 Ronald Reagan addressed the Veterans of Foreign Wars Convention in Chicago as the Republican nominee for that year's US Presidential election, he identified a readiness to employ maximum military force, the political backing to use it and the moral and cultural rehabilitation of the armed forces as foremost among the cures for the Vietnam Syndrome:

> *There is a lesson for all of us in Vietnam. If we are forced to fight, we must have the means and the determination to prevail or we will not have what it takes to secure the peace. And while we are at it, let us tell those who fought in that war that we will never again ask young men to fight and possibly die in a war our government is afraid to let them win.*[13]

Prefiguring a political and cultural keynote of his period in office, Reagan announced the return of American power, singling out the nation's armed forces as the emblems of a resurrected nationalism. Yet by the end of the 1980s, despite a decade of *Rambo*, countless welcome home parades, and armed interventions in Lebanon, Libya and Grenada, it was clear from Bush's remarks that the fear of a new Vietnam continued to haunt the administration and the military into the 1990s.

While the military aims of the war in the Gulf were focused on liberating Kuwait and defeating Saddam Hussein, its principal cultural goal, 'to extirpate all vestigial traces of Vietnam', was centred on another conflict fought on another continent a generation before.[14] At times, listening to President Bush in the build-up to the war, it was difficult to determine whether he was dispatching troops to the deserts of the Persian Gulf or to the deltas of the Mekong:

> *In our country, I know that there are fears about another Vietnam. Let me assure you, should military action be required, this will not be another Vietnam. This will not be a protracted, drawn-out war. The forces arrayed are different. The opposition is different. The resupply of Saddam's military would be very different. The countries united against him in the United Nations are different. The topography of Kuwait is different. And the motivation of our all-volunteer force is superb.*[15]

In his address to the nation announcing the commencement of hostilities against Iraq on 16 January 1991, the President once again invoked the spectre of Vietnam with the explicit aim of laying it to rest:

> *I've told the American people before that this will not be another Vietnam, and I repeat this here tonight. Our troops will have the best possible support in the entire world, and they will not be asked to fight with one hand tied behind their back.*[16]

By the late 1980s, the conviction that the US news media had been one of the principal restraints on the exercise of American military power in Vietnam and bore a heavy responsibility for the country's defeat there had become axiomatic in popular culture and was 'a defining feature of the US military's public affairs policy for the next quarter century'.[17] This time, as the government and the military prepared for war in the Gulf, they were

determined to keep the media in their place. To this end, they drew up detailed plans for the management of the fourth estate, centred on two key features: military briefings and media pools.[18] In turn, its patriotic purpose recharged by the nationalism of the Reagan years, the mainstream media clamoured to cover the US armed forces as they prepared to lead the largest military assault since the Second World War. Given Hobson's choice, it readily accepted the military's restrictions on reporters' access to and freedom of movement in the area of operations, its insistence on reviewing their copy and controlling its transmission, in return for the chance to cover, however partially, the nation at war again.

From the military's point of view, these arrangements could hardly have been implemented more smoothly. From the moment that the Bush administration announced a military response to the Iraqi invasion of Kuwait on 2 August 1990, the mainstream media fell in behind the decision, becoming 'a vital conduit for mobilizing support for U.S. policy'. Over the following weeks, 'hardly any dissenting voices were heard in the mainstream media, while TV reports, commentary and discussion strongly privileged a military solution to the crisis'. Consistently promoting both the administration's justifications of its armed response and the military's deployment of its forces, the media became 'little more than public relations outlets for the White House and the Pentagon'.[19] Once the coalition's tanks rolled over the Iraqi border on 24 February 1991, the media scrambled to cover the major events as the war was over within 100 hours. After an initial embargo on news of the ground assault, imposed and then lifted by Secretary of State for Defense Dick Cheney, it appeared that 'the stage was set for one of the best U.S. Army stories ever'.[20] However, the media who were forward with troops found that it was not only difficult to access and tell the story; it was also impossible to distribute the material they had gathered: 'The Army-designed pony express system of couriers and its teams of reporter escorts', set up to transmit copy and images back to Dhahran for vetting and onward transmission to news bureaux in the US, completely collapsed. John J Fialka of the *Wall Street Journal* recalled: 'As the battles raged, we (couriers, escorts, journalists) and news copy, film and videotapes spent a lot of valuable time lost in the desert.'[21] As a result, despite the media's efforts to ingratiate themselves with the military in the build-up to the ground assault and the presence of a select few in media reporting teams close to the front lines, there were no eyewitness accounts of any of the war's major military events—VII Corps's gigantic tank battles on the Saudi–Iraqi border,

the liberation of Kuwait City, the flight of the Iraqi army or the massacre on the Highway of Death.[22] Unseen by correspondents, these events—the war's critical military engagements—were never described to the public and remain largely unknown. As such, despite the unprecedented number of reporters in the Gulf, the media coverage of the war was most notable for its omissions and failures.

Significant responsibility for the failure to reap the publicity rewards in the Gulf rested with the Army, whose 'loathing for the press' had scarcely abated in the years since Vietnam and had spread like a virus to militaries around the world.[23] As retired Marine Lieutenant General and *New York Times* contributor Bernard Trainor noted: 'The credo of the military seems to have become "duty, honor, country, and hate the media".'[24] The rot began right at the top. Secretary of Defense Cheney's disdain for the fourth estate was illustrated in his orchestration of arrangements that ensured minimal media coverage of the invasion of Panama. Under Cheney's direction, the Pentagon 'delayed the departure of the National Media Pool until just two hours before the fighting started, and then upon its arrival in Panama the government held the reporters captive on a U.S. base for another five hours'.[25] Among those in uniform: 'Several of the Gulf War's architects, most prominently Norman Schwartzkopf, were well known scourges of the press, steeped in animosity a quarter-century old.'[26] In the face of such enmity among the highest echelons, it was hardly surprising that 'Army commanders only grudgingly accepted journalists assigned to them in the Gulf and, at times, could not conceal their deep-seated hostility towards the press'.[27] The failure of the pony express system, whose personnel were 'hopelessly understaffed, underequipped, and poorly trained and motivated for the job', was not an unforeseen calamity but an entirely predictable outcome of the Army's hostile media policy.[28]

Things could hardly have been more different in the US Marines. I Marine Expeditionary Force was commanded by a former head of the Marine Corps Public Affairs office, Lieutenant General Walter E Boomer, who had a keen understanding of how the media could serve the interests of the Marines while also serving the public. Within days of the Marines' deployment to the Gulf, Boomer issued an instruction to his subordinate commanders emphasising the importance of their openness towards the media:

> *'The long term success of DESERT SHIELD depends in great measure on support [sic] of the American people. The news media are the tools through which we can tell Americans about the dedication, motivation and sacrifices of their Marines. Commanders should include public affairs requirements in their operational planning to ensure that the accomplishments of our Marines are reported to the public.'*[29]

Boomer practised what he preached, setting 'the tone for openness by availing himself to reporters from the first week he was in Saudi Arabia'.[30]

> Responding to Boomer's orders, Colonel John Shotwell recalls:
>
> *[W]e began setting up as many news media visits as were feasible without interfering with operations and training. Our philosophy was simple. We were proud of our MARINES and what they were doing in DESERT SHIELD, and we wanted to show them off.*[31]

And they did. John J Fialka recalls that, keen to facilitate maximum access for correspondents, the 'Marines never seemed [able] to get enough media people in the field'.[32] To his surprise, Shotwell discovered that the greater familiarity engendered by the Marines' extended cohabitation with the media bred mutual warmth, not contempt:

> *Some of our commanders actually began to enjoy having reporters around … Friendships and relationships developed between the journalists and the troops they covered. Perhaps more significantly, Marines grew accustomed to having journalists in their midst, and this paid dividends later on as we prepared to take the media through the breach.*[33]

Once the fighting commenced, the Marines recognised that there was no point having the media with them to witness their good work if they could not get their story back to the newsrooms and out to their readers; hence facilitating the transport of reporters' copy was made a top priority. Unlike the Army, they ensured that their arrangements worked:

> *[W]e devised a system that exploited existing logistical channels to return the video, film, and print articles to the rear. We strategically placed about a dozen people as couriers at key points in the resupply chain. This allowed our couriers to piggyback aboard medevacs, fuel trucks, and ammo wagons returning from the battlefield to rear areas where other Marines were waiting to rush them by air or ground to Jubail or Dhahran.*[34]

The differences between the Army's and the Marines' approaches to their relations with the media were 'so vast that reporters sometimes wondered whether they were representing different countries'. The results of these differing approaches were no less stark. Though they accounted for barely 10 per cent of the coalition forces in the Gulf, 'the Marines garnered most of the publicity, skewing the coverage of the ground war, in which they performed a much smaller, supporting role to the Army'.[35]

There was more to the Marines' strategy than vanity. While good headlines were welcome they also appeared to exercise a positive influence on the Marines' performance. Reflecting on the correspondents' 'glowing accounts' of their time with the Marines, Shotwell concluded:

> *It isn't unreasonable to postulate that this media coverage heightened public appreciation, which in turn became a force multiplier that kept spirits soaring and honed our determination to overwhelm the enemy and liberate Kuwait.*[36]

Good headlines generated better performance, which brought more positive coverage, and so the virtuous circle turned. In the light of this, Shotwell and the Marines recognised that in order to keep the public fully informed and so reap the positive psychological and performance outcomes their approval bred, it was imperative that the media accompany the Marines in the field. Hence, public affairs had to be 'incorporated into operational planning'.[37] In this recognition of the centrality of information to the effective conduct of a campaign, the Marines were almost a decade ahead of their comrades

in Army and many years in advance of the military's most sophisticated source of information operations policy and doctrine, the United States Air Force (USAF).

After the initial euphoria of victory in the Gulf had passed, misgivings about the restrictions imposed on the media that had been circulating mostly among progressive outlets during the build-up to and at the time of the air and ground campaigns finally went mainstream. On 1 May 1991, executives from the US media establishment, representing 15 of the nation's most influential television networks, newspapers of record and magazines, wrote to Secretary of Defense Cheney, alleging that:

> *the flow of information to the public was blocked, impeded or diminished by the policies and practices of the Department of Defense ... Stories and pictures were late or lost. Access to the men and women in the field was interfered with by a needless system of military escorts and copy review. The pool system was used in the Persian Gulf War not to facilitate news coverage but to control it.*[38]

In Cheney's eyes, this charge sheet was less an indictment of the failings of the Pentagon's media policy than a roll call of its successes. This was exactly what he and the Pentagon had hoped for. Defense's media management practices during the war, he claimed, were 'a model of how the Department ought to function … If we had to do it tomorrow, I would start with what we've just done'.[39] Pete Williams, the Assistant Secretary of Defense for Public Affairs, went further, claiming that as a result of the Joint Information Bureau (JIB) briefings and the pool system, 'the press gave the American people the best war coverage they ever had'.[40]

This was not a view universally shared among the US media establishment, for whom the end of hostilities brought some uncomfortable soul-searching. John MacArthur noted that:

> *… in the weeks and months of postwar wailing and self-criticism by the media, it was difficult to find anyone who didn't, at least officially, count Desert Storm as a devastating and immoral victory for military censorship and a crushing defeat for the press and the First Amendment.*[41]

Dan Rather, the CBS news anchor, was one of the more outspoken critics of the 'high-cost, low-benefit horde journalism' that marked the coverage of the war.[42] He condemned the media's failure to stand up to the generals and the administration, to demand access, to refuse censorship, to ask the hard questions and so hold the nation's military and political leaders to account: 'there was a lack of will, a lack of guts to speak up, to speak out, speak our minds, and for that matter to speak our hearts'. Rather suggested that the coverage of the Gulf War was not an isolated failure but magnified:

> *a general trend of American journalism over the last five to ten years that you can see in the coverage of political campaigns, in the coverage of domestic issues such as race and the economy … and manifested itself in the intensive coverage which is an inevitable consequence of war. It is: just get in the middle and move with the mass; don't cause any trouble; don't ask any tough questions; don't take the risk.*

The outcome of this approach, he lamented, was a preponderance of 'Suck-up coverage' from a media now seemingly more interested in cosying up to power than speaking truth to it.[43]

If the Army had proved itself incapable of working cooperatively with the media in the field, the briefings it ran through the JIB in Dhahran for reporters not allocated to forward pools were a signal success and revealed an unanticipated facility for managing, mesmerising and ultimately supplanting the fourth estate. Though ostensibly staged for the benefit of the reporters crowded into the briefing room, the military spokespeople's true audience were the American and international publics, who, through the good offices of CNN, were able to follow the proceedings live-to-air. Nothing was left to chance. The two main spokesmen, Brigadier Richard Neal, Schwartzkopf's Deputy Director of Operations, and Tom Kelly at the Pentagon, were selected after exhaustive auditions, the former chosen because he projected 'unflinching honesty'.[44] The briefings were carefully stage-managed. While the open Q&A sessions lent an appearance of openness and transparency, question time was kept short, questioners were carefully selected and there was little opportunity for genuine probing of issues. The centrepiece of the briefings was the nose-cone camera footage of US and British smart bombs homing in on and obliterating their targets. This footage embodied the calculated portrayal of the war as 'uncannily sanitised',

characterised by ‘clever bombs that wrecked real estate but somehow seemed to leave people unscathed’.[45] As Philip Taylor noted, through such footage the Americans and their allies aimed ‘to change public perception of the nature of war itself, to convince us that new technology has removed a lot of war’s horrors’.[46] The smart bomb and the footage it captured thus became ‘simultaneously image, warfare, news, spectacle and advertisement for the Pentagon’.[47] This was a war of television, by television, for television. Footage of this kind, and its deft presentation to enthralled domestic audiences, demonstrated that the revealed effect, if not the intended purpose, of the JIB briefings was not to inform and so galvanise the media but to usurp their role and disempower them by directly addressing the American public.

If this was an unexpected outcome of the military’s information management, a more deliberate information campaign, employing different media and directed at a different audience, was just as successful. Over the course of the conflict, coalition aircraft dropped 29 million leaflets over enemy lines encouraging Iraqi servicemen to capitulate.[48] Helicopter-borne transmitters brought ‘The Voice of the Gulf’ to the front lines. Its broadcasts, warning Iraqi troops that ‘the “Mother of All Battles” would turn out to be the “Mother of all Defeats”’, urged them to save themselves and desert.[49] On the ground, psychological operations teams equipped with loudspeakers accompanied frontline troops, shouting instructions across no-man’s-land to the Iraqis explaining how to hand themselves over to coalition troops. The effects were spectacular: before President Bush called a halt to hostilities, more than 80,000 Iraqis had surrendered to coalition forces—whole fronts melted away as the troops yielded in company and battalion sized groups. While there was much talk about the performance of Scud and Patriot missiles in the First Gulf War, the weapon that truly came to the fore was as old as warfare itself: information. In a potent demonstration of how effectively information had been weaponised, 25 years later ISIS employed Twitter, Snapchat and other social media to publicise the gory fate that awaited those who defended Mosul. As an attacking force of scarcely 1,500 ISIS fighters bore down on Iraq’s second city, 60,000 Iraqi military and police fled, their morale shattered by a targeted information offensive.[50]

It was not only the Americans who pursued an increasingly sophisticated information campaign during the First Gulf War. The Iraqis showed themselves to be unexpectedly deft when it came to information operations

and media management. While the US information offensive was principally directed at its domestic constituency, Saddam Hussein had little need to worry about public opinion at home, where the media were cowed or muzzled. The focus of his information offensive was the US public, whose support for the war in Vietnam, he believed, had buckled under repeated exposure to evidence of casualties suffered and inflicted. It was Hussein's aim to give the American public a generous serving of the same from Iraq. In fact, it could be claimed that Saddam Hussein was hardly less obsessed with Vietnam than was President Bush. Accordingly, Western reporters who had remained in Baghdad during the coalition bombardment of the country over January and February of 1991, where they worked under the close supervision of the Iraqi Ministry of Information, were given every assistance to cover stories where there was evidence of coalition mis-targeting or, better still, Iraqi civilian casualties. On the night of 13 February 1991, a USAF F-117 'Stealth Bomber' dropped two 2,000-pound smart bombs on what was alleged to be a command and control bunker in the middle-class suburb of Amiriyah, being used that night as an air-raid shelter by local civilians. Apprised of the tragedy, the Ministry of Information urgently bussed in members of the international media to witness the recovery of the charred remains of more than 400 men, women and children being lifted from the rubble. Though the most shocking images were never broadcast, 'deemed likely to offend the "taste and decency" of western audiences', those that were used were 'at such variance from the coalition's previous pronouncements about minimal "collateral damage"' that they had a profound effect on viewers.[51]

Ironically, this effect was most notable among politicians and media supporters of the war, who turned their fury on their dissenting colleagues. The *Daily Mail* alleged that, in the light of its coverage of the Amiriyah bombing, the BBC might more accurately be thought of as the 'Baghdad Broadcasting Corporation' while Wyoming Senator Alan Simpson dismissed CNN's Peter Arnett, who reported from the scene, as an Iraqi 'sympathiser'.[52] Variously, as Philip Knightley observes, the reporters who remained in Baghdad—who included, besides Arnett, John Simpson of the BBC and Brent Sadler of ITN—were denounced as 'friends of terrorists, ranters, nutty, hypocrites, animals, barbarians, mad, traitors, unhinged, appeasers and apologists for a dictator'.[53] The pictures also had a significant impact back in Washington—with concrete outcomes on the ground in the Gulf. Spooked by the harrowing images from the bunker and the ever-present fear that the US public might turn against the war, the US

halted air strikes on Baghdad for the next 10 days. Thereafter the Chairman of the Joint Chiefs of Staff, General Colin Powell, instructed General Schwartzkopf to erase all target lists, relocating approval authority for air strikes on Baghdad from the theatre of operations to Washington.[54] This was a significant tactical victory for Hussein and a startling demonstration of how information power could be readily leveraged into military effect.

However, the Iraqi dictator's conviction that if the US public saw enough shocking material from the Gulf they would withdraw their consent to the war, as they had purportedly done in Vietnam, not only betrayed a fundamental—if widespread—misapprehension about the role of the media in shifting US public opinion on the war in Vietnam.[55] It also demonstrated a critical misunderstanding of US public attitudes towards him. Unlike Ho Chi Minh, who, numbers of Americans believed, was a patriotic nationalist pursuing the just cause of self-determination, Hussein 'had no constituency in the US'.[56] Hated and feared, he was manifestly a despot and a thug. As such, though he failed to dent US public support for the war, or garner much public sympathy among coalition countries, his information policies prompted vigorous debate in the Western media about the rights and wrongs of reporting from 'enemy' territory and kept the coalition militaries on the back foot.[57] His army may have crumbled, but his information offensive stood up and landed some telling blows.

Chastened by their media management failings in the Gulf, the US military was quick to recognise the power of information as a force multiplier. Through the 1990s they published an array of policy documents, reports and doctrine in which they endeavoured to articulate the emerging role of information in warfare. The USAF's summary of lessons learned, the *Gulf War Air Power Survey*, published in 1993, acknowledged that press coverage 'is an unavoidable yet important part of military operations'. However, the principal lesson that the USAF took from the Gulf did not bring it or the Army any closer to the realisation that they needed to integrate information management into their operational planning. Their conclusions served only to reinforce existing knowledge and practice: 'Experience again proved that while the press could be *managed* more or less successfully, it could not be ignored, and it could not be *controlled*.'[58] They had not yet realised that it was information, not the media, that they needed to manage.

Chapter 2: Somalia and Kosovo

While the US military were still fixated on managing the media, just how little control they could exercise over the flow of information from the media to the public, or the public's responses to that information, was graphically illustrated during their operations in Somalia. After the outbreak of civil war early in 1991, the government imploded, the Army fragmented and Somalia descended into anarchy. As warlords and their factions battled one another for power in the cities, towns and villages, food production collapsed and more than five million Somalis stood on the brink of starvation. By early 1992, more than 300,000 had died while another 3 million had sought refuge in surrounding countries. When the Organisation of African Unity and the UN sent peacekeeping forces to Somalia to enable NGOs to distribute food relief to the hungry, the warlords plundered their convoys and attacked their personnel. In late 1992, a Unified Task Force (UNITAF), led by US forces, initiated Operation Restore Hope, implementing UN Security Council Resolution 794, to establish a safe haven in the south of the country from where humanitarian operations could be conducted. On 9 December 1992, US Marines landed in Mogadishu and within a matter of days had secured the port, the airport and a substantial portion of the city. Yet this show of force did little to dissuade the warlords, who adopted an increasingly aggressive stance towards the humanitarian program and the armed servicemen there to protect its operations. One of the most powerful warlords, Mohammed Farrah Aidid, took his campaign to the airwaves, broadcasting anti-coalition propaganda over Radio Mogadishu. When Pakistani UNITAF personnel raided the radio station, Aidid's forces attacked, killing 24 and wounding 57. In early June 1993, the UN Security Council passed Resolution 837 authorising the arrest and prosecution of those responsible for the deaths of the Pakistani soldiers.

Accordingly, on 3 October 1993, US Special Forces raided the Olympic Hotel in central Mogadishu where some of the leading members of Aidid's Habr Gidr clan were meeting. Stout opposition from Aidid's forces fomented broader resistance on the streets. What should have been a straightforward 'snatch and grab' operation developed into a rolling battle involving ground troops, attack helicopters and eventually a two-mile-long armoured relief column. In less than 24 hours of fighting, the Battle of Mogadishu cost the Americans 18 dead, 84 wounded and one captured. Iconically, they also lost two Black Hawk helicopters to small arms fire.[59]

The world's media, on hand to cover the humanitarian mission, were well-placed to report the fallout from this disastrous operation. When CNN broadcast footage of the naked body of a dead US Ranger being dragged through the Mogadishu streets amid cheering crowds, the public response in the US was as visceral as it was immediate. Pressured by their constituents, members of Congress demanded the withdrawal of their forces from Somalia. As Republican Senator Phil Gramm noted: 'The people who are dragging American bodies don't look very hungry to the people of Texas.'[60] Senator Robert Byrd of West Virginia sponsored an amendment to the enabling legislation for the mission that would cut off funding for it. In the White House, the graphic images from Mogadishu led to a rushed reassessment of US policy. As President Clinton's National Security Adviser Anthony Lake noted, the images 'helped make us recognize that the military situation in Mogadishu had deteriorated in a way that we had not frankly recognized'.[61] Yet the pressing issue here was not military but political. The images, and the public pressure they uncorked, forced Clinton's hand. In a broadcast to the American people three days after the battle he pledged to withdraw all US forces from Somalia within a matter of months. Reflecting on the undue haste with which these decisions were taken, Clinton's Director of Communications, George Stephanopoulos, observed that decision-making in the White House was affected by the 24-hour news cycle as 'CNN assures that you are forced to react at any time' to unexpected events or new information.[62] Yet in reacting so precipitately, another of Clinton's advisers noted, 'There's really no time to digest this information … so the reaction tends to be from the gut, just like the reaction of the man on the street'. Not only are policy responses potentially ill-formulated; in the compressed time frame imposed by the immediacy of live news, there is no time to establish the veracity of their premises. As a consequence, 'High-level people are being forced essentially to act or to formulate responses or policy positions on the basis of information that is of very uncertain reliability'.[63]

In this case, it seems that the policy failure that saw the US hurry out of Somalia was less the surprise outcome of chaotic events than the careful targeting of weapons-grade information by the enemy. The images of the dead Ranger and the 'interview' with captive Black Hawk pilot Michael Durant that CNN broadcast and that engendered such a violent public reaction in the US were supplied by a stringer, Mohamoud Hassan, who had formerly freelanced for Reuters and who, it was alleged, was now associated with Aidid. His pictures had been rushed through Nairobi to London and on to CNN headquarters in Atlanta for broadcast to America and the world. The Somalis were convinced that just as the Americans had been moved to go into Somalia by images of thousands of starving civilians, so their will to remain would not withstand the sight of their own casualties. They were right. The CNN footage, David Stockwell noted, 'called America's bluff on perseverance'.[64] The images were weapons that found their precise target and detonated to spectacular effect.

Thomas Rid argues that the experience in Somalia 'made it forcefully clear' that the media:

> *were not just becoming a permanent tactical condition of the battlefield … they had become a strategic factor in the* political *environment in Washington, and that factor could determine the outcome of an entire military operation.*[65]

But 'forcefully clear' to whom? Two years after the withdrawal from Somalia, Lieutenant General Anthony Zinni of the Marines was still convinced that the principal lesson from Somalia was that 'The U.S. Commander must understand how to deal with the media and the important implications of media coverage'.[66] While the US military continued to fixate on elementary matters of military–media organisation, its competitor, in this case an African gang unable to match the US military's firepower, used the weapon at its disposal, information, and deployed it against the US and international publics, with impressive results. Recognising that 'public opinion is a military operation's centre of gravity', Aidid and his followers were operating in the information environment while the US military and its allies were still trying to work out what it was.[67] The real lesson from this chastening experience for politicians and the armed forces was both more fundamental and more sophisticated than they had thought. The lesson of Somalia was less the need to control the media than it was the imperative to recognise where

battle was being joined, with what weapons, against which enemy and to what ends. When the media was the battlefield, public opinion the prize, and words and images the weapons of choice, the goal was clear: 'if you do not want to be controlled by the information environment, control the information environment'.[68] While Western militaries did not take long to work this out, it took them a lot longer to generate the necessary doctrine and to determine how best to organise themselves effectively to act on this simple but powerful truth.

Leigh Armistead notes that the seeds of US military policy development on information warfare were sown in the wake of the collapse of the Soviet Union and bore fruit in doctrine during the first Bush administration and President Clinton's first term.[69] In late 1992, strategic planners at the Joint Chiefs of Staff produced DOD Directive TS3600.1 'Information Warfare', a policy on the use of information as a warfighting tool. Principally focused on organising for the threat of computer network attacks, the document remained top secret, thus curtailing any wider discussion about the integration of information and computing technology into military strategy and operations. The wider debate was formally inaugurated in March 1993 when General Colin Powell, the Chairman of the Joint Chiefs of Staff, issued Memorandum of Policy (MOP) 30. This introduced and defined the concept of Command and Control Warfare (C2W) as 'the military strategy that implements information warfare on the battlefield and integrates physical destruction'.[70] In the wake of this memo, 'Many units and all four military services in the United States developed command and control warfare cells and began training in this new doctrine throughout the mid-1990'.[71]

One of the key publications laying out the seismic consequences of information's new centrality in warfare appeared in early 1993, notably from a non-military source. In 'Cyberwar is Coming!' John Arquilla and David Ronfeldt of the RAND Corporation's National Security Research Division proposed that the innovations in platforms, ordnance and communications, 'precision guided munitions, stealth designs for aircraft, tanks, and ships, radio-electronic combat (REC) systems, new electronics for intelligence-gathering … futuristic designs for space-based weapons and for automated and robotic warfare', taken together, constituted 'a military technology revolution (MTR)'. At the heart of this transformation in how militaries thought and fought were 'new information and communications systems that improve command, control, communication,

and intelligence (C3i) functions' that were themselves part of a broader 'information revolution' sweeping developed societies.[72] In the light of these developments, Arquilla and Ronfeldt argued:

> *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.*

To profit from their superior mastery of information, these militaries must not only know 'how to find the enemy while keeping it in the dark' about their own positions; they must also have the 'doctrinal and organizational' systems in place to ensure that their information assets are collected, communicated and deployed with optimal efficiency.[73] What Arquilla and Ronfeldt were pointing to here was that militaries did not just need to think and fight differently, but that they could only do so by revolutionising how they organised themselves internally. The shock waves from the information bomb were as disruptive to and within military systems as they were on the battlefield:

> *The information revolution in both its technological and non-technological aspects, sets in motion forces that challenge the design of many institutions. It disrupts and erodes the hierarchies around which institutions are normally designed. It diffuses and redistributes power, often to the benefit of what may be considered weaker, smaller actors. It crosses borders, and redraws the boundaries of offices and responsibilities.*[74]

Officially, the US Army pronounced itself ready to meet the challenge, prepared to undertake 'a structured effort to redesign the Army—units, processes and organizations—from those of the industrial age to those of the information age'.[75] This would entail the introduction of greater 'doctrinal flexibility', 'strategic mobility', and 'flatter … less rigidly hierarchical' organisations.[76] Yet while this was easy to promise, it was massively more challenging to deliver. If, as Army Field Manual 100-6 *Information Operations* put it, 'information is the currency of victory', then Army was going to have to heavily invest in internal reorganisation before it could hope to reap the dividends.[77]

While at this point only a few militaries realised that the effective management of information assets would require wholesale internal reorganisation, there was a wider understanding by the mid-1990s that information was more than a weapon or a platform, and that it constituted a whole new operating domain. It officially came into being as the fifth domain of warfare when, addressing the Armed Forces Communications and Electronics Association in Washington on 25 April 1995, USAF Chief of Staff General Ronald Fogelman reflected on how warfare, and in particular the environments in which it was conducted, had evolved over the 20th century. The struggle for dominance had moved from land and sea to encompass first the air, then space, and most recently information. 'Information', he claimed:

> *… has an ascending and transcending influence—for our society and our military forces. As such, I think it is appropriate to call information operations the fifth dimension of war. Dominating this information spectrum is going to be critical to military success in the future.*[78]

Fogelman's analysis was remarkably far-sighted. He identified how information advantage must be seen as a means to an end rather than an end in itself:

> *It's one thing to have highly technical, sophisticated observation platforms that operate in space, in the atmosphere or operate on the sea. But if you can't use the information in a timely manner, it's wasted.*

Likewise, as the US advanced into the information domain, Fogelman warned of the physical, technical and psychological weaknesses this exposed: 'As an information-intensive service, we are vulnerable to others exploiting our networks and our data bases. So we must protect these critical assets.' Further, prompted by the unanticipated sophistication of the US's competitors in Iraq and Somalia, Fogelman cautioned that the information domain was likely to become an increasingly crowded space, and that the US must not become complacent or think that its technological pre-eminence made it the sole, or the best, player in the game: 'we run a tremendous risk if we look at information warfare only as a unique American advantage. It is not.'[79]

However, despite these doctrinal innovations and the US military's unparalleled technical advantages, it struggled to derive strategic advantage from its domination of the information space. The US Army and the USAF may have known what information operations were, but in the late 1990s the organisational challenges identified by Arquilla and Ronfeldt were beyond them. They, and their allies, lacked the bureaucratic systems needed to implement a fully integrated joint force civil–military information offensive. Their collective failings were graphically illustrated during Operation Allied Force. Launched on 24 March 1999, and conducted exclusively through air power, Operation Allied Force was a humanitarian intervention intended to halt Serbian efforts to drive Kosovo's ethnic Albanians from their homes and villages. With an extended build-up to hostilities, and many years of the Yugoslav Civil War already behind it, NATO was aware of the need to project its message to both domestic and international audiences, allies and competitors, and so it prepared itself for an information war. Long before the first bombs fell over Serbia and Kosovo, the US and its 18 partner militaries had 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'.*[80]

However, their efforts were undermined by the military's reluctance to arm its public affairs and media relations staff with the information they needed to prosecute the NATO case. Though the contributing members of Operation Allied Force had varying views on what information could be released and how they should interact with the media, their efforts to balance 'political sensitivities and security concerns against the need to tell the "NATO story"' meant that 'the alliance (in concert with the Pentagon) eventually adopted restrictive policies on the release of information'.[81] The Pentagon's ground rules for the media in Kosovo stipulated that 'specific information on friendly force troop movements, tactical deployments, and dispositions could jeopardize operations and endanger lives. Therefore, release of some information will be denied or embargoed'.[82] Further, the policy limited the media's contact with the mission's senior officers on the basis that 'this would allow them to focus on their wartime duties while still maintaining a unified "alliance" message'. As a consequence, when the operation got underway in late March 1999, not only was information flow from the area of

operations reduced to a trickle but also the only senior officer 'authorized to conduct media interviews in the area of responsibility' was the one with the least time to do so, the Supreme Allied Commander Europe, General Wesley Clark.[83] Burdened by his many duties and responsibilities, Clark had little time to spend on the fourth estate.

The military's decision to err on the side of information constraint was, in part, a response to the changed media landscape, in particular the proliferation of 24-hour news services, spawned by CNN's spectacular ratings and financial success during the First Gulf War:

> *By 1999, cable subscribers in many American cities could choose from as many as nine different news and information channels … CNN, the pioneer in cable news, had no fewer than six information channels on the air when Allied Force began.*[84]

NBC invested heavily in coverage of the war. Its news division supplied content for three separate networks, most prominently MSNBC, the cable channel it co-owned with Microsoft. The decision to dedicate almost the entirety of MSNBC's coverage to Operation Allied Force paid dividends, bringing a 103 per cent increase in its ratings. As the *Washington Post*'s Howard Kurtz noted, this was not an isolated case. Both CNN and Fox News Channel, who each offered extensive coverage and analysis of the war, saw their ratings multiply by, respectively, 82 and 38 per cent.[85] If the news providers' blanket coverage of the fighting made them more attractive to advertisers, it had the opposite effect on the military. In the eyes of the Pentagon, this crowded and competitive field, and the colossal demand for content that it stimulated and fed, had resulted in 'much less respect in the media for protecting operational information'. As a consequence, Pentagon spokesman Kenneth Bacon reported:

> *Secretary of Defense [William S] Cohen and [Chairman of the Joint Chiefs of Staff Henry H] Shelton did make a conscious decision in the early days of the war to take a very conservative approach in releasing information. They felt we had gotten too lax in dealing with operational security.*[86]

As such, at the very moment when there had never been more outlets on the air for a longer duration, when there had rarely been more journalists at home and abroad chasing down every scrap of news from the world's biggest story, the military choked off the flow of information and the media

were forced to look elsewhere for the material to fill their 24-hour news schedules. It was a spectacular own goal.

When the British had taken a similar decision during the Falklands War in 1982, reducing the release of official information from the Ministry of Defence to one, later two, official communiques per day, the media had set off in a panic, desperate to turn up any information they could. The results of their pursuit were part embarrassing, part potentially catastrophic. Latin American news sources, though openly hostile to British claims, brought the gold dust of images from the occupied islands. Widely utilised and quoted at length, they furnished a ready channel for Argentine propaganda. Retired military men were drafted on to news analysis programs and invited to speculate on how and where the British task force, sailing south at that moment, might best put troops ashore—which some did with prescient accuracy. One defence columnist, starved of any hard news to unpack, instead opined on the most likely place for a British beachhead. In doing so, weeks before the first troops came ashore, he inadvertently identified in a national daily newspaper what was at the time the military's most closely guarded secret: the precise location of the British landing ground. The task force was saved from potentially catastrophic losses by good luck and Argentine military ineptitude. It had been imperilled by a deficient communications policy which directly resulted from the military's reluctance to release information to the media.[87]

In the light of the armed forces' reluctance to provide a ready flow of information from the battlefront, NATO public affairs went on the attack, launching an aggressive 'media saturation strategy' through which it sought to control the news cycle by almost permanently occupying it:[88] 'our credo at NATO', Spokesman and Deputy Director of Information and Press Jamie Shea, recalled, 'was just to be on the air the whole time, crowd out the opposition, give every interview, do every briefing'. That is exactly what they did:

> *We had an MOD briefing from London late in the morning, and just as the audience was switching off from that, on came the 3 P.M. briefing (from NATO), and as soon as the 3 P.M. briefing was off air, up jumped the Pentagon, the State Department, and the White House. 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 acknowledged that both the timing and the form of the NATO briefings were tailored to the needs of the news channels:

> *It suits CNN or BBC World Service to have a daily show …*
> *They have a lot of space to fill, and they want to do it cheaply.*
> *The best way of filling an hour virtually cost-free is to put NATO's daily briefing on the box.*[89]

According to PJ Crowley, who was seconded from the US National Security Council to work on NATO's public affairs effort, the success of the strategy was measured by the hours of screen time it occupied: 'Between our three daily briefings, we were able to command 18 hours of the 24-hour news day.'[90] Jamie Shea agreed: 'the one thing we did well in the Kosovo crisis was to occupy the media space'.[91]

Yet quantity was only one of the elements on which the success or failure of the saturation strategy rested. The information NATO provided also had to be timely and good.[92] While its interviews and briefings certainly dominated the news cycle, Crowley's claim that, as a result, 'The media dwelt more on our information than it did on Belgrade's' does not stand up to scrutiny.[93] Many in the media were not only irked by what NATO did not tell them; they put little faith in the information that they were given. In a context where 'the military's attitude is "We'll tell you what you need to know"' the *New York Times*'s Bernard Trainor claimed that information from official sources could not be trusted: 'the media manipulation got so transparent that I didn't believe anything Jamie Shea or Ken Bacon had to say'.[94] Further, NATO's most senior personnel, from Secretary-General Javier Solana down, recognised that it didn't matter how abundant or timely your information was if nobody read or saw it—it had to be compelling enough to demand the public's attention. Here NATO faced a core problem. Alastair Campbell, British Prime Minister Tony Blair's press secretary, who was drafted in to help sell the NATO message, observed that winning the media war 'required two things. We had to justify the action, show we had right on our side. And the military action had to be seen to be effective'.[95] That is to say, NATO had to make the virtue of its cause visible. Thus, NATO was competing with the Serbs for the exposure that the front page and the top of the bulletin brought.

While moral virtue was important, what mattered above all else in this competition for visibility was newsworthiness, and in the context of Operation Allied Force, the currency of newsworthiness was images. Here, NATO was in a double bind. If the military's reluctance to pass on information was not enough of a handicap, the airborne nature of the operation exacerbated the situation. Without boots on the ground, NATO had no credible sources on the spot who could collect images attesting to the systematic human rights abuses committed by the Serbs in Kosovo or the effectiveness of the air campaign in combating them. Almost all of the reporters from NATO countries had been expelled from Serbia within 48 hours of the commencement of hostilities. After CNN and others secretly filmed the first NATO bombing raids on Belgrade from the roof of their hotel and later broadcast the green-tinged night-vision of the resulting impacts, Serb authorities broke into the journalists' hotel rooms, damaged their equipment and took them into custody.

> *The next morning, having been ordered to leave the country, members of the [CNN] crew were physically accosted before watching their remaining equipment smashed again … According to a New York Times report, crowds of Serbian passers-by cheered at the sight, while frightened fellow journalists watched from the relative safety of the hotel's lobby.*[96]

> As Justin Raimondo noted, this response was hardly a surprise:

> *[T]hose Western journalists who have placed themselves and their profession in the service of Allied Force should not be too surprized to find that the people they have demonized are less than hospitable.*[97]

In the eyes of the Serbian regime and many of its people, Western reporters had not merely covered the NATO bombing raids; they represented the information arm of the same offensive and were thus regarded as 'part of the whole attack structure'.[98]

With the Western reporters deported, the ground belonged to the Serbs, and with it the opportunity to gather, deploy and, through the enemy's own media channels, promote visual 'evidence' best suited to advance their narrative of outraged victimhood. Mustering the NATO media arsenal to combat the Serbian information offensive, Alastair Campbell reflected that efforts to press the NATO cause brought it into conflict with not only Serb media manipulation but also traditional Western news values:

> *Our enemy was Milosevic's media machine but our judge and jury was the Western media. Their editorial decisions over which pictures to run, whether to run them, and how prominently, were of considerable influence. And it was not balance, surely, but competition, and common denominator news judgement, that drove broadcasters to put Milosevic's pictures of 'NATO blunders' at the top of their bulletins, and it was our job to try to provide competing stories, pictures and arguments.*[99]

As such, despite the omnipresence of NATO spokespeople on the world's television screens, the alliance's failure to gather credible and timely images of Serb atrocities or coalition successes on the ground meant that it suffered a humiliating defeat in the information war. As Jamie Shea remarked: 'Milosevic was the aggressor but he used the Western media to portray himself as the victim.'[100]

Along with NATO, the British and US governments sought to compensate for their lack of physical presence in Kosovo by supplementing their omnipresence in the mainstream media with an aggressive presence online. The Prime Minister's Office, the Foreign and Commonwealth Office, the White House and the State Department each used their websites to publish transcripts of speeches, press releases, briefings and communiqués, and to feature maps, charts and other data promoting their accounts of events in the region. The Serbian government made similar use of its own official websites. The hostility being played out in the airspace over Serbia and on the ground in Kosovo found its echo in the virtual world of cyberspace. After NATO bombs targeted Serbia's broadcast and transmission facilities, the internet 'was perhaps their only weapon of retaliation'.[101] Serb hackers attacked NATO and British and US government websites using a range of tools including distributed denial of service (DDoS), spam, ping bombardment and the more primitive, if effective,

method of sending a stream of emails with massive file attachments that clogged NATO's email system.[102] As Matheson and Allan note: 'These forms of "cyber-terrorism" were surprisingly successful.' Not only was the NATO website 'the first cyber-casualty' but the websites of the US Department of Energy, the Department of Defense and the White House were also defaced and disabled.[103] Yet whatever the legitimacy of describing the Kosovo campaign as the 'first internet war', it is important to consider how little internet penetration there was in the former Yugoslavia at the time:

> *Only about 1 percent of the population in Serbia and Kosovo was able to get online and those that could were overwhelmingly urban and educated. Net access in Kosovo was far scarcer than in Belgrade and in the rural areas where the Serb forces were pursuing their ethnic cleansing it was almost non-existent.*[104]

Despite this, Phil Taylor argues that though the internet 'was not a decisive factor in the conflict … it was a new one', and that 'with comparatively limited resources a widespread global impact' had been achieved.[105]

Whatever the lure of the information domain, in its determination to control the flow of information about the war, NATO directed the greater portion of its resources to more traditional military methods. This was manifest in its air attacks on Serbia's civil and military communications systems, most notably in the airstrike on Radio Television Serbia's headquarters on 23 April 1999 that killed 16 journalists. While the attack was widely condemned by international journalists' organisations, the Chief of Joint Operations at the Ministry of Defence, Admiral Sir Ian Garnett, argued that Milosevic's 'propaganda machine consists of transmitters but also the studios from which the information is transmitted. That makes it part of the overall military structure. Both elements have to be attacked'.[106] Clearly, at this point in the development of the internet, cyberwar was still conducted by way of brutally old-fashioned means.

Despite their relative powerlessness, the Serbs ran a sophisticated information campaign, fighting a model asymmetric campaign, turning NATO's greatest advantage, its overwhelming military superiority, into its principal vulnerability by exploiting its communications weaknesses.[107] In its efforts to contain Serb aggression and prevent Kosovo's ethnic Albanians from being driven from their homes and villages, NATO aircraft flew thousands of sorties and dropped tonnes of explosives on Serbian

power stations, bridges, government buildings and military formations.[108] Jamie Shea maintained that the vast majority of this ordnance found its mark:

> *In Operation Allied Force, NATO dropped 23,000 bombs, whereas only 30 were misdirected and failed to hit the intended target accurately. This is a fraction of 1 percent, a degree of accuracy that has never been achieved before. The paradox here is that as the weapons become more accurate, the media and public opinion in general are all the more shocked when things go wrong, as inevitably they do in warfare. The incredible 99.9 percent success story is ignored; the 0.1 percent or failure, statistically insignificant, becomes the central drama of the conflict and the yardstick for judging NATO's military and moral effectiveness.*[109]

The Serbs exploited these failures to the full, putting images of the destruction caused by the 0.1 per cent of inaccurate ordnance at the heart of its information campaign. Photographs and moving pictures from what were in truth tactically trivial episodes dominated international media coverage of the war and were used by Milosevic's information ministry to build a picture of a superpower and its allies indiscriminately bombarding defenceless Serbian civilians:

> *Milosevic, who controlled the pictures, could show the western media the pictures that he wanted them to see of NATO's collateral damage and make sure that none of the pictures that would have embarrassed him, the real pictures of the war, the atrocities, the mass graves, the burning houses, were never filmed or were never released because of censorship.*[110]

Looking back on the information war in the Balkans, the Commander of Allied Forces in Southern Europe, Admiral James Ellis, conceded:

> *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.*[111]

The Djakovica incident offers a striking case in point. On 14 April 1999, USAF F16s attacked a convoy of tractors evacuating ethnic Albanian Kosovars near the village of Djakovica, mistaking it for a Serb armoured

column. Dozens of civilians were killed. Apprised of the attack, the Serbian Ministry of Information immediately offered free transport to the site to the Western journalists who had remained in or returned to Serbia. One journalist who took up the offer, CNN's Alessio Vinci:

> *filed graphic reports from Djakovica, featuring gruesome images of burned and bloodied corpses scattered among bombed out vehicles. Video footage from the scene led evening newscasts in the United States and Western Europe; equally searing still photographs from the scene received prominent play in subsequent editions of* Time*,* Newsweek *and hundreds of newspapers around the world.*[112]

Over the next five days CNN featured more than 60 reports on the episode. The incident was page one news in the *New York Times*, 'Civilians Are Slain In Military Attack On A Kosovo Road', with a second news analysis piece, also above the fold on the front page, subheaded 'Bombings By NATO May Be Destabilising A Region Where Peace Has Cost So Much'.[113] While there is no question that this was a tragic and highly newsworthy incident, Shea argues that in terms of 'the real story' of the war in Kosovo it was insignificant:

> *The media is primarily interested in the instantaneous image, which becomes the reality of the day. In other words they are interested in news and the problem here is that news is often not important or rather because it is news does not mean to say that it its [sic] always important. The Djakovica convoy incident in which perhaps 10 to 20 people died became the dominant news story for five days. During those five days 200,000 people were expelled from Kosovo. Was that not more newsworthy than the 10 to 20 people who died because of a NATO accidental strike against a convoy? I would argue that it was. It was much more intrinsic to the real story of what was going on inside Kosovo. But why did the media not report that? Answer—no pictures. And this is a fundamental lesson that we are going to have to learn. It is quite simple: no pictures, no news. In other words I, as NATO spokesman, everyday was using thousands of words to explain what was going on. I was talking about atrocities, about summary executions, about lootings, about house burnings, about rapes; I was talking about identity thefts of people's documents. None of that was believed because I could not present the photographic evidence.*[114]

Shea's difficulties were compounded by NATO's bungling news management of the incident. The initial response from General Wesley Clark blamed the Serbs for the attack, while Pentagon spokesman Ken Bacon claimed 'we only hit military vehicles'.[115] As increasingly graphic images from the scene flowed in, all that NATO could offer were evasions. Dana Priest of the *Washington Post* observed that 'NATO officials obfuscated about operations while evidence accumulated that NATO bombs accidentally killed civilians'.[116] In *Newsweek*'s opinion, the fact that NATO 'couldn't get its own story straight … hurt its credibility far more than Milosevic did'.[117] Finally, five days after the episode, Brigadier General Dan Leaf of the USAF, whose planes had dropped the ordnance and who had led the official enquiry into the incident, fronted a packed press conference in Brussels to explain what had happened. After detailing the chronology of the bombing and the challenges pilots faced in distinguishing ground targets, he conceded that 'it is possible there were civilian casualties'.[118] The whole episode was a public relations catastrophe. No wonder Shea was such a busy man.

However 'insignificant' the event itself, or the casualties at Djakovica, they had concrete operational outcomes. In the wake of the convoy bombing, NATO cancelled daytime sorties, leading Wesley Clark to observe that 'The weight of public opinion was doing to us what the Serb air defence system had failed to do: limit our strikes'. In retrospect, he conceded: 'The war was almost as much about public opinion as it was about the destruction of targets in Serbia.'[119] As Thomas Rid noted: 'The line between military action and the coverage of military action was increasingly blurred.'[120] Despite its crushing military superiority, NATO took a beating in Kosovo. While its air forces were well equipped to destroy targets in Serbia, its information assets were not nearly as well organised or calibrated for their public affairs or information operations missions. Though it ultimately achieved its military objectives, with the capitulation of Serbian President Slobodan Milosevic and the withdrawal of Serbian forces from Kosovo in June 1999, in information terms the operation was a failure, exposing how ill-prepared for war in the cognitive domain NATO and its constituent militaries were. While NATO overvalued its own information capabilities, it seriously underestimated those of its enemy and paid the price in ignominy and lost prestige.

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'.[121] Indeed, militaries cannot do one without the other. In order

to win the media campaign, it is not enough to dominate the information space; militaries need to exercise effective control over it. To do this, they need to set up a fully integrated information operations organisation and ensure that it is functioning optimally and that it is directed to deliver a commonly understood information strategy. At ground level, they need to agree on and consistently promote their core narrative; they need to source an adequate supply of images to support it; and they need to get these images out to the media and the public in a timely fashion. NATO signally failed to achieve any of these aims, not only because it was unable to collect images on the ground to support and advance its narrative of the war but also because it failed to set up an organisational apparatus that was fit for purpose and had no information strategy to direct it.

While military restrictions on information release starved public affairs of the material they needed to promote NATO's cause—even Brigadier General Leaf felt that the military 'could have been more accessible without giving away the farm'—a bigger problem lay in entrenched differences of opinion about the appropriate tools, channels and audiences for particular kinds of information held by different branches of the information division.[122] Specifically, military public affairs officers (PAOs) were, in many cases, ambivalent about getting involved in an information operations (IO) campaign. Despite the preparations for the operation, which saw dedicated IO cells established within many partner militaries in the months leading up to the outbreak of hostilities, the USAF's attempts 'to integrate public information into IO planning … eventually came to naught', thus 'preventing the implementation of IO initiatives based on public information'.[123] The PAOs' ambivalence arose from their fear that putting public information at the service of information operations, with its links to propaganda, psychological operations, misinformation and the other black arts of communication, would damage the reputation for trustworthiness on which its operations depended.[124] Lieutenant Colonel Barbara Carr, USAF Europe's Deputy Director of Public Affairs during Operation Allied Force, summarised these concerns:

> *A PAO's credibility is essential. Once lost—in reality or perception—word spreads through the media in record time. And that PAO (and sometimes other PAOs in the vicinity who get painted with the same brush) can no longer function effectively in his mission. We need to be very careful on how our role in IO is articulated. I wouldn't say participating in IO puts us on a 'slippery slope,' but the potential is there.*[125]

Her view was underlined by the military's own internal structures at the time, where 'a detailed institutional division of labor has evolved' between public affairs (PA) and IO personnel.

> *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.*[126]

Despite these profound cultural oppositions, the Deputy Director of the USAF's Public Affairs Centre of Excellence, Colonel Jack Ivy, argued that Carr's concerns were unfounded, and that one could and should deploy truth-based public information as an information operations asset. One could because 'truth-based public-information efforts represent the best of both worlds, allowing full integration of public information into the IO campaign without sacrificing the credibility and integrity of the PAO'. One should because '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'. To exercise one's scruples and vacate the field, Ivy argued, is to surrender it to the enemy, and this is not an option open to any military intent on victory.

Ivy's designation of public information as a battlespace generated fierce debate within the PA community. PJ Crowley thought it had 'dreadful implications', dangerously weaponising the information space: it 'establishes our own press as antagonists and the enemy media as possible targets', thus setting the stage for 'an adversarial relationship with our own reporters and potential retaliatory action against Western journalists in enemy territory'.[127] It was a prophetic observation, as America's return to Iraq in 2003, and the wholesale weaponisation of information that this brought, would prove.

Chapter 3: Afghanistan and the Second Gulf War

Going back into Iraq in early 2003, the US armed forces were acutely conscious of how effectively Saddam Hussein had used disinformation to counter their military superiority in 1991. This time, they were determined to neuter his information assaults by taking the media with them into battle to provide objective verification of claim and counter-claim. As James DeFrank, Director of Press Operations at the Pentagon during the Second Gulf War, observed:

> *We knew from our previous experiences in dealing with [the Iraqis] that they lied, that they staged events, that they distorted the truth. We all believed that the truth was our friend: the truth was on our side. There was nothing that we could do that would be as bad as what they were trying [to] say we did. Skeptics around the world, but particularly in the Arab world, would be predisposed to believe the Iraqi side rather than us. What we needed were credible, third party observers present with us, and so we started talking about including media.*[128]

At the time that DeFrank and others in the Secretary of Defense's office were contemplating whether and how to bring the media aboard, officers in the field in Afghanistan were being reminded why they needed them. Over the first year of Operation Enduring Freedom, military operations and their media aftermath had settled into a familiar pattern. As Terry McCreary, Special Assistant for Public Affairs to the Chairman of the Joint Chiefs of Staff, described it:

> *You'd raid a camp, there wouldn't be any press with you, you do an operation, you leave, the enemy comes back, the press come in, and everybody tells them you murdered innocent people, you slaughtered them, and that becomes the story for the next 48 hours until you can fix it.*

In the face of the Taliban's ability to exploit the US's weakness in the information domain, setting the news agenda and forcing the US to react and play catch-up, it became clear that the military needed a credible information source with them in the field:

> *The only way you can counter deception was to have the truth told first. The only way to do that is have an independent truth-teller tell it first. The only way to have an independent teller tell it first, is to have them with us. And the only way to have them with us was to embed.*

According to McCreary, Afghanistan was 'the watershed event' that finally pushed the military to realise that, whatever their misgivings about the media, they had to bring them along because they could not do without them.[129] Yet it was a lesson that the armed forces were slow to learn.

In the wake of its bruising experience in Kosovo, the US military was determined to maintain tight control over the message, offering the media a semblance of cooperation rather than the substance of it. Bringing journalists close the action but denying them access to it only served to strain military–media relations. When Operation Enduring Freedom was launched on 7 October 2001, none of the correspondents who had been transported to forward Air Force bases in the region were allowed to travel beyond the wire to report on the rolling back of the Taliban. Worse off were the reporters aboard the US naval vessel USS *Carl Vinson*, from where many of the air strikes on Afghanistan were launched. Not only were they unable to cover the bombing attacks; they had to wait more than

20 hours before they could file the copy or broadcast the footage they had shot. Their editors were not impressed. Robin Sproul, ABC's Washington bureau chief, politely observed that while 'It was a good start to get us on board those ships … we're very interested in getting access to U.S. troops wherever they are'. The *Washington Post*'s assistant managing editor for foreign news, Phil Bennett, was more forthright: 'We have basically had no access except for [*Washington Post* reporter Steve] Vogel on a ship in the Indian Ocean.' In his view, bringing reporters physically close to the action but not allowing them to witness it, interview the troops involved or report on it, was a recipe for unhappy journalists and poor coverage. The access they were given 'rarely yields the kind of information we think is decisive to understanding the scope, nature or success of the operations'.[130]

In an effort to bring the media closer to the action, on 20 October 2001, the day after the war's first major ground operations, the Pentagon provided a briefing for reporters that included exclusive vision of a Special Forces raid on Mullah Omar's compound captured the night before by a combat camera crew. The military's substitution of independent media coverage with footage taken by uniformed combat camera teams caused consternation. At this point the campaign was almost exclusively a Special Forces and Air Force bombing operation, but with conventional forces slated to arrive in numbers over the coming weeks, arrangements for the media suddenly became a critical issue. Pressure to embed the media with troops came both from media bureau chiefs and from the military, with the US Marines pressing hardest of all. Major General Andrew Davis, Director of Marine Corps Public Affairs at the Pentagon, persuaded his superiors to approve the embedding of reporters with the 15th Marine Expeditionary Unit which, when it landed south of Kandahar on the evening of 25 November 2001, was the first conventional force deployed in Afghanistan. The presence of embedded journalists had spectacular results. Reports on the Marines 'skyrocketed with more than 350 individual news stories in two months featuring the Marines in Afghanistan'.[131] The Army were not far behind, but they remained cautious. The embed they arranged for Donatella Lorch of *Newsweek* sent her to Mazar-i-Sharif *after* the fighting there had finished. According to Sean Naylor of the *Army Times*, the Special Forces unit she joined had been 'carefully chosen' specifically because 'not much happened on those missions'.[132] In March 2002, the Army extended its commitment to embedding when it hand-picked a small number of reporters to cover Operation Anaconda, the major offensive against remnant Al Qaeda and

Taliban fighters in the Shah-i-Kot Valley. If the mission did not go entirely as planned, in the eyes of the Army the embedding exercise had been a success. US Army Public Affairs Officer Colonel Melanie Reeder, who had served in Afghanistan, noted that the principal value of having the reporters on hand was the veracity they brought: 'When journalists were provided access, the accurate story was told. When they were not provided with information, the result was speculation, misinformation, and inaccuracy.'[133] Although the embedding experience in Afghanistan was underpinned by official ambivalence, given that 'Only a small group of journalists was embedded' and 'the responsible officers were still in a reluctant and insecure experimentation mode', in Melanie Reeder's view its effects were far-reaching: 'the eight embedded reporters in Operation Anaconda helped blaze the path for a large-scale, Secretary of Defense-dictated, embedded-media program in Operation Iraqi Freedom'.[134]

As a result, on 10 February 2003, little more than a month before US forces and their allies in the 'Coalition of the Willing' invaded Iraq, the Secretary of State for Defense issued the *Public Affairs Guidance on Embedding Media during Possible Future Operations/Deployments in the U.S. Central Commands [sic] (CENTCOM) Area of Responsibility (AOR)*.[135] The guidance detailed the duties and responsibilities that the military and the media owed one another, laid out in more detail in the regulations governing access to, freedom of movement within, and review and transmission of copy from the area of operations. The document begins by outlining the principles on which its specific stipulations rest: the conviction that a ready supply of trustworthy information from the area of operations is not only the most reliable means of combating the distortions of truth on which tyranny rests but also advertises the US military's commitment to democratic values:

> *Our ultimate strategic success in bringing peace and security to this region will come in our long-term commitment to supporting our democratic ideals. We need to tell the factual story—good or bad—before others seed the media with disinformation and distortions, as they most certainly will continue to do. Our people in the field need to tell our story—only commanders can ensure the media get to the story alongside the troops.*[136]

In order to effect this, commanders were directed to 'Ensure the media are provided with every opportunity to observe actual combat operations'.[137] To that end they were required to provide 'Seats aboard vehicles, aircraft and naval ships' and, 'To the extent possible', make available 'space on military transportation … for media equipment necessary to cover a particular operation'.[138] Scarred by the failures of the pony express system during the First Gulf War, the public affairs guidance (PAG) recognised that having the media on hand to get the story was of no use if they could not then transmit their material to their editors and on to the public. Accordingly, military units were instructed to:

> *plan lift and logistical support to assist in moving media products to and from the battlefield so as to tell our story in a timely manner. In the event of commercial communications difficulties, media are authorized to file stories via expeditious military signal/ communications capabilities.*[139]

In an effort to avoid impediments to timely filing, to move the onus for information security from the media onto the military and, in the process, to rebuild a degree of mutual trust between the military and the fourth estate, it was determined that:

> *Media products will not be subject to security review or censorship … Security at the source will be the rule. U.S. military personnel shall protect classified information from unauthorized or inadvertent exposure. Media provided access to sensitive information, information which is not classified but which may be of operational value to an adversary or when combined with other unclassified information may reveal classified information, will be informed in advance by the unit commander or his/her designated representative of the restrictions on the use or disclosure of such information.*

Even in the face of disputes about sensitive information or its release, the PAG affirmed, 'Media products will not be confiscated or otherwise impounded'.[140]

The principal goal of the PAG was to level the playing field in the fight against undemocratic regimes, for whom public information was merely another arm of state power. By guaranteeing the media 'long-term minimally restrictive access to U.S. air, ground and naval forces' the PAG recognised the potency of information as both a shield and a weapon:

> *Media coverage of any future operation will, to a large extent, shape public perception of the national security environment now and in the years ahead. This holds true for the U.S. public; the public in allied countries whose opinion can affect the durability of our coalition; and publics in countries where we conduct operations, whose perception of us can affect the cost and duration of our involvement.*[141]

If the PAG guaranteed a constant stream of bottom-up information flowing from the area of operations, the US and British governments worked in close cooperation to maintain top-down control over the war's strategic narratives and micro-messaging. Their coordination grew out of the arrangements established during the invasion of Afghanistan in October 2001. Then, Alistair Campbell had worked with Bush aide Karen Hugh to establish Coalition Information Centres (CICs) in Washington, London and Islamabad to ensure that the coalition could 'get the message across at all times of the news cycle'.[142] After the invasion of Iraq, the CIC in Washington returned as the Office of Global Communication (OGC), once more working in close cooperation with other arms of the US government and with Blair's office in London to make sure that they all 'sang from the same hymn sheet'.[143] The coordination began with Ari Fleischer, the White House Press Secretary, 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 director Tucker Eskew—a routine that mirrors procedure during the conflict in Afghanistan.*[144]

From the White House, the message 'cascaded down to the rest of the propaganda apparatus'.[145] The specific role of the OGC in this process 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” e-mail containing talking-points and ready-to-use quotes’. As a consequence, wherever they were in the world, the US, British and global publics received a consistent set of messages about the war 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 … The later in the day, they’ll hear from the Pentagon, then the State Department, then later on the White House will brief.*[146]

As Miller notes, 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 CIC 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, the propaganda apparatus comprised four main elements:

> *First was the external system of propaganda run by the Foreign Office and co-ordinated by the Public Diplomacy Policy Department. Second was internal propaganda focused on the alleged ‘terrorist threat’ co-ordinated 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 are said only to target enemy opinion to break resistance.*[147]

In the face of the actions of the OGC, the CIC and their subordinate actors, it is clear that by 2003 the formerly strict division between public affairs, intended to provide domestic audiences with a truthful account of the nation at war, and psychological operations, purposed to influence competitor thinking and behaviour, was collapsing. The fact that public information might be used to influence foreign audiences as well as to inform domestic publics, while operations intended to shape competitor thinking might just as readily influence domestic audiences, had been a perennial source of tension between public affairs and information operations personnel. Indeed, the experience during Operation Allied Force demonstrated that these unresolved tensions had prevented the US military and its allies from optimally deploying their information arsenals in the fight against Serbia.

As the PAG indicates, by the first decade of the 21st century the firewall between the truth-based public information it provided to its own people and the influence material it directed at the public in antagonist and neutral states had become increasingly porous. Putting to one side the deliberate efforts of the US and British governments to justify their forthcoming invasion of Iraq by portraying it as harbouring WMD and so an imminent threat to domestic security, the traditional controls over the distribution of national press and broadcasting products that had enabled a strict separation between domestic and foreign consumption were giving way in the face of technological advances and the market innovations they brought. The silicon chip, the mobile communications revolution and the near-universal spread of digital platforms it enabled meant that efforts to quarantine foreign from domestic audiences were pointless. By early 2003, just as defensive public information targeted at a domestic audience could be picked up by and influence foreign audiences, so offensive information operations, calculated to manage the perceptions of competitor and foreign audiences, could readily loop back to influence domestic audiences. Shock and awe flowed in both directions.

Over this period, militaries struggled to ensure that doctrine kept abreast of rapid technological advances, the new capabilities they made available and the ways in which they reshaped the contemporary battlefield. By the turn of the century, there was consensus across the US military, driven home by the chastening experience of Operation Allied Force, that information was not only a key battlespace but also an increasingly potent weapon of war. Its understanding of how this weapon could and should be used,

where it might most usefully be directed and with what effects, significantly deepened over a relatively short span of time. As early as 1997, the USAF's *Basic Doctrine* acknowledged that 'Dominating the information spectrum is as critical to conflict now as controlling air and space was in the past'.[148] When this doctrine was revised in 2003, it demonstrated both a more sophisticated grasp of the battlespaces specific to information operations and a more nuanced understanding of the contested assets that had to be targeted and controlled to ensure information advantage. The revised doctrine proposed that information operations, the 'action taken to affect competitor 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'.[149] While electronic warfare operations focused on control of the electromagnetic spectrum, namely radio frequencies and optical and infrared regions, network warfare operations focused on the struggle over the 'collection of systems transmitting information' including 'radio nets; satellite links … telemetry … telecommunications; and wireless communications network systems'. If dominating these systems enabled militaries to control the electromagnetic battlespace and the channels which operated within and across it, influence operations took place in the 'cognitive battlespace' where, shifting the focus from hardware to the human, the aim is to sway thinking and shape behaviour:

> *Influence operations employ capabilities 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 competitor's decision process, which aligns with the commander's objectives.*

That is to say, militaries see influence operations as a means of getting into the heads of the enemy, changing the enemy's thinking, sowing uncertainty, doubt and disillusionment, undermining the enemy's will to fight and thus imposing their will on their competitors by means other than violent force.

The principal tools of influence operations, according to the revised doctrine, are 'counterpropaganda operations, psychological operations, military deception, operations security, counterintelligence operations and public affairs operations'. The inclusion of public affairs operations in this list reflects the established perception among information operations professionals that public affairs should be regarded not as separate to but as a subset of information operations. If the role of psychological operations and military deception was to mislead competitor forces into acting in ways contrary to their interests, the purpose of public affairs was to ensure that the morale of domestic audiences was kept strong and defended by equipping commanders with the means to:

> *convey information and indicators to audiences; shape the perceptions of decision makers; secure critical friendly information; protect against espionage, sabotage and other intelligence gathering activities; and communicate unclassified information about Air Force activities to the global audience.*[150]

These assumptions were given practical effect during the Second Gulf War when the PAG, and the embedding policy it enabled, conscripted correspondents into the service of the military's information assault and weaponised their reporting. Just how important a weapon information was in the assault on Iraq is reflected in the number of embed places the coalition military made available to the media, the breadth and multinational provenance of the news outlets who took them up, and the pains taken by the armed forces to ensure that their dispatches were transmitted in a timely fashion. Among the 2,300 journalists reporting from Iraq in March/April 2003, almost 700 were embeds representing the television networks, cable providers, newspapers of record, and local press, as well as a range of popular magazines including *Esquire*, *Rolling Stone*, *Men's Health* and *People*.[151] While the majority of these embedded reporters were American, British and French:

> *Nearly a quarter of all embed slots (24.4%) were designated for international media, defined as intending to serve audiences in more than one country. Another 13.9% of embed slots went to media organizations serving the domestic audiences of foreign countries.*

Among these, media organisations from within the region were prominent: 'eight media outlets from seven Arab countries received thirteen embed slots'.[152]

Susan Brockus argues that for the US military, the purpose of embedding was focused less on third-party verification of events than it was on persuasion:

> *The embedding of reporters with military units put journalists in a position of obligation to the U.S. government for both access and safety, a situation that limited both coverage and perspective. The journalists lived, travelled and identified with the troops … Rather than illuminating the scope and ramifications of the invasion of Iraq, individual embed coverage thus tended to humanize the troops and emphasize the importance of the coalition's mission for the American public.*[153]

Putting reporters in close proximity to the troops they were purportedly observing not only engendered empathy for them but also brought 'reporters' and soldiers' perspectives into complete alignment. As a result, civilian audiences in the US would also apprehend the war through the military's sights: a spectatorial position that would enhance popular support for the invasion and occupation of Iraq'.[154] While this sort of coverage might have brought the public on side with the military's assumptions and perspectives, it underpinned the 'bad reporting and editing' that Thomas Ricks points to as one of the causes of the disaster in Iraq.[155] Just how intrinsic the media were to the military's attainment of its strategic goals in Iraq, and how much it invested in ensuring that the media continued to echo the top-down narratives from Washington and London, was illustrated by its treatment of two marginal groups: unilateral reporters who elected to operate beyond the embed system, and news organisations who remained within it for a period of time but whose loyalty the military questioned.

From the earliest days of the conflict, Al Jazeera adopted a defiantly Arabist perspective on the fighting and its consequences. With its network of reporters spread out across Iraq, it had no need to rely on CENTCOM briefings for its information.[156] The tagline for its television coverage, 'War on Iraq', subtly shaded the BBC's 'War in Iraq'. In keeping with this viewpoint, 'the decision was made to fill the [Al Jazeera] website with stories and features based on themes that reflected the concerns on the

Arab street rather than of western politicians'. Its coverage focused on 'The humanitarian fallout of the invasion … civilian casualties, toxic waste from depleted uranium, refugees, ethnic and sectarian civil strife, and the further marginalisation of the Palestinians'.[157] Both the focus and the nature of this coverage attracted fierce criticism in the West. The American press dismissed Al Jazeera's reports as 'evidence of its ideological bias'. Yet there was clearly an audience for its coverage. Its Arabic-language website saw a tripling of its traffic over the course of the invasion, while over the same period both 'Google and Lycos search engines reported that "Al Jazeera" had become the most common search term entered by web surfers, with three times more searches than "sex"'.[158] Americans were prominent among those flocking to Al Jazeera online. A Pew Internet and American Life Project study from 1 April 2003 revealed that 'in the conflict's first six days, 10 percent of American internet users visited foreign news websites'.[159] Such popularity did not go unnoticed, or uncontested. Soon after, Al Jazeera's US web host cancelled its contract and the company had to relocate its US accounts to a host in Europe. In late March 2003, the Al Jazeera website was hacked and subjected to a DDoS attack 'that kept its English-language site unavailable throughout most of the war and knocked down its Arabic-language site for almost a week'.[160]

While Al Jazeera reporters were among the first wave of international embeds, they pulled out of the program soon after, claiming that US officers refused to brief them, citing their perceived hostility to American policy and actions in the Middle East.[161] In the eyes of the US government and media, this 'hostility' was evidenced not only in Al Jazeera's focus on the collateral damage suffered by Iraq's civilian population and infrastructure but also through a purposely negative portrayal of the invading forces. Some regarded this as active collaboration. Paul Wolfowitz, the US Deputy Secretary of Defense, accused Al Jazeera's Arabic television channel of 'slanting the news incredibly' and so 'endangering the lives of American troops' by 'inciting violence against them'. Some US officers claimed that Al Jazeera had 'advance notice of attacks on US troops' and made no effort to warn them. In response, the US military launched a range of retaliatory actions, arresting Al Jazeera's reporters and raiding the broadcaster's offices in Ramadi. In Baghdad, its bureau chief claimed that his staff had been 'subject to strafing by gunfire, death threats, confiscation of news material, and multiple detentions and arrests, all carried out by US soldiers'.[162]

American patience finally gave out on 22 March 2003, when Al Jazeera broadcast images of Iraqi personnel interrogating five US prisoners from the 507th Maintenance Company. Not only was this an affront to domestic sensibility; it was also an apparent breach of the Geneva Convention's provisions around the public display of prisoners of war. What made the broadcasts especially offensive to the Americans was that the dead bodies of at least four US soldiers, some with gunshot wounds to the head, were clearly visible in the background. Little more than a fortnight later, on 8 April, the day after American forces rolled into the centre of the Iraqi capital, a US missile hit Al Jazeera's Baghdad bureau, killing one journalist and wounding another. The US military claimed that this was a mistake rather than a militarised act of censorship. 'This coalition does not target journalists', Brigadier General Vincent K Brooks told a news conference at CENTCOM in Doha. 'We don't know every place journalists are operating on the battlefield. It's a dangerous place indeed.'[163] Yet as Al Jazeera's chief editor, Ibrahim Helal, told the *Guardian*, the US military had been given the map coordinates of the office to avoid just such an event: 'Our office is in a residential area, and even the Pentagon is aware of its location.'[164]

What US bombs began, the interim government of Iraq finished. As the country descended into near anarchy in the months after the US invasion, Al Jazeera faithfully documented the 'chaotic combination of insurgency, sectarian violence, criminality, and factional fighting' that ensued.[165] Graphic images of the breakdown in law and order, widespread looting, random killings and the rise of a new economy in kidnappings, was not the vision of a grateful, pacified, liberated Iraq that the US or its allies wanted to see on the world's screens. In early August 2003, the Iraqi Interior Minister, Falah al-Naqib, claimed that by broadcasting videos made by kidnappers and hostage takers, Al Jazeera was 'encouraging criminals and gangsters' and transmitting 'a bad picture of Iraq'. A week later, the President of the Governing Council of Iraq, Ayad Allawi, announced a 30-day renewable ban on the broadcaster's operations in Iraq, accusing it of 'inciting hatred'. The Interior Ministry chimed in, claiming that having become 'the voice of terrorist groups', Al Jazeera had failed to show 'the reality of Iraqi political life'.[166] A month later when the ban was made indefinite, Al Jazeera evacuated its remaining staff, shuttered its offices and continued to cover the chaos in Iraq through its extensive network of stringers.

Unilateral reporters who chose to cover the war from beyond the relative safety of the embed program, and the implicit narrative suasion it brought, were likewise regarded as suspect, if not hostile. According to Susan Carruthers, in the eyes of the US-led military coalition, merely 'to step outside the embedded arrangement was to declare one's opposition to Operation Iraqi Freedom and thus to invite rough treatment'.[167] Such rough treatment became so common that it spawned its own dark humour. One well-known joke making the rounds among reporters at the time asked: 'What's the difference … between the Iraqi army and the American Army? Answer: the Americans shoot at you.'[168] Clearly, if during Operation Allied Force PJ Crowley had been concerned that the weaponising of public information would produce 'an adversarial relationship' between the US military and 'our own reporters and potential retaliatory action against Western journalists in enemy territory', then the Second Gulf War saw his fears realised. The US and the British actively discouraged reporters from seeking to cover the war without the protection afforded by an embed. The *Green Book* issued to reporters by the Ministry of Defence, detailing 'the practical arrangements for enabling correspondents to report on operations', offered a sober warning to unilaterals, specifically drawing their attention to the danger from friendly fire:

> *Correspondents who gain access to operational areas, other than under the auspices of MOD or Media Operations (Ops) staffs, do so at their own risk … Media representatives need to recognise that operations, and particularly those involving war-fighting, create extremely hazardous environments in which lethal force may be employed. In the often-challenging situations that this engenders, mistakes resulting from mis-identification, weapons systems failure or mallocation [sic] may result.*[169]

On the other side of the Atlantic Victoria Clark pointed out to reporters that 'it is very, very dangerous out there'. And the danger came from all sides. As ABC correspondent John Donvan noted: 'The Iraqis saw journalists as part of an invading force. And the invaders—the coalition forces—saw unilaterals as having no place on *their* battlefield. There was no neutral ground.'[170]

Unilaterals covered different aspects of the war, quite distinctly from their embedded comrades, producing reports less likely to engender public support and so threatening the coalition's carefully coordinated messaging. The heterodox nature of their coverage, Fahmy and Johnson noted, arose from 'the different physical conditions they operated under, and different external forces'. Embedded reporters were entirely reliant on the military units to which they were attached. As they were 'were prohibited from travelling independently … they could only go to where the military took them' and 'had access to few sources other than the military'. Further, 'being tied to one military unit meant journalists could only present the war from the perspective of the unit they covered'. Fahmy and Johnson's survey of embedded journalists 'found that the embeds believe they presented a different reality than did the unilaterals', a reality 'focused on the troops and individual battles'. By contrast, though unilaterals enjoyed greater freedom of movement, their mobility denied them proximity to the troops and excluded them from the protection the troops provided. Unable to cover their own troops, the unilaterals' reports 'concentrated on other issues, such as refugees … Iraqi civilians wounded and killed and their reception and perception of the U.S. military'.[171] When John Donvan travelled to the Iraqi city of Safwan in the early days of the ground war he realised that unilateral reporters were uniquely positioned to tell a story that was not being told by the embeds:

> *The Iraqis of Safwan were not dancing in the streets. In what would become a pattern elsewhere in Iraq, U.S. troops (and the reporters embedded with them) would often witness a warm welcome at the front end of the coalition advance. But later, when the tanks had rolled by, that would change. Safwan is the city that gave the world that widely broadcast image of a just-liberated Iraqi slapping Saddam Hussein's portrait with his shoe. But only hours later, we encountered hostility. Everyone we met voiced suspicion of U.S. intentions, outrage over civilian casualties, and skepticism over promises of U.S. aid. The message from the people of Safwan—now voiced by many Iraqis in many places—was that the U.S. had its work cut out for it. Just getting rid of the dictator is not enough to win the hearts and minds of the people.*[172]

This sort of coverage did little to endear the unilaterals to the troops or their political masters. Of the 14 journalists killed in the war's early stages, almost all were unilaterals, seven of whom were the confirmed victims of coalition fire. Already on edge in an unpredictable combat environment, troops were encouraged to regard all unidentified vehicles or personnel as hostile and treat them accordingly. The effects of this shoot-first-and-ask-questions-later approach were predictable. On 22 March 2003, having waited two days for clearance to cross into Iraq from Kuwait, ITN's experienced defence correspondent Terry Lloyd, Belgian cameramen Daniel Demoustier and Fred Nerac, and Lebanese interpreter Hussein Osman were making good progress on the road to Basra. They were travelling in two four-wheel drive vehicles, the bodies of which were plastered with tape spelling out 'TV' in large letters. Some hours into their journey, they encountered Iraqi military traffic travelling in the opposite direction, away from Basra towards the Kuwaiti border. They decided to turn around and head back as well. As they did this, Osman and Nerac's vehicle was ambushed and seized by Iraqi militia. Lloyd and Demoustier escaped, though Lloyd was injured by gunfire. Soon after, further down the road, despite the clear markings, Lloyd and Demoustier's vehicle came under sustained tank and small arms fire from US Marines, who were in positions by the side of the road. While Demoustier managed to throw himself clear of the vehicle before the first shell hit, Lloyd, because of his injury, was left in his seat. He was rescued from the vehicle soon afterwards by a Red Crescent ambulance. However, while being evacuated in the ambulance he suffered a fatal injury from a helicopter gunship attack. Osman's body was exhumed and identified some months later. Nerac's has never been found.

Lloyd's death marked a defining moment in British coverage of the war as many editors decided at that point that 'US military action had actually made it unsafe to operate as unilaterals'.[173] While the US Marines who had fired on Lloyd's vehicle had plausible reasons for doing so, the US military's readiness to open fire was well known to reporters.[174] As one ITN reporter remarked to Tim Gopsill: 'They just didn't wait that extra second to see that the car had TV markings … They're scared stiff and they just shoot at everything that moves.'[175] The day after Lloyd's death, John Donvan and his ABC colleagues decided 'it was time to rip the duct tape off the car … the tape that spelled out in eight-inch letters—"TV" on every side of the vehicle'. They did so because while in previous conflicts 'The safest thing for journalists was to shout from the rooftops that they were present at this

conflict *as reporters*, not combatants. This time, the opposite may have been true'.[176] While there is no evidence that troops were given specific orders to go after unilaterals, Tim Gopsill notes that 'a strategy of targeting reporters', official or otherwise, had an obvious if 'sinister logic' to it, in that in many cases it served 'to discourage them from independent reporting'.[177]

With heterodox voices muffled or silenced, the media became both a platform and the principal vector for military communication, conveying 'information and indicators to audiences' at home and abroad, calculated to sustain domestic morale while undermining the competitor's will to fight. In some ways, the Second Gulf War represented a high point for public information provision by the media. Embedded with military units, the media were both objects and agents of the saturation strategy, consumers and providers of plentiful and timely, if not always good quality, coverage of US forces and their allies at war. As Susan Brockus noted, 'the role of the embedded journalist tended to take on a public relations function for both the U.S. military and their home news organizations'.[178] At the centre of the embedded media's coverage was the 'live cross' from the area of operations. As well as offering 'an assurance of access to truth and authenticity', 'liveness' has long been seen as synonymous with good television.[179] Yet the quality of the live coverage from the Gulf was variable. For every tense dispatch from a correspondent under fire, there was the obligatory extended tracking shot of the desert landscape being traversed by US military vehicles. The Project for Excellence in Journalism's content analysis of the embedded reports on television from three of the first six days of the war concluded that the coverage was largely anecdotal: 'It's both exciting and dull, combat focused, and mostly live and unedited. Much of it lacks context but it is usually rich in detail. It has all the virtues and vices of reporting only what you can see.'[180] Ironically, despite the fact that the express purpose of bringing the media to the Gulf was to verify the military's actions there, the anecdotal nature of the embeds' coverage produced a distorted impression of the war. In Susan Carruthers's view, this was less by accident than by design, given that, for the military, the accuracy of the media's reporting mattered far less than their role as 'conductors of energy between the battlefield and civilian society'.[181] Accordingly, as it turned out, the media's principal role was less to provide factual verification of the military's actions in the Gulf than it was to provide the public with an emotional connection to the troops and so sustain morale at home. The public service journalism they provided was shot through with persuasive intent.

Part 2: Command and Control Meets the Decentred Network

Chapter 4: US military responses to social media

It is no small irony that at the very moment, during the Second Gulf War, when the US military's triumph in the information domain seemed complete, when it appeared to have attained full spectrum dominance, the communications model it had mastered and the organisational systems that supported it were being rendered obsolete by the new media revolution unfolding around it.[182] In 2001, as Rid and Hecker note, 'the Internet … like the old media, remained a platform for mass monologue, albeit with a growing number of corporate senders and individual receivers'. Growing public demand for greater participation in the development of online content saw the rapid development of software that enabled genuine peer-to-peer interactivity. Within five years,

'Web sites that boasted so-called "user-generated content" had climbed to the very top of the traffic ranking lists', marking the birth of Web 2.0. The term describes 'a second-generation Internet where contributions of private individuals and self-organized communities compete with those of companies and governments … The new Web connects people directly and enables dialogue'.[183]

These developments had profound effects on the conduct and communication of warfare—bringing the two into ever closer alignment. If, in the 1970s, those seeking the liberation of Palestine needed to hijack airliners or attack an OPEC meeting to attract the attention of the world's media, by the mid-2000s as US forces struggled to suppress the Sunni insurgency in Iraq and the Taliban were recovering lost ground in Afghanistan, all that they needed to publicise their causes was a cheap mobile phone and an internet connection. As Brendan Koerner put it:

'Never before in history have terrorists had such easy access to the minds and eyeballs of millions.'[184] When conventional forces tried to silence the insurgents by bombing their operations centres and communications facilities, as they had in Serbia and Iraq, they could not locate them. This was because they no longer communicated with their followers from iconic institutional structures through transmission towers and satellite dishes but via a decentralised network of distributed, semi-autonomous nodes that carried their voices and images to their followers in every corner of the world. Shut down one source and another emerged within minutes. Nodes came and went, but the network lived on and any attempt to silence it was bound to end in failure and frustration.

The futility of trying to bomb a virtual target or silence an intangible voice laid bare the extent to which the conduct of war itself was undergoing a paradigm shift at this time. As the US military and their principal allies struggled to suppress the insurgencies in Iraq and Afghanistan they recalibrated their combat aims and reappraised the tools they needed to achieve them. Traditional warfighting, defined by Rid and Hecker as War 1.0:

> *is a predominantly military exercise, 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.*

The invasions and swift victories in Iraq and Afghanistan were emblems of War 1.0: greater force of arms, superior manoeuvrability and better intelligence were regarded as the keys to what looked at the time like decisive military triumph. War 2.0, by contrast, 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 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.*[185]

As the early victories in Iraq and Afghanistan faded from memory and each conflict settled into its insurgent phase, it became clear to the US military and its allies that the contest for territory was a proxy for the war's true centre of gravity, the struggle for the trust and loyalty of the local people. In an effort to win that trust, the US and its allies increasingly turned to the strategies and tactics of War 2.0, and a central weapon in that fight was social media.

It is notable that it was not the well-resourced, technologically advanced Western militaries who were first to take up and adapt social media to their needs but the under-equipped non-state actors they were combating. Arquilla and Ronfeldt's assertion, more than 10 years earlier, that the information revolution would diffuse and redistribute power to the benefit of weaker parties and the detriment of 'large, bureaucratic, aging institutions' was resoundingly borne out in the innovative ways that Al Qaeda and later ISIS used social media and the information advantage this afforded them.[186] Indeed, the meagreness of their military resources has traditionally pushed non-state actors to adopt innovative tools. Without:

> *air forces, navies, regular army units, highly sophisticated weapons systems, or other powerful and expensive means to project physical power ... insurgents have to compensate in the psychological dimension for a lack of force in the physical domain.*[187]

Taking the fight to the cognitive battlespace, '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"', non-state actors used social media to indoctrinate, recruit, organise and deploy their forces while conventional militaries were still fretting about rogue postings and reputational damage.[188] As NATO's Strategic Communications Centre of Excellence observed in its 2016 report *Social Media as a Tool of Hybrid Warfare*:

> *Virtual communication platforms have become an integral part of warfare strategy. The recent conflicts in Libya, Syria, and Ukraine have demonstrated that social media is widely used to coordinate actions, collect information, and, most importantly, to influence the beliefs and attitudes of target audiences, even mobilise them for action.*[189]

However, wedded to a War 1.0 view of information as 'protected, secret and used primarily for internal purposes', conventional militaries have, in most cases, moved hesitantly into the online space. This halting advance has been further slowed by a combination of factors, among them active resistance from an old guard wedded to established practices, social media's discordance with many of the norms of military culture, and its incompatibility with the armed forces' established bureaucratic and organisational systems. Yet despite all of this, at a time when control of the information environment is seen as increasingly central to success in warfighting and no combatant force can afford to ignore its digital capability, Western militaries are, officially at least, enthusiastic proponents of social media as an operational capability. The Multinational Capability Development Campaign (MCDC), a NATO 'test-bed' for concept and capability development, argues that for conventional militaries fighting to influence both domestic and dispersed overseas audiences:

> *The question is no longer whether to be on social media, but how to be there ... Though it is difficult to control discourses or to shape perceptions, it is less dangerous than staying away from the digital IE.*[190]

While acknowledging that the information environment is a crucial space of war, even those conventional militaries that are genuinely committed to the adoption of digital and social media technologies have struggled to integrate them into their systems. Though comfortable laying out parameters for the safe and secure use of social media by their personnel—a list of dos and don'ts—or advertising its benefits as a recruiting and reputation management tool, their progress towards its fuller integration as a tool of influence operations has been marked by risk aversion and fear.[191] The conventional forces who have overcome these institutional ambiguities have recognised the central role played by social media, its ability to help 'affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects', and adapted their organisational systems and cultures to facilitate its use.[192]

For more than 75 years, the US military has been at the forefront of innovations in military communications within its forces. It has enthusiastically embraced technological advances that have revolutionised the battlefield, given commanders a clearer overview of force disposition

and more immediate contact with their men and women on the ground, and so afforded them a greater responsiveness to the shifting dynamics of combat. Yet its enthusiasm for the communications advances made possible by the advent of Web 2.0 and the interactive revolution it brought was notably ambivalent and was marked by an instinct to protect and limit the circulation of information beyond the military. Rid and Hecker argue that while military caution about the potential hazards of too free a flow of information was fed by ignorance and fear, 'the most salient feature of the American security establishment's reaction to the new information environment' was 'confusion'. This was because when 'senior generals and admirals are in charge of new technologies they themselves have not been socialized in' they 'tend to either over- or underrate their significance'.[193] Social media offers a case in point.

Further, disputes about how, by whom and for what purposes social media should be deployed reflected ongoing debate within the US military about the role of the modern warfighter on the information battlefield. Sean Lawson notes:

> *Though there is general agreement that information and networked ICTs are central to achieving success in contemporary conflicts, the introduction of a new ICT can still pose a challenge to professional identities and theories of warfare … The ongoing controversy over social media within the US military is one indicator that these difficulties continue to this day … This controversy provides a small window into a larger struggle to define the reality of and determine the requirements for success in information-age conflicts.*[194]

In the wake of the US invasions of Afghanistan and Iraq, the growth of the insurgencies in both countries coincided with the rapid spread of new social media tools. Soldiers on the front lines and at home blogged about where they had been, what they had seen, what they had done, what had gone well, what had not and how their experiences of the war were reflected in the mainstream media. Jean-Paul Borda, a National Guardsman and keen blogger who served in Afghanistan in 2004, felt that the mainstream media was not telling the full story about the war. He told the *Wall Street Journal*'s Mike Spector, 'You hear so much about what's going wrong … It gets hard to hear after a while when there's so much good going on'. He was not alone in his view that the mainstream media was missing the

real story. Reading soldiers' blogs, he found 'Hundreds of other troops and veterans were blogging world-wide, and many focused on a common enemy: journalists'. One of the most influential of the early military blog (milblog) sites, *BlackFive*, was started by Army veteran Matthew Burden in December 2003:

> *after he learned that an Army buddy, Maj. Mathew Schram, had been killed in an ambush near the Iraq-Syria border. Mr. Burden, 39, felt his friend received short shrift in media coverage and decided to blog about military stories he felt weren't getting the attention they deserved. 'Does Abu Ghraib need to be told 40 times above the fold in the New York Times when half your readers couldn't name the guy who won the Medal of Honor?'*[195]

The year after he returned from Afghanistan, in an effort 'to make it easier for people to read soldiers' accounts' of war, Borda set up Milblogging.com. The site provided hotlinks to hundreds of military blogs organised by country, arm of service, military branch and subject matter.[196] By 2006, when Borda sold the site to Military.com, it linked to more than 1,400 individual blogs; six years later there were 3,016 milblogs listed at Military.com.[197]

This proliferation of first-hand accounts from the men and women on the front line of the US's fighting in Afghanistan and Iraq spooked the Pentagon. The US military feared that the wealth of detail provided in some of these blogs, freely accessible to all on the internet, might lead to breaches of operational security and inadvertently disclose information of use to the nation's competitors. In 2005 the Army acted. US Army Regulation 530-1 *Operations Security*, section 2.19, specifically addressed the operational security threats posed by social media. It required that all Army personnel:

> *h. Consult with their immediate supervisor and their OPSEC program manager, prior to publishing or posting information that might contain sensitive and/or critical information in a public forum—this includes, but is not limited to letters, e-mail, Web site postings, Web log (Blog) postings, discussion in internet information forums, discussion in internet message boards, or other forms of dissemination or documentation. Supervisors will advise personnel to ensure that sensitive and critical information are not disclosed. Each unit's OPSEC representative will advise supervisors on means to prevent the disclosure of sensitive and critical information.*[198]

Punishments for infractions of the guidelines ranged from administrative sanction to court martial or criminal action for civilians. The milblog community denounced the policy as heavy-handed and counterproductive. *BlackFive* claimed that the regulations would see 'the end of military blogging as we know it'.[199] Matthew Burden told *Wired*:

> *This is the final nail in the coffin for combat blogging … No more military bloggers writing about their experiences in the combat zone. This is the best PR the military has—its most honest voice out of the war zone. And it's being silenced.*[200]

The author of the guidelines, Major Ray Ceralde, pointed out that there was some leeway in enforcement of the rules:

> *It is not practical to check all communication, especially private communication … Some units may require that soldiers register their blog with the unit for identification purposes with occasional spot checks after an initial review. Other units may require a review before every posting.*

However, as Jeff Nuding of the *Dadmanly* blog observed, with the regulations so tightly drawn:

> *many commanders will feel like they have no choice but to forbid their soldiers from blogging—or even using e-mail. If I'm a commander, and think that any slip-up gets me screwed, I'm making it easy: No blogs.*[201]

In 2007 when the Army issued a revised version of the policy, it distributed a Public Affairs fact sheet, 'Army Operations Security: Soldier Blogging Unchanged'. The purpose of the fact sheet was to allay the bloggers' concerns and contradict some of the wilder rumours circulating around the policy. It reassured bloggers that they were free to continue their work without oppressive oversight:

> *In no way will **every** blog post/update a Soldier makes on his or her blog need to be monitored or first approved by an immediate supervisor and Operations Security (OPSEC) officer. After receiving guidance and awareness training from the appointed OPSEC officer, that Soldier blogger is entrusted to practice OPSEC when posting in a public forum.*

Further, it reassured twitchy emailers that 'Soldiers do not have to seek permission from a supervisor to send personal E-mails. Personal E-mails are considered private communication'.[202] Despite its emollient tone, the fact sheet insisted that there were no changes of substance to the 2005 policy:

> *Army Regulation 530-1, 'Operations Security,' was updated April 17, 2007—but the wording and policies on blogging remain the same from the July 2005 guidance first put out by the U.S. Army in Iraq for battlefield blogging.*[203]

The Army was clearly intent on ensuring that its personnel were conscious of their responsibility to maintain operational security and to counter the perception that blog posts were free fire zones where anything might be said.

Melissa Wall describes how the Department of Defense (DoD) and the US Army sought to control bloggers not merely by regulation but also through co-option:

> *The DoD's head of new media operations has barnstormed across the United States attending major blogging and technology conferences … where he sits on panels, shakes hands, and promotes the integration of bloggers within the Pentagon's own information apparatus.*

The Electronic Media Engagement Team at CENTCOM provided bloggers with press releases and facilitated interviews with serving personnel. The Pentagon introduced DoD Live, 'home of the Blogger Roundtables', conference calls where bloggers were invited to ask questions of selected service personnel. As Wall notes:

> *Critics suggest that these bloggers are part of the Pentagon's use of surrogates to spread its point of view … By providing access and a steady source of information, the military can offer a seemingly attractive resource to usually cash-strapped citizen media … The military and its supporters might argue that there is little difference between a blogger re-mixing information culled from the Associated Press or information supplied by the Pentagon … Of course, the Associated Press, like other corporate news media, is generally not overtly attempting to change opinions and generate support for policies.*[204]

Just as the Department of Defense issued the revised Army Operations Security policy and was mulling over the most effective ways to deal with the security threat posed by blogging, Estonia's online infrastructure suffered what was at the time the largest ever DDoS cyberattack, thought to have originated from Russia. At its peak, on 9 May 2007, up to 85,000 hijacked computers brought down 58 Estonian websites and the online services of the country's largest bank, Hansapank, were crippled for more than an hour.[205] A year later, Russia's invasion of Georgia was supported by an attack on government websites. Suddenly, 'cyberwar' was at the top of every government's security policy agenda. The Obama administration's 2009 review of US cybersecurity policy resulted in the creation of a civilian 'cybersecurity czar' as well as a military 'Cyber Command'.[206] The Department of Defense's sudden and urgent focus on cybersecurity and its new awareness of the vulnerability of its computers, systems and networks had an immediate effect. In July 2009, STRATCOM issued a warning order 'asking for feedback on a social media ban on the NIPRNet, the Defense's Department's [sic] unclassified network'. A source at STRATCOM outlined the rationale of the proposed policy to *Wired* magazine's Noah Shachtman:

> *The mechanisms for social networking were never designed for security and filtering. They make it way too easy for people with bad intentions to push malicious code to unsuspecting users.*[207]

Yet the mooted ban on 'Twitter, Facebook and all other social networking sites' came at the same time that the US Army was moving to embrace social media as never before.[208] In June 2009, the Chairman of the Joint Chiefs of Staff, Admiral Mike Mullen, unveiled his Facebook page, while his Twitter account had already attracted 4,000 followers. A month earlier, after years of blocking access to popular social media sites on military networks, an operations order from the Army's 93rd Signal Brigade to all domestic directors of information management flagged 'the intent of senior Army leaders to leverage social media as a medium to allow soldiers to "tell the Army story" and to facilitate the dissemination of strategic, unclassified information'. Accordingly, it instructed that 'the social media sites available from the Army homepage will be made accessible from all campus area networks'.[209]

Echoing Rid and Hecker's appraisal of the different approaches to information embodied in War 1.0 and War 2.0, Sean Lawson notes that the Army's apparently contradictory positions in respect of social media, one intent on harnessing its properties to tell the Army story, the other focused on guarding against the vulnerabilities arising from its use by personnel, reflect a larger struggle within the Pentagon and the US military over contrasting views about the nature and purpose of information:

> *[O]pponents of social media often see information primarily as data, as a commodity to be protected by securing the technological infrastructure that stores and transmits it. Thus, opponents tend to worry more about threats to the confidentiality, integrity and availability of military networks and information and see the use of social media by individual military professionals as a dangerous new vector for such attacks.*

By contrast:

> *[S]ocial media advocates 'tend to understand information and its value as stemming primarily from its ability to improve situational awareness, collaboration and morale within the military organization, as well as to fight the battle for the hearts and minds of both domestic and foreign audiences. Social media supporters often argue that allowing individual military professionals to act in a decentralized way to address these challenges is crucial for success.*[210]

The victory of the social media advocates was confirmed on 25 February 2010, when the Department of Defence released its Internet Based Capabilities Policy.[211] The policy affirmed that, with immediate effect, the DoD would 'allow access to social networking sites from the military's non-classified computer network'.[212] As a result of this new policy, the Marine Corps was required to lift its ban on most social media sites, while the US Army had to lift the restrictions on its directory of blacklisted sites, the most prominent of which was YouTube. Driving home the revolution in communication that this policy set in motion, the first news of the policy's announcement came via the Principal Deputy Assistant Secretary of Defense's Twitter feed.

A key influence in the victory of social media's proponents was the increasing influence of counterinsurgency (COIN) doctrine over the conduct of the wars in Iraq and Afghanistan. COIN's emphasis on winning the loyalty and trust of the local populations while retaining the support of the domestic constituency through clear and constant communication, the prioritisation of hearts and minds over bombs and bullets, gave social media and their associated technologies a central role in the day-to-day conduct of the campaigns. The appointment of the principal author of the US COIN doctrine, General David Petraeus, as commander of the Multi-National Force in Iraq in 2007 saw an increased role for social media technologies in US military operations first in Iraq and later in Afghanistan, after he assumed command of US forces there in 2010. In 2009, two separate reports, one from the Army War College's Center for Strategic Leadership, the other from the Center for Technology and National Security Policy at the National Defense University, endorsed the efficacy of social media as means of evading the supposed anti-military bias of the mainstream media and getting Army's message directly to the people.[213]

In January 2011, the Online and Social Media Division of the Office of the Chief of Public Affairs of the US Army issued its *Social Media Handbook*. This has since been regularly updated, with the last print iteration appearing in 2016.[214] The *Social Media Handbook* offered soldiers and their commanders a practical guide to safe, effective, and secure use of the major social media platforms. It provided clear and explicit examples of good and bad practice, a step-by-step guide to 'Creating Effective Communication Platforms', checklists for establishing official social media accounts and handy directories to a range of the Army's social media sites.[215] It also offered a clear guide on how to recognize scams and impersonations and what to do about them, and detailed information about how to ensure that the user's social media posts observe the requirements of operational security. At the time, it represented a model approach to the use of social media and was a testament to the US military's determination to engage with its publics and tell them its story directly.

In 2016, to enable more timely updating, the social media guide was moved online to the *Army Social Media* website.[216] This includes links to policies and guidance documents establishing social media use within US military doctrine, links to mandatory training and a list of recommended social media training sites—including 'Twitter Flight School' and the 'YouTube Creator Academy'.[217] Through a hotlink to the Army's 72-page guide *Social Media Protection: A Handbook for Privacy and Security Settings*, the site offers a 'step-by-step guide covering good cyber-hygiene practices and the steps you need to take to strengthen the security and privacy for Facebook, Instagram, Twitter, and LinkedIn'.[218]

Inevitably, despite the clear explication of policy, not all soldiers' posts were compliant with the designated norms. In 2012 Sergeant Gary Stein was given an 'other than honorable discharge' from the US Marines for 'misconduct' after posting anti-Obama comments on his Facebook page.[219] Such infractions are minor and the price that militaries can expect to pay for extending social media freedoms to their personnel. In a more serious breach of security protocols, detailing the risks attendant to geotagging, an Army spokesperson cited an episode in 2007 when soldiers in Iraq took photos of a recently arrived fleet of helicopters on the flightline that they later uploaded to their social media pages. It transpired that one or more of the soldiers had forgotten to switch off the geotagging features on their phones. As a result, using commercially available software, the enemy plotted the exact location of the helicopters and launched a mortar attack that destroyed four of them.[220] Such episodes stoked the fears of cybersecurity experts who were already fretting over the exponential increase in cyberattacks and the concern that social media provided an easy vector for such assaults. At the May 2011 Department of Defense Intelligence Information Systems conference, the Defence Intelligence Agency's Chief Information Security Officer, Sean McCormack, noted that in the face of increased cybersecurity risks, 'almost half of all employers in the U.S. now ban social media in the workplace because of "security concerns" and "loss of productivity"'.[221]

But the problem was not confined to social media. In November 2017, Strava, a 'social network for athletes', announced a major update to 'its global heat map of user activity that displays 1 billion activities—including running and cycling routes—undertaken by exercise enthusiasts wearing Fitbits or other wearable fitness trackers'. Nathan Ruser, a graduate student

at the Australian National University, identified clusters of Strava user activity 'potentially related to US military forward operating bases in Afghanistan, Turkish military patrols in Syria, and a possible guard patrol in the Russian operating area of Syria'. This was only the tip of the iceberg:

> *Other researchers soon followed up with a dizzying array of international examples, based on cross-referencing Strava user activity with Google Maps and prior news reporting: a French military base in Niger, an Italian military base in Djibouti, and even CIA 'black' sites.*

While this was worrying enough, it was feared that there was a greater threat from:

> *potential competitors figuring out patterns of life,' by tracking and even identifying military or intelligence agency personnel as they go about their duties or head home after deployment … Paul Dietrich, a researcher and activist, claimed to have used public data scraped from Strava's website to track a French soldier from overseas deployment all the way back home.*[222]

In the face of these threats the Central Command Press Office in Kuwait announced that the Coalition was 'in the process of implementing refined guidance on privacy settings for wireless technologies and applications', adding that 'such technologies are forbidden at certain Coalition sites and during certain activities'.[223]

Faced with similar concerns in 2015, the Chinese military warned 'troops and the wider public that network-connected wearable devices pose a national security risk when used by military personnel'.[224] Five years earlier the People's Liberation Army banned access to and the use of social media by its 2.3 million servicemen and women:

> *The* People's Liberation Daily*, the armed forces' official newspaper, said passing on personal details such as a soldier's address, duties or contact details could risk revealing the location of military bases. It added that particular risks exist in users posting photos of themselves, such as during training, which could divulge military capabilities and equipment.*[225]

This blanket ban was lifted in 2015 but only after the PLA's IT experts had developed 'comprehensive counter-espionage software' that was then installed on all devices used by PLA soldiers. The software, developed in association with the operators of the country's domestic mobile networks, not only ensured that the user's activities 'can be closely monitored by the Army's newly established internet administration centres … It also tracks off-duty officers in case they visit "unwanted places"'.[226] The PLA was highly sensitive to possible breaches of security via smartphones and uploaded photographs, and soldiers' internet and smartphone use was hedged around with regulation. Quoting from a PLA report, Celine Ge noted:

> *Soldiers were allowed to use smartphones to access the internet during extracurricular activities, days off, holidays and during other downtime, but the browsing should be done via encrypted mobile terminals or at military internet cafes to prevent any leakage of information.*
>
> *The report said soldiers were prohibited from taking photographs at garrisons with their smartphones and sharing them, while officers sent on peacekeeping missions abroad had also been urged to be cautious when receiving invitation messages from 'foreign friends' via social media.*[227]

In the face of this powerful example, there was clear pressure from within for the US military to reverse its policy and return to a more draconian policing approach to social media. Yet, while keenly aware of the challenges posed by social media in the connected battlespaces of the 21st century, the military was also alive to the solutions it brought:

> *Major trends affecting military operations in the strategic environment include the increasing breadth and depth of information available through all forms of communications media, the increasing speed with which information flows from and through a population, and the proliferation of interoperable digital devices. This global hyper-connectivity is more than just a technological trend; it is a societal and cultural trend as well. An entire generation has grown up not knowing a world without the internet, and these 'digital natives' interact with others within virtual environments in ways fundamentally different than in previous generations. In most parts of the world, nearly everyone and everything is connected in some*

> *manner, and the convergence of information technology with human values, attitudes, beliefs, and perceptions has created new challenges and new vulnerabilities for the United States.*[228]

The Department of Defense's *Strategy for Operations in the Information Environment* (IE) (2016), from which the above is taken, identifies a desired end state only attainable with the use of social media, in which:

> *Through operations, actions, and activities in the IE, DoD has the ability to affect the decision-making and behavior of adversaries and designated others to gain advantage across the range of military operations.*

It specifies nine ways to support the attainment of this end state that 'serve as guidance to enable effective Departmental operations in the IE':

- *Improve the capability of the Department to monitor, analyze, characterize, assess, forecast, and visualize the IE …*
- *Update joint concepts to address the challenges and opportunities of the IE …*
- *Train, educate, and prepare the Joint Force as a whole for operations in the IE …*
- *Train, educate, and manage IO professionals and practitioners.*
- *Establish policy and implement authorities, coupled with doctrine and tactics, techniques, and procedures, which maintain the agility of the joint force in the IE, including the capability to adapt as the IE changes….*
- *Acquire and maintain sufficient capability and capacity of resources focused on operations in the IE …*
- *Integrate and synchronize DoD efforts for operations in the IE with other USG activities …*
- *Foster the credibility, legitimacy, and sustainment of U.S. and coalition operations, actions, and activities …*
- *Establish and maintain enduring and situational partnerships.*

These ways are served by means or tools focused on four categories, 'people, programs, policies and partnerships' through which the ways can be attained, refined and developed.[229] They include adequate training of

personnel, resourcing of capabilities and capacities and the embedding of social media competencies and support in doctrine, thereby ensuring that 'doctrine relevant to operations in the IE remains current and responsive based on lessons learned and best practice'.[230]

Yet despite this clearly defined posture, by 2014, when ISIS forces seized Mosul, spearheaded by a highly successful social media campaign, it brought home to conventional militaries around the world that they possessed neither the organisational systems nor the expertise to deploy their own social media assets and combat their non-state competitors in the information environment.[231] To address the shortfall and map the path to competence, in 2015 the US-led Multinational Capability Development Campaign sponsored a two-year 'collaborative joint, multinational and coalition concept and capability development' campaign, the Multinational Information Operations Experiment (MNIOE), to report on the challenges standing between NATO militaries and the successful integration of social media into their operations.[232] Its report, *Analytical Concept for the Use of Social Media as an Effector*, was published in December 2016.[233] Despite the US military's manifest commitment to the provision of doctrine, policy, strategic support and significant resources to drive the integration of social media with its broader operations, its implementation seemed frozen. There were countless plans for social media, but little in the way of coordinated or successful implementation or use.

In December 2017, the Director of Information Operations in the Office of the Secretary of Defense, Robert Presler, observed that the organisation, personnel, training and operational capacity of the US military's digital resources were still 'barely adequate' and that they were 'poorly' prepared to conduct an information campaign: 'I would say we're getting better, but we're climbing out of a hole.' Presler was particularly concerned by what the US military's information failures in Iraq and Syria boded should it be drawn into a larger conflict against a well-resourced conventional competitor:

> *[W]hat if we were to increase our scale and scope to a conflict with a national state? I mean here we're talking, you know, a non-state group of actors, roughly affiliated, somewhat disorganised, but also with a lot of capability at times. So, it's a very different thing to think about the run-up- to a crisis with a nation state like China or Iran.*[234]

Presler was not alone in his fears. The 2017 *National Security Strategy of the United States of America* expressed a similar concern about the nation's failure to track or counter its competitors' information advantage, noting that while 'America's competitors weaponize information to attack the values and institutions that underpin free societies', the US military's 'efforts to counter the exploitation of information by rivals have been tepid and fragmented'.[235] A principal source of this fragmentation lay in the lack of coordination between the differing arms of the military and the widespread dispersal of responsibility for information operations and effects across the DoD:

> *[E]veryone's got a piece of it [information], and no one has the overarching coordinating role. We can't expect the Sec. Def. or the Dep. Sec. Def. to occupy a large amount of their time organising a range of pieces … But below that, if you say, who's in charge of information in this department, I mean, our Director, who's, you know, the equivalent 06 [Brigadier General] level. We've got leaders above him who have information as part of their portfolio, but it's not the major part of their portfolio, and we've got, you know, related officers, like cyber and the intel portions of DoD, et cetera, that also have portions … I mean, once again, our Under-Secretary IO Policy is designated as the principal staff adviser for information ops, but he is a man with much in his portfolio.*

It was not only the dispersal of authority that was holding the Army back in the information space; it was also the failure to appoint somebody suitably senior to lead it, thereby clearly signalling its importance:

> *[A]t a service level, I would tell you, and I hate to admit this as an Army officer, but the Marine Corps I think perhaps is heading down the right path. They've appointed a Deputy Commandant at the three-star level [Lieutenant General], you know, and given that the Marines are a much smaller service than the US Army, for them to take a three-star and go, 'we're going to have this guy in charge of information and all these related capabilities.' That is an enormously significant investment. Do we have anything like that in the US Army, a three-star that we …? We don't. Not at this time.*[236]

In an effort to enable effective connection between and communication within the different parts of the information operations structure, the *National Defense Authorization Act for Fiscal Year 2018* directed the Secretary of Defense 'to establish processes and procedures to integrate strategic information operations and cyber-enabled information operations' and to 'ensure that such processes and procedures provide for integrated Defense-wide strategy, planning, and budgeting with respect to the conduct of such operations by the Department'.[237] In recognition of the need for clear chains of command and the delegated responsibility for setting and implementing strategy that this brought, the Secretary was required to designate a senior official to develop:

> *a strategic framework for the conduct of information operations by the Department of Defense … coordinated across all relevant elements of the Department of Defense, including both near-term and long-term guidance for the conduct of such coordinated operations.*

This senior official would also be responsible for the 'Development and dissemination of a common operating paradigm across the elements of the Department of Defense' and the 'Development of guidance for, and promotion of … liaison with the private sector, including social media, on matters relating to the influence activities of malign actors'. With central planning and guidance in place, 'each commander of a combatant command' would then be required to develop 'a regional information strategy and interagency coordination plan for carrying out the strategy'.[238] In short, the Defense Authorization Act empowered the Secretary of Defense, and his or her Information Operations Director, to establish the organisational structure they needed to ensure that a Defense-wide joint information operations strategy could be instituted, planned, disseminated and deployed wherever the US military sought to operate.

Yet there is a yawning gap, and a considerable time lag, between receiving the political approval to establish such an organisation, disseminating the orders and standing it up as a fully formed, active force. The US military's ongoing reluctance to promote its information resources or celebrate its triumphs has reinforced scepticism about its credibility as an asset. For US commanders, information has been more of an ontological than an

organisational challenge—it is not that they cannot use it; they just are not sure that they need to—which helps explain the tepid nature of the military's response to competitor information campaigns:

> *Because we have been so good at this kinetic side of war, [commanders] don't understand that every military action has an informational component and how you array that to get after your adversary's story and your adversary's will, and their decision-making process. It's like, 'why bother?' Except that, we've discovered that, winning the kinetic side of the fight is only half the fight.*[239]

The unique, and sometimes confounding conditions of the information battlefield have also been a source of concern for commanders, further temporising their readiness to join it. As one senior officer observed, commanders have been particularly exercised by two specific features of information warfare, the 'always-on' nature of the conflict—'there is no peace time in the information environment. You are always having information rounds lobbed at you 24/7'—and the legal status of grey war:

> *[T]hey have so focused on the phasing system of planning of when are you in conflict and when are you not, that it has legally created boundaries and inhibitions against using information capabilities. Because, legally, are you in phase three or four, and you're not in conflict? You can't do that. And so, they don't understand that the fundamental geometry of warfare has changed.*[240]

Ambivalence about how, when, or why one should engage has been exacerbated by the absence of a shared language through which information operations can be described and debated:

> *Those of us in the information field too often put this in terms that our manoeuvre commanders can't understand … We need to speak in a common language. We need to have some visualisation tools that bring this to bear and show a commander where things are going right in his area of operations, where they're going wrong, and where an information effort perhaps can make a difference. And then we need an action arm which blends these capabilities together and takes action that will show a commander that, hey, if he employs his information taskforce to fix this problem, he'll get some effects that aren't just theoretical or conceptual.*[241]

Planning for and effective action in the information space has been further hindered by the absence of a common understanding of what victory in the cognitive domain might look like. In the absence of this, while commanders press on with tried and tested approaches to subduing the enemy, information operations—its personnel, practices, aims and tools—continue to be regarded as peripheral to military core business:

> *[T]he most critical component ... is for leaders to understand that describing what success looks like and its informational aspect of the operating environment, is just as critical as describing what success looks like on land, in the sea, in the air and space. So, when you're a Joint Force commander, and you're describing to your staff what outcome you expect and what success looks like to you, you should be describing it in informational terms. What decisions do you want your adversary to make and not make? How do you expect to get there? What do you expect to see from a physical standpoint? … It's commander's duty to do this from the beginning, and describe what does success look like in the information environment?*
>
> *Because they're used to doing that in the physical environment … They haven't quite learnt the vocabulary yet of thinking of it in the cognitive sense of, 'How do I break my adversary's will? How do I get him to certain decision points to lead to that? And what needs to happen for my adversary to reach those decision points, to get to that point of breaking their will, and getting them to do, and then defeat?' Because, that's in essence where we have not done well in recent conflicts.*
>
> *I'll take Iraq for example. Militarily, we were brilliant. You know, we defeated the Republican Guard, and very quickly, you know, we were rolling tanks into Baghdad, and had control of Iraq with all the coalition forces. The problem was, the Iraqi people didn't feel defeated. Because we hadn't done anything about the will, and we had completely forgotten the civilian impact.*[242]

In the face of limited understanding among its personnel about the purposes of information operations or a shared language in which they might be described, the US military is working to adapt its training regime to address the varying levels of information literacy among its commanders:

> *At the moment, [in] most schools it's an elective. It's not part of the core curricula … What we're now looking at is how do we change the curricula, and the professional military education, to inculcate that same thinking, those same ideas, so that somebody, whether they're coming in at basic training, or officer training school, or the academies, right up to the senior level education for general officers such as, CAPSTONE for one-stars and PINNACLE for three-stars, how do we incorporate this thinking of integrating information and physical power to be successful? So, we're at the beginning stages of that …* [243]

Just how close to the beginning is reflected in the Senior Joint Information Operations Course, taught twice a year to 'one- and two-stars who have a likelihood of going on to be joint force commanders and directors of operations and deputy commanders and commanders of combatant commands'. The course is focused on 'describing to them … what is this thing called the information environment … and what tools and capabilities do they have to shape it?'.[244]

Given the ground it has to cover, it is no surprise that the US military conceives of the outcomes of this educational program in the long term, with strategic uptake measured over years rather than months and the resultant planning looking decades into the future. In the summer of 2016, former Secretary of Defense Ash Carter signed off on:

> *the Department's Strategy for Operating [sic] in the Information Environment. And it was looking at from [2017] to about 2025. What changes did we need to make to enable a joint force commander to be successful in dominating this informational aspect of their operating environment?*

The military is also working on:

> *a joint concept for operating in the information environment that looks out to the future … say from about 2025 out twenty years or so. It's an attempt to describe, what do we think the information environment's going to look like then? And therefore, what capabilities are we going to need to be able to have a Joint Force commander succeed?*[245]

The US military is doing what militaries do by instinct when confronted with an unfamiliar technology or situation—they observe and they plan. Yet while the US military schools its commanders in how to operate in the cognitive domain and seeks to convince the sceptics as to the efficacy of information operations, the Russians, Al Qaeda, ISIS and other non-state actors are conquering ground, both physical and virtual, that the US and its allies can scarcely locate, let alone defend. The US military response exemplifies the sort of rigid, top-down planning, command-centred implementation whose slowness and rigidity stifle the decentralised, bottom-up creativity that has so empowered its competitors. Comparing its competitors' nimble, networked response to the deployment of information with the US military's leaden-footed, doctrine-driven strategy, one US commander concluded, 'we're always kind of shooting behind the target when it comes to information and the information space'.[246] It is little wonder that they have so seldom found the target.

Chapter 5: The British Army's social media experiment

On 23 March 2007, an Iranian border patrol vessel detained 15 sailors from HMS *Cornwall* patrolling in disputed waters close to the Iran–Iraq border. The detention triggered a diplomatic crisis, and media interest in Britain became so intense that Fleet Headquarters deployed six 'media shielders' to provide 'protection and advice' to the detainees' families in their dealings with the media.[247] On 4 April, Iranian President Ahmadinejad ordered the release of the detainees as a 'gift' to Britain. Soon afterwards, the Ministry of Defence (MoD) announced that, given the 'exceptional circumstances', the former captives would be allowed to sell their stories to the media. As a result of this decision the detainees' families were once again besieged by the fourth estate:

> *[Many] felt themselves overwhelmed by the pressure of the media. A number were subjected to constant telephone calls and letters asking for comments and interviews. Others described unsolicited face-to-face approaches ('door-stepping') and media 'camps' being set up outside their properties.*[248]

In the wake of this unsavoury episode the Secretary of State for Defence, Des Browne, commissioned the then Chief Executive of the Royal Opera House and former BBC Director of News, Tony Hall, to undertake a review of media access to service personnel.[249] In particular, Hall and his team were tasked to:

> *make recommendations on how to balance our duty to support our people with our duty of transparency, our duty to protect the reputation of the services and, most important, our duty to protect the security of our personnel in a demanding media environment.*[250]

The resulting *Review of Media Access to Personnel* report, otherwise known as the Hall Report, noted:

> *[T]he conditions—including the media environment—in which the MOD and the individual Armed Services are operating are changing fast … Today, the public knows far more about the details of military operations and the thought processes behind them than at any point in the past. This greater level of openness and scrutiny has, to a large extent, been accepted by MOD and the Armed Forces as part of modern public accountability, but its consequences have not yet been fully worked through … Finding the correct balance between openness and operational and personal security is crucial, but that balance will always be dynamic, and therefore requires constant, mature reflection by all involved.*[251]

Among the key factors affecting that balance were rapid changes in the 'attitudes and approach of the media' towards their subjects and the means by which their coverage was distributed and consumed: 'the proliferation of all forms of media: 24 hour news; the challenge to the print media represented by online media; and greater competition amongst broadcasters and newspapers' all combined to make the industry 'more competitive' than ever before. 'In order to secure market share,' Hall noted, 'media outlets are having to seek more "exclusive" stories and are having to go to greater lengths to get them'.[252] The focus of the media's stories had also shifted. The age of the all-powerful consumer had produced a more intense interest in individuals, their preferences and rights, that in turn bred 'a ferocious appetite for human-interest stories' among the media.[253] All of these factors combined to reset the means, parameters and priorities of media coverage of the military, and their repercussions echoed through the media's coverage of the British Army's deepening commitment in Afghanistan.

From 2006 the British Army was drawn into high-intensity operations against the Taliban in Helmand where, in little more than three years, it lost almost 250 personnel. In the face of these severe losses, the government and the military top brass were keen to promote the successes of the British mission in reconstruction, development and improved governance. Then Secretary of State for Defence Bob Ainsworth emphasised the gains made and the lessons learned, telling an audience at the Royal United Services Institute

that the MoD was busy 'attempting to turn recurrent tactical successes into strategic gains'.[254] In a similar vein, the Chief of the Defence Staff, Air Chief Marshal Sir Jock Stirrup, posed himself the question: 'can we actually deliver what's required in terms of improved governance in Helmand with the people who are here at the moment?' He responded without a moment's hesitation in the affirmative:

> *The answer to that is quite clearly yes … you can see by going around at the moment that, where we've got our people on the ground providing security, real governance is starting to emerge very successfully.*[255]

This was not the view of other observers. Robert Egnell of the Swedish Defence University observed that:

> *British troops quickly ran into serious difficulties in Helmand, owing to confusions regarding the purpose of the mission, a flawed intelligence picture and deficiencies in troop levels, as well as tactical mistakes.*

Directly contradicting the claims of both Ainsworth and Stirrup, Egnell notes that despite substantial improvements in performance and resourcing:

> *even now the tactical successes witnessed in Helmand during 2010 are not yet leading to clear strategic gains, owing to a large extent to continued shortcomings within two of the three pillars of ISAF's campaign plan for Afghanistan—governance and development.*[256]

Not surprisingly, the troops were keen to emphasise the price they were paying and their belief that shortcomings in their equipment and logistics had extended their losses.[257] A Continuous Attitudes study of more than 10,000 personnel found in August 2009 that 'only 31% were satisfied with the main equipment at their disposal. A third of senior officers expressed "dissatisfaction", while 28% of senior ranks said that not enough armoured vehicles and helicopters were available'.[258] There was a long and heated debate in Parliament and the media over whether an alleged lack of helicopters meant that British troops were forced to take more ground transport, exposing them to further losses from roadside bombs.[259] Here was a human-interest story crying out to be told—but how to tell it was the problem. Concerned by damaging leaks from Whitehall, stung by criticism from the Army's top brass about its myopic policies in Iraq and

Afghanistan, and challenged by a rising tide of complaints from the men and women on the front lines, the Blair government issued new *Defence Instructions and Notices* in August 2007, through which it sought to 'control the coverage of all military affairs in the news media'.[260] It did this by tightening the rules around public statements and introducing a new set of authorisation procedures. As a result, senior military officers had to seek civilian or ministerial procedures for any public pronouncement, while more junior officers had to refer to their chain of command for permission to speak.[261]

Reporters faced a separate set of challenges. The dangerous conditions in Iraq and Afghanistan ruled out more traditional modes of achieving balanced coverage of the nation's troops at war. The nature of counterinsurgency warfare, in which the military moved among the people in an effort to win their trust, meant that nowhere was safe. Any accompanying reporters were fair game for insurgents and lucrative assets for the kidnapping industry. These conditions meant that journalists were largely reliant on the military units they embedded with for food, transport and security, for the access they afforded and for the information this made available. As in the Second Gulf War, and the Falklands conflict before it, this new proximity generated relationships of trust between individual units and particular defence correspondents. While these relationships ultimately served the interests of both parties, they did not serve the interests of the public or provision a rounded account of what was happening in Helmand. They did, however, undercut the government's efforts to control coverage:

> *When the Ministry of Defence tried to control all public statements coming out of the officer corps, the improved direct contacts between commanders and journalists kept the information flowing, often on a non-attributable basis.*[262]

The determination of the military to have its experiences acknowledged, and the media's imperative to tell that story, were assisted by developments in technology and culture that made it virtually impossible to restrict the flow of information from the front lines back to the public. As Tony Hall noted: 'wider availability and use of … blogs and emails, video from mobile phones and social networking sites makes information, including from operational theatres, more likely to be available'.[263] The MoD was fully cognisant of these changes and busy determining how to harness them to its advantage.

In early 2007, the Director of Communications in the Directorate General Media and Communications, Nick Gurr, distributed the new *Defence Communications Strategy*. Its principal aim was:

> *to maximise the effect of our communications efforts in order to improve understanding and support for Defence and enhance the reputation of the Armed Forces collectively, each Service individually, the Ministry of Defence and its various component parts and MOD civil servants.*[264]

Encouragingly, the strategy argued that new media should not be regarded as a vulnerability or a threat but as a vital tool in enhancing the military's reputation by communicating directly with the public:

> *The way that we communicate must adapt to reflect the culture, attitudes and expectations of our audience. Individuals have access to a wider range of information sources than ever before. We must make our narrative compelling, and use all available means to deliver it, if it is to reach an audience that is bombarded with information 24 hours a day from a vast array of sources. There has been an explosion of media channels, the internet is increasingly a preferred source of information and the importance of new media is growing. The traditional routes used to reach our audiences, both internal and external, are no longer sufficient by themselves. New, emerging channels present an opportunity that we need to utilise to maximum effect.*[265]

In its efforts to 'use all available channels, in particular new media where … increased access to social network sites and blogging provide new opportunities to communicate direct to the public', the unmanaged forms of communication that had so concerned the ministry—the blog posts, social media updates, mobile phone footage and the like—were now identified as 'an increasingly important news source' that it should harness to enhance its opportunities for authentic engagement with its audiences.[266]

In the face of this new assessment of the ubiquity, and utility, of social media, the MoD decided to enlist its personnel in its efforts to enhance the reputation of the services and connect with the public. Its *Online Engagement Strategy*, first issued in 2009, encouraged its employees to:

> *harness new and emerging technologies, new unofficial online channels, and new unofficial online content in order to communicate and disseminate defence and Service messages and build defence and Service reputation, in a way which minimises the risks to personal, informational and operational security, to Service and MOD reputation, and of litigation.*[267]

The question of security and the risk-aversion strategies this entailed was central to the formal guidance issued to personnel. On 1 June 2011 when the MoD launched its 'Think Before You … Share' campaign, Major General John Lorimer, the Strategic Communications Officer to the Chief of the Defence Staff, reiterated the *Online Engagement Strategy*'s encouragement to service personnel to make use of social media, with the onus now on how to inhabit the online world safely:

> *We want our men and women to embrace the use of sites like Twitter, Facebook, LinkedIn and YouTube, but also want them to be aware of the risks that sharing too much information may pose. You don't always know who else is watching in cyberspace.*[268]

As part of this strategy, in association with CTN Communications the MoD produced four short personal security films for broadcast on YouTube, each focused on one of the three armed services, with the fourth directed at the Ministry of Defence's civilian employees. Little more than a minute long, the films use levity to make a serious point about cyber safety. The *Guardian*'s Nick Hopkins described one of the first two films:

> *Two sailors are off for a night out on the town, messaging friends that they are just leaving their ship, and telling them which nightclub they are heading to. The friends are then joined on the dancefloor by two balaclava-wearing men, waving machine guns over their heads. 'Is it just your mates who know where you have checked in?' the film asks. Both videos end with the warning: 'Think before you tweet, blog, update, tag, comment, check-in, upload, text, share.'*[269]

This and a Royal Air Force film have had almost 10,000 views on YouTube. The films did not only impress the public; the industry loved them. In 2012 the campaign won the Gold Award at the International Visual Communications Association Awards.[270] The films were later embedded in the MoD's 'Think Before You Share Online' webpage. Here they were supplemented by advice on security and privacy settings, pictures and video, location services and geotagging and more. The page also included a link to a more comprehensive downloadable *Personal Online Security* guide.[271]

In the light of its commitment to a full embrace of the information age and the weaponisation of its communications technologies, in November 2015 the British Army issued the *Army Information Sub-Strategy (2015–2018)*, which set out its 'Information vision' and its 'required Information outcomes'.[272] Central to this vision was a bold commitment 'to transform Army culture to recognise the value of information as a force multiplier … where its exploitation and protection become second nature'.[273] In pursuit of this goal, the strategy explicitly acknowledged the likelihood of failure and embraced its acceptance as a mark of institutional maturity:

> *The Army needs to take the behavioural leap and start to accept that failure is acceptable in an era of continuous improvement. We should be prepared to try novel approaches and technology on the understanding that failing fast, safe and at a relatively low cost is a success in its own right.*[274]

This enthusiastic adoption of digital media, coinciding as it did with the British Army's drawdown in Afghanistan, led in 2014 to a radical rethink within the MoD of how it deployed its communication resources, how and with whom it interacted and the media best suited to its aims. This in turn resulted in a restructure within the MoD's media departments constituting 'the biggest shake-up to military reporting in a generation'. As the weekly traffic of British reporters through Camp Bastion on their way to or from embeds dwindled to near zero, Christian Hill pointed out that news management teams in the MoD were thinned out and their remaining staff redeployed to work on 'direct to audience communication. In layman's terms, that means the military devoting more of its resources to filming and photographing its own operations, before posting the edited material online'. Under these new arrangements, professional journalists will not disappear from the battlefield entirely, but there will be fewer of

them. The gaps in information provision will be filled by uniformed 'media operators'. Hill spent five years as just such a media operator in the British Army's Media Operations Group (MOG), whose job, he recalled, 'was to film and photograph our troops in action before distributing the material to an increasingly disinterested press and broadcast media'.[275] The media tended to look upon this material with scepticism, regarding it more as PR than as hard news, purposed to promote the Army rather than offer an unbiased account of action in Afghanistan.

The organisational reforms within the MoD were led by Stephen Jolly, Director of the newly constituted Directorate of Defence Communications. Jolly was also a former instructor with 15 (UK) Psychological Operations Group (15 PsyOps). His appointment thus constituted a clear signal from the MoD as to how it viewed its communications relationship with the media and the public. 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'. The concern that this arrangement gives rise to resides in neither the means of news-gathering nor the platforms of dissemination but in the nature and purpose of the 'material' produced by the in-house media operators. In September 2014, as part of the organisational restructure, MOG and 15 PsyOps moved into neighbouring buildings at Denison Barracks in Berkshire and combined their training facilities to form the new Security Assistance Group. It would be hard to think of a clearer statement of the MoD's intent to lower the firewall between news provision and information operations. As Christian Hill notes:

> *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.*[276]

Clearly, the 'direct to audience' material produced by MOG was intended to persuade as well as inform.

Jolly's timing was fortuitous as the media was in the process of quitting the battlefield. The collapse of the traditional media funding model priced all but the best-resourced organisations out of covering distant wars. The targeting of reporters in Iraq, Afghanistan and Syria by insurgent groups bent on garnering publicity through the perpetration of outrages made even the most

valiant reporter think twice, while the killings of James Foley and Steven Sotloff graphically illustrated the perils of freelancing. As Hill notes:

> *In this climate, maybe the MoD has spotted the perfect moment to ramp up its own news-gathering operation. Whether the public will take to the idea of their news coming straight from the military, however, is another matter.*[277]

The principal exponents of the British Army's 'dark arts', 15 PsyOps, had over the preceding years, unusually for such a force, become relatively well known in the UK media. This was largely because the first British servicewoman to die in the Afghan conflict, Corporal Sarah Bryant, who was killed in June 2008 when an improvised explosive device destroyed the Land Rover in which she was travelling, was a Pashtu-speaking member of the unit. Her death raised an array of very public questions about the role and practices of psychological operations in Afghanistan. Research revealed that, given the low rates of literacy among the population and the negligible internet penetration in the country, the most effective channel for PsyOps was not social media but radio.[278] In 2012, 15 PsyOps was awarded the Firmin Sword of Peace, an annual award presented to a unit of the British armed forces deemed to have made an outstanding contribution to improving civil–military relations either in the UK or overseas. The 15 PsyOps unit received the award for their work over the preceding six years in establishing and supporting seven local radio stations across Helmand. The unit's commanding officer , Commander Steve Tatham,[279] was keen to stress that despite the role of PsyOps personnel in their functioning, the focus of the stations' work was open communication, 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.*[280]

One of the young officers engaged in running the stations, Captain Kieron Lyons, had previously 'spent a lot of time planning the "information effect" for large-scale military operations' in Afghanistan. While he acknowledged that the material the stations broadcast had to be truthful and attributable, he was also clear that its purpose was 'to create behavioural change'.[281]

It is notable that once public affairs and information effects are brought under the aegis of information operations, friendly populations, in this case Afghan civilians, are targeted for information effects in the same way as the coalition's competitors.

Just a few months after its formation, the Security Assistance Group was absorbed into the newly formed 77th Brigade, where Tatham's view that information and influence are indistinguishable was a basic operating premise.[282] Named in honour of Orde Wingate's Chindit guerrilla force (part of the 77th Indian Infantry Brigade), which had been noted for its irregular tactics during the campaign against the Japanese in Burma, 77th Brigade was tasked to bring 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'.[283] Part of 6th Division, 'which focuses on cyber, electronic warfare, intelligence, information operations, and unconventional warfare through niche capabilities', 77th Brigade comprises six separate groups: Defence Cultural Specialist Unit; Task Group; Digital Operations Group; Operational Media and Communications Group; Outreach Group; and Staff Corps.[284] When its formation was announced, in January 2015, the mainstream media was obsessed less with its aims or targets than with its tools: 'New British Army Unit "Brigade 77" to Use Facebook and Twitter in Psychological Warfare'; 'British Army Creates Team of Facebook Warriors'.[285] According to then Chief of the General Staff Sir Nick Carter, the purpose of 77th Brigade and its cutting-edge tools was to operate 'smarter'. It would 'play a key part in enabling UK to fight in the information age'.[286]

When Carl Miller, Research Director at the Centre for the Analysis of Social Media, visited 77th Brigade Headquarters in rural Berkshire in the summer of 2017, what he found, 'linoleum flooring, long corridors and swing fire doors', made it look less like the nerve centre of an information-age fighting hub than the marketing department of a cash-strapped small business: 'More Grange Hill than Menlo Park.'

> *One room was focussed on understanding audiences: the makeup, demographics and habits of the people they wanted to reach. Another was more analytical, focussing on creating 'attitude and sentiment awareness' from large sets of social media data. Another was full of officers producing video and audio content. Elsewhere,*

teams of intelligence specialists were closely analysing how messages were being received and discussing how to make them more resonant.[287]

His image of small teams scattered through the building speaking the familiar jargon of digital marketing—'key influencers, reach … traction'—suggested that their tasks were focused more on data capture and analysis than target acquisition. Likewise, the landing page of 77th Brigade's website makes it sound more like a management consultancy than a military command, promoting the transformational, cost-effective, service-driven solutions its people bring to 'the challenges of modern warfare':

77th Brigade is an agent of change; through targeted Information Activity and Outreach we contribute to the success of military objectives in support of Commanders, whilst reducing the cost in terms of casualties and resources. Our outputs are a fundamental part of Army's Integrated Action model. Aside from the delivery and support of Information Activities and Outreach we have a role in planning and advising across the Army and wider Defence.[288]

Yet there was a harder edge beneath this corporate-speak, neatly hinted at in Miller's portrait of soldiers 'having a tea break, a packet of digestives lying open on top of a green metallic ammo box'.[289]

The sharp end of 77th Brigade's social media operations had its origins in July 2016 with the launch of Project DELMER. This set out to establish the organisation and command structure of both an overt social media presence and its non-attributable covert systems and resulted in the establishment of, among others, 77th Brigade's Digital Operations Group (Digi Ops). The Digi Ops Group was divided into two teams. 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'. 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'.[290] According to one of its commanders, the Web Ops team's principal tasks were to 'understand, to monitor, and to engage' online competitors.[291] While they were well-equipped to understand and monitor, in mid-2017 they still lacked the capacity to engage.

While this was partly due to the still-nascent stage of the group's formation, the commander observed that it was also because the sound policy that Joint Forces Command had developed for J1, J2 and J3 (personnel, security and intelligence, operations and plans) was not matched by any equivalent policy for J4 and J5 (logistics, signals and communications). That is to say, just as the US military were struggling to fit the conventional phasing system of planning and operations to the digital environment, so at this point the British had no approval process for digital engagement via social media. As such, though the commander could reasonably claim that, with its focus on monitoring the enemy, 'it is worth thinking of Digi Ops as a Reaper or Predator for the internet, providing constant over watch', his subsequent assertion that it had 'the capacity for the delivery of an information payload' was more aspirational than actual in 2017.[292]

By 2020, the Digi Ops webpage suggested that its capacity to 'deliver influence activity and products across a broad range of communications channels' had been realised.[293] Yet it is clear that its role was focused on public affairs, campaign strategy and broader influencing, engaging in the open source environment with a range of actors, while the delivery of covert strategic and tactical fires had passed to the Task Group, who provided 'the deployable framework to deliver Information Activity and Outreach (IA&O)' through one of its cells or teams.[294] In particular, it is likely that it is the Information Warfare Team that is responsible for payload delivery.[295] The particular nature of the payload, tailored to the specific circumstance and audience, remains secret. However, while Miller saw no evidence of grey or black operations during his visit to 77th Brigade, he suggested that the work of GCHQ's Joint Threat Research Intelligence Group (JTRIG) provides a model for the sort of work undertaken by 77th Brigade. What we know about JTRIG's work comes from a series of slides, leaked by Edward Snowden to Wikileaks in 2013, which reveal the nature of the operations it undertakes, the tactics it employs and the tools it uses:

> *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.[296]

Though we know little about the content of 77th Brigade's messaging, we do know something about how its Digi Ops teams are organised. Operating teams comprise a Team Leader, usually a senior Non-commissioned Officer and two Digital Engagement Operators (DEOs)—Operator-one clicking, searching and monitoring, and Operator-two providing overwatch, analysing material and answering questions raised by Operator-one, referring thornier problems or seeking approval for certain actions to the Team Leader. The team's designated duties are to monitor online systems, manage personas, trace potentially hostile actors and identify targets. The teams are commanded by a Social Media Targeting Director, who communicates orders and oversees their prosecution. These orders take the form of a mission directive with operating instructions. These are issued by the MoD and are reviewed on a weekly basis. DEOs are directed to 'push, amplify or avoid' material. An Operations Officer, a Major or equivalent, is in charge on a daily basis, but 'within these parameters operators are given the freedom to act'.[297] This almost-embrace of mission command, 'the conduct of military operations through decentralized execution based upon mission-type orders', reflects 77th Brigade's efforts to find a balance between the demands of the top-down command structure and the need for bottom-up spontaneity and timeliness of response from the operators who are engaged in the social media space.[298]

While this team structure was established to demonstrate proof of concept, DEOs and their commanders were considering how to operate more effectively by tweaking the structure of the team. In particular, they were keen to add a third DEO to the team whose role would be to engage with operators one and two while also exploring capability development initiatives. The need to constantly train, develop and operate left the DEOs with no space for reconceptualisation, lateral thinking or other left-field approaches. A staff member dedicated to capability development could help ensure that the team were kept abreast of constant shifts in the social media space.

DEOs were largely recruited from, or had a background in, signals and intelligence. Beyond a basic aptitude for social media, recruits were required to demonstrate that they had, or could develop, skills in five key areas:

1. Analysis—the ability to filter, appraise and analyse material
2. Creativity—the capacity to identify what will work on a given platform and to make it do so
3. Web science—an understanding of both the human terrain and the online environment within which they are working
4. Cultural empathy—an understanding of the cultures they are engaging with and the behaviours of the people they deal with online
5. Language and culture—the capacity to develop expertise in one or the other.[299]

Members of 77th Brigade dismissed the assumption that DEO roles could be filled by young tech-savvy digital natives. One NCO noted that while such recruits 'use the technology they do not understand the cultural landscape within which it sits. They need experience as well as technical expertise'.[300] He pointed out that the average age of the staff in Digi Ops was over 30.

Once selected, as of 2017 there was no formal training program for DEO recruits. All training was bespoke, cobbled together from existing instruction packages in military planning, electronic warfare and intelligence, coupled with the local knowledge of the foundation team. The US training system for DEO equivalents takes 18 months, including six months of dedicated language training and six months or more of cultural immersion. Senior officers in 77th Brigade noted that the ideal training program would be an intensive three- to four-month course, offered in-house—though this was not yet a realistic option.[301] A more immediate problem was that the traditional practice of specialist rotation threatened the brigade's ability to develop deep and genuine expertise. As the commander noted, given that 'it takes twelve months of a twenty-four-month rotation to produce a competent specialist', under the established three-year rotation, personnel would move out of 77th Brigade at the very point at which they had mastered the expertise needed to operate effectively in the information environment. It is hoped that including the DEO on the key skills and experience classification will enable long-term specialisation.

To ensure a ready source of professional expertise, a former commander of 77th Brigade brought in Special Reserves from civilian media, marketing and public affairs who were familiar with and had experience working in the information environment. In the opinion of Major General Jonathan Shaw, former Assistant Chief of Defence Staff (Global Issues), the full participation of civilian experts in the information domain was vital:

> *In today's battlefield, the military are minor players in a game in which most of the skill set and capability is civilian. The real experts in this field do not reside in the British Army and, as a nation, we will have to do more to ensure we make use of civilians' skills … The information campaign needs to be civilian-led.*[302]

However, though their use remains high, with the ratio of permanent to Reserve staff at around 60:40, there is little evidence, at this point, that reservists have brought significant innovations from the private sector or exercised any influence on the development of training or doctrine.

As Shaw's remarks make clear, the information environment is a whole of society and thus whole of Army concern. As such, it is vital that guidelines for the appropriate use of social media are regularly refreshed. While the Army encourages its personnel to make use of, and has actively invested in, social media as a key capability, it has also consistently maintained a high level of risk aversion around social media. In the wake of the murder of Fusilier Lee Rigby in May 2013, and the use of social media by his killers to publicise and justify their actions, the MoD was concerned about the possibility of copycat crimes. In the immediate aftermath of the attack it advised service personnel 'that uniform should not be worn by those travelling alone, or on public transport as a "common sense precaution"'.[303] The order was later rescinded, but the MoD remained vigilant. In 2016 when an attempt was made to abduct a serviceman out jogging near RAF Marham in Norfolk, British soldiers were instructed 'to "scrub" their social media accounts of uniform pictures and instructed to jog in pairs to avoid being targeted by jihadists'.[304]

The Army's most recent 'Social Media Guidance' is headlined by a two-minute video highlighting 'Dos and Don'ts'. This contains a range of commonsense instructions about upholding and promoting Army values and observing basic precautions to ensure that personnel do not inadvertently supply potentially useful information to competitors.[305] Its key points can

be downloaded from the website as a poster. The more detailed strategy *#DigitalArmy: Using Social Media in the British Army*, released in September 2018, encourages personnel to make use of social media, identifies the distinction between personal, official and corporate accounts, and outlines the responsibilities that come with the operation of each. While the 12-page document identifies social media's potential for individual and service promotion, one of its longest and most detailed sections focuses on 'How to Set Yourself Up Properly' and 'How to Have Your Say Securely'—thus concerns about 'Operational and Personal Security' remain at the heart of the policy:

> *While social media offers an excellent means of communicating with friends and colleagues, it also presents serious threats to security. You must not publish anything that threatens any individual's personal security or breaches operational security. When communicating on social media:*
>
> *Photographs of yourself and colleagues in uniform or in obviously Army locations may not always be advisable—think carefully before posting them.*
>
> *Do not post details about your work that could be used by criminals, terrorists or potential enemies to harm you or your colleagues.*[306]

Though fear of a damaging breach via social media continues to preoccupy the Army and the MoD, it is clear that the British Army has made considerable strides into the digital environment, ensuring that on top of personal accounts, social media is widely used in an official and corporate capacity throughout its structure:

> *Not everyone in the Army uses social media in the same way (or at all) but the reality is that most of our workforce will have personal accounts on one or more social channels. In addition, many appointment holders (eg Commanding Officers, Regimental Sergeant Majors, Brigade Commanders, General Officers Commanding, ECAB Directors, Defence Attachés/Advisers) have one or more official accounts.*[307]

Clearly, the British Army has determined that the risks of possible security breaches that widespread use of social media brings are more than outweighed by the advantages of a fully connected digital Army and the capability this makes available.

Yet for all this progress, an October 2016 policy briefing 'Social Media in the Armed Forces', arising from a workshop convened by the Economic and Social Research Council funded Partnership for Conflict, Crime and Security Research, identified a number of cultural issues that the MoD and the Army continue to struggle with. These include: 'a disconnection between military policy and social media use, with a clear generation gap in the use and understanding of social media'; and the fact that 'MoD reticence to engage in social media debate about military policy leaves the field open for others to define the terms of the defence debate'. The briefing notes: 'Assessing the effectiveness of social media use in terms of concrete outcomes is very difficult, and at odds with a culture which needs demonstrable outcomes to justify funding.'[308]

In identifying these issues, the briefing draws attention to the uneasy fit between the command structure of the military organisation, with its attendant culture of hierarchy, and the radically democratic forms and uses of social media that recognise neither rank nor territory. The message is clear: a full embrace of social media by the armed forces will demand some challenging changes in defence and military culture. Social media is not merely a handy weapon that the military can take up, use and lay down as it wishes, leaving its existing systems largely untouched. It is part of a wave of cultural change shaping what, how, with whom and why we communicate that is sweeping the world and radically reshaping individual identity and social formation as it goes. The British Army, like its NATO associates and partner militaries from around the world, mirrors the society it serves. The challenge that it faces is to determine just how far it is prepared to go to adapt its culture and bend its practices to meet the demands and reap the benefits of full social media engagement.

Chapter 6: The Israel Defense Forces

The conventional military that has most actively embraced mission command in its uses of social media and successfully integrated it into its systems and operations, while adapting its structures to the organisational logic of the digital age, has been the Israel Defense Forces (IDF). Here, the devolved enactment of the commander's intent via social media has extended beyond the military, as Israel has enjoyed unusual success in mobilising its civil support base, both domestic and dispersed, to support its campaigns and promote its core messages via online social sharing platforms.

The extent to which the IDF can be regarded as a 'conventional' military is hotly debated. It occupies a central and unusually pervasive role in Israeli civil society. Born into war, Israel 'has confronted constant military threats to its survival since 1948'.[309] Surrounded by hostile neighbours, the IDF is the nation's shield and every citizen is required to contributes to its defence.[310] Military service is compulsory—three years for men, two for women—after which men are automatically transferred into the reserves, or *miluim*, which constitute the main Army force and demand between 20 and 30 days of service per year until the age of 55.[311] This obligation extends to all citizens, not least media workers, who have all done military service at one time or another and are still bound by their reserve commitments. In fact, as Yoram Peri notes, the IDF:

> *serves as the major training college for journalists. For many years, Army Radio,* Galei Zahal*, was the biggest and most productive school of journalism in Israel, followed closely by the IDF journal,* Bamahane*. Dozens of journalists, editors, and anchors as well as producers, who reached the peak of the Israeli media in all the news organizations, had done their military service in IDF media organizations.*

Steeped in the cultural norms of the IDF, it is likely that many media workers felt the same as Ido Dissenchik, the editor of Israel's second biggest selling Hebrew newspaper, *Maariv*, who, during the First Gulf War, told an interviewer: 'I am first of all an Israeli and an IDF reserve officer, and only then a newspaper editor.'[312]

Due to their service obligation, most Israeli men and many women 'spend a significant part of their lives in the IDF'. As a result, their experience of 'being part of the community of citizens is dependent upon a traditionally non-civil activity: military participation'.[313] The constant traffic between civil society and the armed forces means that in Israel, far more than in other countries, 'civilian-military boundaries remain porous or … virtually non-existent'.[314] Consequently, the latest corporate innovations, cutting-edge technology and novel social trends are promptly registered within the IDF. In an effort to keep abreast of the latest advances in the field, the head of one of the IDF's social media teams noted that while she and her staff monitor what their military colleagues around the world are doing with social media, they 'are much more inspired by general industry and pop culture'.[315] As a consequence of this persistent and pervasive intermingling with civil society, while it might look like a conventional military, the IDF's organisational structures are necessarily loosened by the regular flow of part-time reservists into and out of uniform and the shifting civil society norms they carry with them—not least a more established culture of bottom-up innovation. These unique features have enabled the IDF to adapt itself to War 2.0, adopt social media into its systems and operations, collapse the virtual and real spaces of war and so make it, arguably, the most potent conventional force operating in the information environment. However, its now comfortable habitation of the digital domain was achieved only after a protracted struggle.

The IDF has long been admired for its command of the information environment in its domestic and regional conflicts and is often held up as a paragon of organisational agility, quick to respond to changed circumstances and adapt the latest capabilities to its advantage. It was among the first militaries to engage in cyber conflict when, in September 2000, then Prime Minister Ariel Sharon's incendiary visit to Temple Mount set off the Second Intifada, convulsing the streets of Israel and the occupied territories. Over the following days, hackers from Israeli and Palestinian groups, as well as Hamas and Hezbollah, took the fight to the internet and the 'cyber intifada' moved online:

> *The first attack was launched by a group of Arab hackers against major Israeli government sites. Israeli hackers, however, did not wait long to respond—soon thereafter, they posted the Israeli flag on the main page of Hezbollah's website, together with a sound track glorifying Zionism. Another Israeli hacker posted the Israeli flag on the same website, but this time the word 'war' flickered and swayed across the page, accompanied by a message in English and Hebrew that said: 'This page was uploaded to protest against Arab attacks of the past few days.'*[316]

Over the succeeding years, Israeli and Palestinian hackers waged a never-ending, tit-for-tat struggle against their online competitors:

> *The cyber war is a constant dialogue between hackers who support both sides. Each time one of the two parties scores a success in penetrating an enemy website, the other quickly tries to score a counter coup with help from its own supporters.*[317]

In November 2000, anti-Israeli hackers breached the website of the American Israel Public Affairs Committee; in 2001, Israeli hackers defaced the website of Hezbollah's official television channel, Al-Manar, taking down the website of the official Palestinian news agency, Wafa, later in the same year. In recognition of the increasing power of the cyber domain, when Israel reoccupied the West Bank in 2002 it not only targeted traditional communications assets, destroying Palestinian television and radio stations and their broadcasting and transmission equipment, but also paid special attention to the offices of internet service providers and the networks that supported them.[318]

It is notable that any early success Israel enjoyed in the cyber domain was the work not of the IDF itself but of a dispersed network of civilian hackers acting in support of the state. This circumstance points to a larger, if less well-known, truth about the IDF: 'despite its glorious reputation for being one of the most nimble and adaptive armies, and despite the unorthodox and innovative enemies it is facing, the IDF has long underperformed in its public communication activities'.[319] Nowhere is this clearer than in its tardy and reluctant advance into the digital domain. In the years before the outbreak of the Second (Al-Aqsa) Intifada:

> *The IDF's media strategy … was characterized by a limited perception of the Spokesperson's Office (later Division)'s role as a means of conveying information about military activities and operations to both Israeli and international audiences … The media's role was seen by the military as a mediator, expected to reflect the 'reality' on the battlefield as conveyed by the military officials. This functionalist approach resulted in a reactive, ad hoc, defensive and denial of access approach to media management that centred on creating media blackouts and limiting media access to conflict zones.*[320]

Over the succeeding years, the IDF's responses to, relations with and uses of the media underwent profound transformation. Firstly, it moved beyond a defensive approach to the media, determining 'whether it is possible to win the battle without winning over the television screen', to consider instead 'how to win on the television screen'. Its new conception of the media's role in contemporary conflict ascribed 'central importance … to influencing the perceptions of various target audiences as a major component of warfare', thus ensuring that 'media considerations … became part of the operational planning processes'.[321] In 2005, as it disengaged from Gaza, the IDF's approach to the exercise of military force was increasingly subject to media logic. Its media strategy, 'aimed largely at influencing and shaping public opinion', included the use of 'embedded journalism, media campaigns and practices for establishing and preserving the consensual images of the IDF'.[322]

Yet in the first decade of the 21st century, as the IDF focused on using the mainstream media to burnish its image in the eyes of the public, new communications technologies were reshaping the information ecology and the IDF was slow to grasp how the accelerated pace of digital networks was leaving the timelines of old media for dead.[323] Its handling of the Hezbollah missile attack on the Israeli Corvette INS *Hanit* illustrated the costs of inattention to the changed media landscape. On the night of 14 July 2006, in the first days of the Second Lebanon War, the *Hanit* was struck by a Hezbollah anti-ship missile while patrolling off the coast of Beirut, killing four Israeli sailors.[324] The first that the IDF's public affairs leadership heard about the strike was when they were questioned about it during a press conference. Though the IDF Spokesperson, Brigadier General Miri Regev, immediately called the Chief of the Navy for a briefing, it was already too late. The Navy

took ‘about ninety minutes to establish a full operational picture of what had happened: it took Hezbollah fifteen minutes to broadcast a video of the attack and dominate the Israeli media coverage’.[325]

Throughout the Second Lebanon War (2006), Hezbollah out-thought and outgunned Israel in the digital domain. As Kuntsman and Stein note, the war was notable as:

> *the first instance in the history of the Arab-Israeli conflict in which virtual and real battlespaces were actively conjoined … Israeli hackers used Google Earth to identify areas where the Israeli army had successfully targeted Hezbollah’s positions, while Hezbollah employed the same service to identify Israeli-wrought destruction in civilian areas.*[326]

In the mainstream media, the war was notable for the ‘sheer scope of IDF media exposure … compared to what the Israeli public had become accustomed to in previous wars and in times of normalcy’. The unprecedented scale and unremittingly promotional nature of this exposure generated ‘considerable criticism towards the Israeli media and what was perceived as excessive openness on the part of the IDF’.[327] In Israel, the war was widely regarded as a defeat. After the cessation of hostilities the government launched a range of inquiries into the conduct of the war and how its communications aspects were planned, managed and prosecuted.[328] The main issues identified in the subsequent reports were: ‘first, the absence of a clear message on the part of the political and military leaders, and, second, a lack of coordination between the various agencies responsible for getting out that message’.[329] The military’s investigation into the performance of the armed forces was:

> *pointed in its criticism, castigating the Israeli army for a failed and bungled military effort, and contending that lack of media coordination and preparedness had been among the war’s chief secondary failures. Indeed, some critics credited Hezbollah with decisive victory on the media stage—in part, due to superior usage of cyberspace to deliver its political message to international audiences—while the IDF was faulted with an erroneous focus on traditional modes of information dissemination and psychological warfare (for example, dropping leaflets, jamming broadcasts, etc.). For their part, Israeli soldiers on the battlefield were accused of*

> *compromising national security by means of casual cellphone usage, which was thought to contribute to successful Hezbollah intelligence-gathering. Many of Israel's internal critics would argue that the national media had collaborated in the military failure through public criticism of IDF strategy, thought to harm army morale, and by means of lax coverage that publicized sensitive information about IDF coordinates and strategies, some of which was broadcast to viewers in real time.*[330]

In the wake of this painful self-examination, the IDF publicly adopted a new media strategy. Pursuing a 'modest, measured and reserved spokespersonship operation', it sought to wrest back from the fourth estate 'control over the flow of information and media framing and to reduce public expectations'. The central aim of the strategy was to bring about 'a significant lowering of the IDF's public profile so as to convey a message that that the Army was focused on implementing the lessons learned from the last war rather than engaged in self-promotion'.[331] The IDF's profession of born-again humility was disingenuous. When, in December 2008, it launched Operation Cast Lead, its assault on Gaza:

> *the Spokesperson's Division viewed its role in the campaign not only in terms of executing the IDF's media policy, but also as part of the IDF's strategic effort to rehabilitate the army's public image, restore public trust in its professional abilities, and overcome the public sourness regarding the Lebanon War.*[332]

To this end, the Spokesperson's Division was fully integrated into the planning process leading up to the operation, 'enabling it to prepare in advance diverse media content that was ready for immediate dissemination once hostilities broke out'. To ensure the success of its media strategy the IDF had to own and control the message; it thus instituted a range of measures to ensure that 'most of the information reaching the Israeli public via the Israeli media originated from official army entities'.[333] Though the media strategy showed every mark of the coordination and preparedness it had lacked in Lebanon, it was ill-conceived and very nearly disastrous. Banning its personnel from using mobile phones may have reduced the incidence of security breaches and ensured consistent messaging from within the armed forces. The IDF's closure of the Erez Crossing was a major mistake. Not only did it preclude Israeli and international reporters

from accessing Gaza; it needlessly antagonised them in the process. As a consequence, however consistent the Israeli narrative, the media remained stubbornly unreceptive to it. Officers in the IDF's Spokesperson's Unit believed that, furious at their exclusion, the international correspondents unofficially boycotted IDF materials: '"We're not doing another story on rockets going into Israel" was the message [they] kept receiving'.[334] In their place they ran stories, communicated via mobile phone and social media from within Gaza, about the IDF's targeting of civil infrastructure and the innocent people who inhabited and used it. The IDF's tactics unleashed a 'tidal wave of international criticism' which washed through mainstream and social media as the IDF again faced defeat in the digital battlespace.[335] Hamas had clearly learned some important lessons from Hezbollah's victory in Lebanon about the power of digital messaging in being first with the story and so setting the news agenda.

In fact, the Spokesperson's Unit had abundant material to counter Hamas's digital assault, including cockpit video showing Israeli Air Force jets aborting attacks when civilians came into view, secondary and tertiary explosions in mosques when stored explosives detonated after air strikes, and the firing of rockets from populated areas. While some younger officers in the Spokesperson's Unit were keen to post this material online, they ran into a generational obstacle. The middle-aged officers who commanded the IDF's communications operations could not see the military applications of what they regarded as an entertainment platform:

> *Facebook had only just opened up, and it was considered a toy for kids … YouTube was the same. They didn't think of it as a dissemination tool that could be effective.*[336]

The commanders were not only ignorant about the potential of social media; they were afraid of the risks it carried:

> *Up to the summer of 2008 there was still no understanding at the command level of the Spokesperson's Division of the potential of this domain. Additionally, there was an apprehension of the risk of investing resources that the IDF believed would only produce dividends far into the future.*[337]

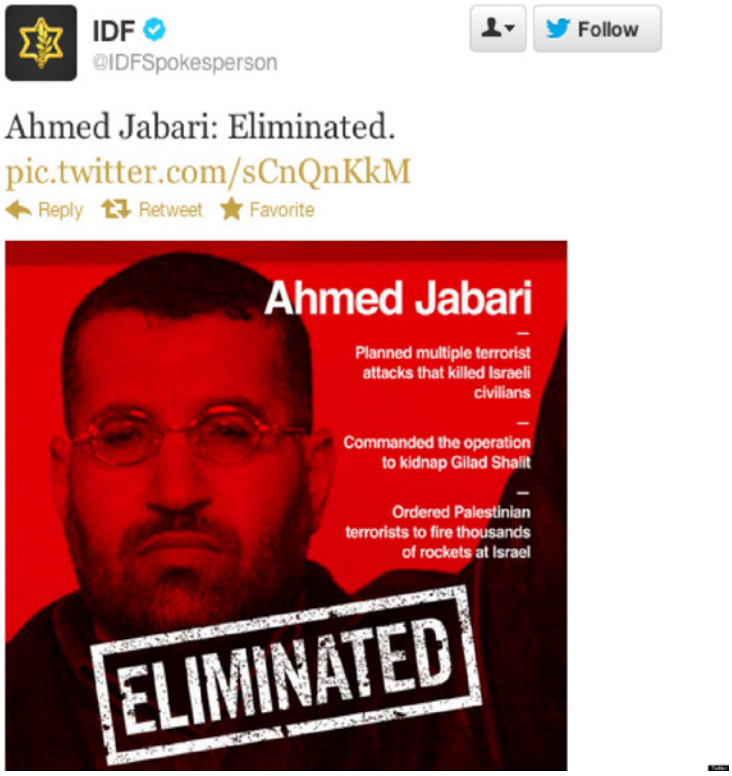
But the future was already here. Six months earlier, with a colleague on the North America desk of the Spokesperson's Unit, a junior officer, Aliza Landes, had written a position paper on the importance of new media as an influence vector that was highly critical of the IDF's failure to move into the digital battlespace. The paper was never published and her suggestions 'remained stuck in the chain of command'.[338] Now, determined to get the Israeli story of Operation Cast Lead out, and the IDF into the virtual domain, Landes began attaching the video clips to her blog and emailing them to family, friends and contacts at home and abroad:

> *With the mainstream media alienated, and with no official social media platform to use, Landes was, in effect, now acting as a mini Spokesperson's Unit within the unit, focusing on the new media she so desperately wanted to reach.*[339]

As it became impractical to upload such huge files, Landes was given permission by the head of the Spokesperson's Unit Foreign Press Branch, Lieutenant Colonel Avital Leibovich, to set up a YouTube channel for the video material she had received. Within a fortnight, the 40 or so videos that the IDF had uploaded to its YouTube site had garnered more than 1.7 million views. Among those watching were the commanders of the Spokesperson's Division, who finally began to grasp the potential of the digital domain. Landes' innovation revolutionised military media practices within the IDF. Her superiors realised how well suited the medium was to 'enabling better control of the message and allowing the IDF to directly influence diverse target audiences', thus opening a vital new front in the struggle for international public support in the Israeli–Palestinian struggle.[340]

Over the following years the IDF moved steadily into the information domain, establishing idfblog.com in 2009, a Flickr account in 2010 and an official Facebook account in 2011, while in 2012 it enabled live-streaming and launched its first interactive game, *IDF Ranks*. In late 2012 the IDF went back into Gaza and, over the course of Operation Pillar of Defense, 'the development of the new media domain in the Spokesperson's Division, reached full maturation'.[341] The operation began with both a physical and a virtual bang when, on 14 November 2012, the IDF took to Twitter to announce that an Israeli airstrike had killed Ahmed al-Ja'bari, Chief of the al-Qassam Brigades, Hamas's military wing in Gaza—making it 'the first military campaign in the world to be declared via Twitter'.[342]

343

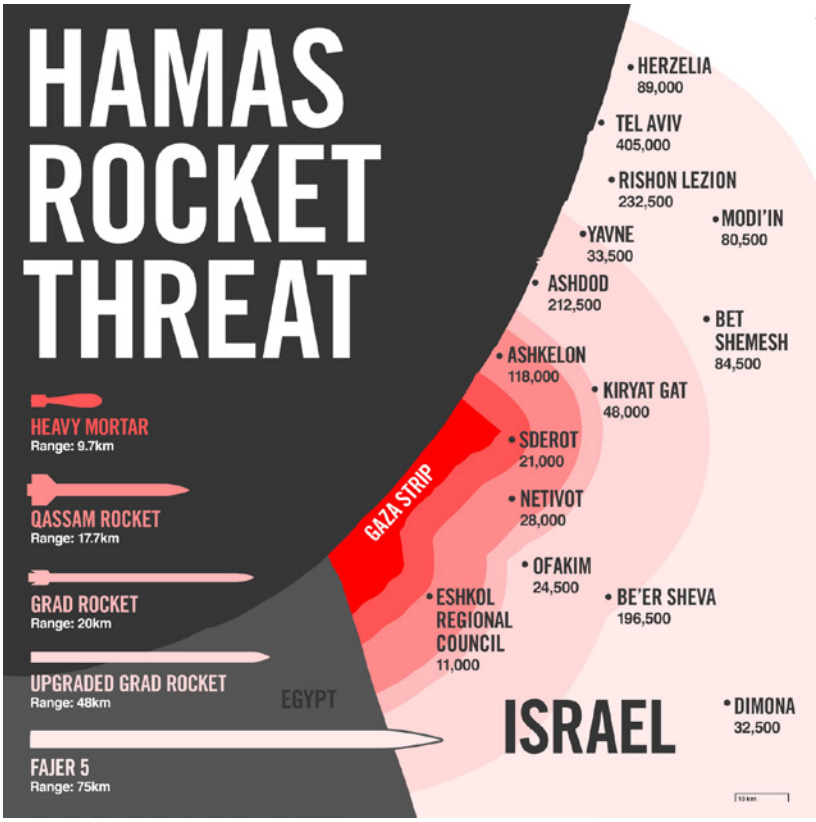


Soon after, the Spokesperson's Division uploaded video of al-Ja'bari's assassination to YouTube, which it linked to appear on a number of its other websites. A succeeding Tweet from the IDF recommended 'that no Hamas operatives, whether low level or senior leaders, show their faces above ground in the days ahead'.[344] The al-Qassam Brigades responded with the announcement of a counteroffensive, Operation Shale Stones, and a Twitter threat of their own: 'Our blessed hands will reach your leaders and soldiers wherever they are (You Opened Hell Gates on Yourselves).'[345]

Over the rest of the day the IDF 'uploaded to YouTube video clips documenting strikes against Hamas installations', while posting to its website 'updates every few minutes on what was happening in combat'.[346] With its power to source material from the battlefield, swiftly upload it to traditional and new media platforms and flood the internet with its narrative of the operation, the IDF exercised overwhelming information superiority, which it used to structure and fine-tune the war's reality. Over the course

of the campaign the IDF relentlessly tracked social media responses to its actions. Thomas Zeitzoff argued that the IDF was highly sensitive to public opinion and that the number of likes and re-tweets its posts garnered directly affected its targeting.[347] The IDF's successful coordination of digital with military action, its power to exclusively source and promptly disseminate information from the battlefield to traditional and new media platforms, potently integrated the cognitive with the physical battlespaces. Dominating the physical terrain, the IDF was also able to govern the cognitive domain, shaping both the narrative and the perceived reality of the war.

For the Israelis, the collapse of the real and virtual battlespaces facilitated closer integration of bottom-up domestic enthusiasm for the cause with top-down coordination of public messaging. Widespread public participation in Operation Pillars of Defense via social media reinforced the permeability of the civil and military spheres in Israel and was used to promote to domestic and international audiences two key themes of the nation's struggle—one centred on the potency and precision of IDF weaponry, the other on 'the suffering within Israel'.[348] The danger faced by the country and its people was illustrated in a series of images distributed on social media by the Spokesperson's Unit mapping the reach of Hamas rockets and the numbers of Israelis under threat from them.[349]



A 16 November tweet depicting missiles raining down on Sydney, London, New York and Paris defiantly asserted Israel's 'right to self defense'. It invited international observers to consider 'What would you do?' in this situation, while urging its supporters to carry the message to the online community and 'Share this if you agree that Israel has the right to self defense'.

351

Sharing online was, for the millions of Israel's geographically dispersed supporters, their opportunity to enter the digital conflict environment and play an active part in Operation Pillar of Defense. Throughout the eight days of the operation, and for many months afterwards, pro-Israeli groups used the full spectrum of social media platforms 'to share patriotic testimonials, to voice hatred towards anti-war "traitors," to track sites of wartime devastation within Israeli territory, and to employ hashtags to catalyze solidarity, all capitalizing on the narrative of Israel victimhood'.[352]

On 15 November 2012, the Ministry of Public Diplomacy set up the 'Israel Under Fire' project on Facebook, providing its supporters with a dedicated platform for their advocacy and encouraging them to utilise the information provided on the site to take the fight to the online world of public opinion:

> *Our mission is to show the truth about Israel and how it's Under Attack by Arab neighbours as well as by Palestinian terror groups and parties. We'll inform you and you can help us share the truth to the world.*[353]

This project, which continues to run with the direct support of the Prime Minister's Office and the Ministry of Foreign Affairs, is regarded as an exemplary form of *hasbara* (public diplomacy) which, as Reuven Ben-Shalom notes, constitutes 'Israel's main "soft power" tool, aimed mainly at external audiences'.[354] During Operation Protective Edge, in 2014, Matthew Hall described the efforts of students from one private university north of Tel Aviv in 'challenging propaganda from Hamas':

> *Inspired by the role of social media during the Arab Spring and boosted by the support of the Israeli government and Israel Defence Force, student volunteers at the Interdisciplinary Center (IDC) Herzliya, a private university north of Tel Aviv, are waging their own propaganda war countering online anti-Israeli sentiment. Volunteer groups include a team that translates messages from Hebrew into 30 languages and a graphics team creating charts and images to be distributed via Facebook and Twitter. There is also a video editing department and a talkback team.*[355]

Peer-to-peer persuasion, it was argued, freed such engagement from the taint of organised information shaping and lent Israeli advocacy a human face. Facebook and Twitter thus extended Israel's mass conscription policies online, providing a virtual space within which its dispersed community of sympathisers and supporters could take up its cause and participate in its struggles. Harnessing authentic testimony with immediate images, and giving them the reach and publicity afforded by official endorsement, an initiative like 'Israel Under Fire' provides an exemplary illustration of how to successfully weaponise social media.

Between Operation Cast Lead and Operation Pillars of Defense, the Spokesperson's Unit formalised the role of social media within its communications structure. In September 2012, it appointed Avital Leibovich as its Digital Spokesperson and Director of its Interactive Media Branch.[356] Here, she commanded a 35-person team of tech-savvy young IDF personnel who 'tweet, Facebook, blog, build apps, edit videos, snap Instagrams, and update Google+ posts'.[357] The Interactive Media Branch operates on more than 30 platforms, in six languages: English, Hebrew, Arabic, French, Spanish and Russian. Its Twitter account has more than 1 million followers, while its Facebook page has more than 2.2 million followers and more than 2.1 million 'likes'.[358] The 'Social Media' page on

the IDF Spokesperson's Unit website invites young Israelis anywhere in the world to join its International Social Media Desk, a virtual community of online 'conscripts', to advance the state's official messages around defence and security and to counter anti-Israeli sentiment wherever they find it online.[359]

For young Israelis seeking to fulfil their military service in the Spokesperson's Unit, competition for places is fierce and selection and training are rigorous. A junior officer in the unit detailed the process: 'First of all, would-be recruits go through the intelligence and behavioural tests that are part of the general draft process.' The Spokesperson's Unit requires that 'anybody who serves here has the highest scores in all of those different criteria'. Applicants then go through a separate testing process featuring 'a more customised intelligence exam' with a focus on 'behavioural issues, group dynamics leadership, initiative' and an interview. At these interviews, the officer observed, she was looking for:

> *people that are comfortable and excel in group settings. But also, people that look at the world in an interesting, creative way, and that aren't necessarily always a big fan of rules, which in a military context, is always an interesting balance.*

She was looking for recruits who were prepared to push the boundaries and would not take 'No' for an answer, noting that such traits are:

> *critical here. It's part of the culture in the whole unit, to have people that push. I mean, the answer [to a refusal] is, "No, it's not OK … 'Why? Why is it no?" And that's incredibly important here.*

Once accepted, recruits are sent on a three-month in-house training program. In the process of designing this training, the staff in the Spokesperson's Unit recognised that trainees were digital natives and so familiar with the technology, the platforms and their differing affordances. Accordingly, they asked themselves:

> *What do you need to teach an eighteen-year-old who's just finished high school, … in three months, to be able to prepare that person to Tweet on behalf of IDF, or to be a spokesperson for a regional brigade and be able to interact with leading journalists? What do you do there?*

They determined that the recruits needed to understand two key things: the nature of the organisation they were joining, and how one might best represent and promote it in a range of media outputs. Accordingly, the training ensured that soldiers moved on to their postings with 'a very deep understanding of the military as a whole' and a strong grasp of how to build a media product 'for all of those different platforms'—an understanding of, for example, 'the difference between trying to do … a piece in the biggest Israeli newspaper for the weekend, versus, a TV piece for an international audience'.

The Spokesperson's Unit delegates junior officers to oversee the management of its social media presence. They, in turn, empower its young personnel to produce the material that will resonate with its target audiences. This approach, around rank, age and the perceived risks of engaging in social and digital media, stands in stark contrast to that of more conventional military cultures. As the officer observed:

> *All of my soldiers that are in the social media department here range in ages between eighteen to, twenty-three. Twenty-three is like, on the old [side] … I'm twenty-nine, my deputy is twenty-five. We're a bit older again. We're not, thirty-five, forty, we're not at that life stage. We're a bit older. The head of the branch for instance is usually around forty years old. So, leadership tends to be a bit older. But I think that if you want to have creative, innovative, unique content on social media, it can't be done by forty-year-olds.*[360]

Under mission command, the social media operatives are given broad directives about the narratives to prioritise and the freedom to generate content and employ the most appropriate platforms to post and disseminate that content. When not responding to an incident or a crisis, members of the team are expected to initiate their own stories. For example:

> *[O]ne of the soldiers … in the English department will say, 'OK, I want to write an article for a blog, let's say about ISIS, in Sinai.' So, she will reach out to the IDF Spokesperson's representative in the Southern Command … the Southern Command person will say, 'Great … you do a phone interview with one of our intelligence officers.' She'll write the article, then if it's relevant for the, let's say, French audience or for the Spanish audience, one of the soldiers there will translate it. Or … the photographer will go join an operational activity somewhere,*

let's say in the West Bank, bring the content back and then it will be adapted for each audience. But there's a lot of overlap that goes on, which is just wonderful … it's content that can be used for all of the different platforms. And then he or she will also use it in all of the different social media platforms, different platforms in terms of language, and also different in terms of, blog, Instagram, Twitter, video. So, we try to be as efficient as possible, and to squeeze out as much as we can from a single interaction.

IDF Interviewee 1 claimed that the fact that this approach was possible, let alone successful, was because the chain of command in the IDF, or at least in the Spokesperson's Unit, was more condensed and fluid than that in other conventional militaries, enabling better adaptation and integration:

[T]he bureaucratic level of approval is, I think, much thinner and much narrower than it is elsewhere, which can sometimes be a disadvantage, but I think that when you're trying to introduce Something new or start something new, it's definitely an advantage.[361]

The combination of these factors ensures that IDF initiatives, or responses to a specific event, are relevant, timely and coordinated, and that the bottom-up spontaneity of the social media operators is married with the top-down direction of command.

Delegating so much responsibility to junior officers and conscripts brings inevitable risk. IDF social media has developed a cultural tolerance for useful failure, a readiness to accept and learn from mistakes. As IDF Interviewee 1 noted:

I think that a big advantage that we have is the understanding that … sometimes mistakes happen, like it happens … It's OK. You have to breathe deeply. No one died. Everything is fine. We're not cardiologists that have made a mistake in the operating room. And it's to learn and to move on. And here we very much have a culture of looking back and trying to learn from errors that are made.

So, if that happens and the soldier who is dealing with it will have to do, kind of an after-action assessment to understand, what were the processes, what were the steps that were taken, what were the issues in that process, what could we have done differently? And then we talk about it. And then honestly, we just move on. Use it as a learning experience, and we just move on from it.[362]

If the organisation is intolerant of risk-taking this may minimise risk, but at the cost of paralysed operators and bland product:

I think that, if you're constantly afraid of making a mistake, you will be paralysed, and your actions will be paralysed, and you will only play it safe, and you'll generate like, completely non … You know, it'll be 100 per cent OK work, but it's going to be pretty boring. And I think, being able to take the risk in an environment that encourages risk-taking, is really really important for that.

Indeed, the principal frustration that IDF Interviewee 1 expressed was not the excess but the lack of risk-taking in her area:

I would like to take more risks, in terms of the content that's going up. I see, probably one of the biggest advantages that we have is being able to show people, like, who is this IDF soldier? I think … we really humanise, I guess, who we are. So, I'd like to do a lot more, riskier, deeper kinds of projects, or pieces, of, you know, following a soldier from his recruitment through his whole training process. Or, being able to create more of a sense of identifying with the character or person, for our followers. I think going into the deeper … And doing things that are, again that are a little bit riskier, because these things are very unscripted … I like the unscripted, I think the unscripted is much better. It's just much riskier.[363]

The digital wave that Aliza Landes initiated for the IDF, and its enthusiastic adoption within the Spokesperson's Unit, offers a textbook case of the organic uptake of social media. Its introduction and original deployment, born of crisis and necessity in active operations, were bottom up, initiated and pursued by motivated individuals of junior rank with the support of enlightened mid-career officers. Together, they transformed a once inhibiting, command-centred bureaucracy into a flexible, responsive organisation. Here, working within designated parameters, junior staff are empowered to use their initiative when pursuing the nation's cause in the virtual battlespace. The IDF's adoption of social media acted as a significant force multiplier, extending the opportunity to take up arms and join the fight in the information environment to domestic and dispersed civil society participants. As a consequence, in terms of organisation, tactics, and effects, the IDF's operations in the information environment have more in common with those of Al Qaeda or ISIS than any other conventional military. They provide a model of best practice that other militaries looking to make their mark in the information environment would do well to heed and adapt to their own needs.

Conclusion: Learning from our enemies

On the basis of this analysis it is clear that there have been two dominant approaches to the adoption, adaptation and integration of social media among conventional militaries. The first is an organic method, marked by bottom-up initiative from junior ranks, enabled by supportive superiors and bureaucratic flexibility, born of crisis, attuned to and eager to exploit the affordances of digital media. The second is a command method, which is top down, planned, risk-averse, and unaware of or culturally resistant to the revolutionary potential of social media. The latter, and the drawbacks that this approach engenders, is exemplified in the work of the Multinational Capability Development Campaign (MCDC), to which the US, British and Australian militaries contributed. Established in 2002, the MCDC is a US-led initiative which operates under the auspices of NATO's Allied Command Transformation (ACT).[364] One of ACT's four core functions is 'Development of capabilities', for which the MCDC serves as a laboratory.[365] To this end, the MCDC sponsors two-year multinational campaigns focused on issues most relevant to NATO's current and projected operations. Its campaigns over the last decade have included 'Autonomy, Hybrid Warfare, Cyber, Medical, Logistics … Strategic Communication' and 'Social Media in Support of Situational Awareness'.[366]

During 2015–2016, the MCDC sponsored the Multinational Information Operations Experiment (MNIOE), tasking it to examine the hazards, projected advantages and means of integrating and deploying social media into military operations. The outcome of its investigation, the *Analytical Concept for the Use of Social Media as an Effector*, was published in December 2016. 'The overarching challenge for security and defence actors', the authors observed:

> *is to adapt to the changes in the digital IE and use the new technologies to meet their own objectives. Making social media an effective tool in one's own toolbox as well as integrating it into operations planning and execution will be one of [sic] military's future challenging tasks.*[367]

In this process the key challenges that militaries and other 'security actors' faced were focused on integration, adaptation and deployment. Can social media be integrated into the given military's existing information operations architecture? Can it be adapted to established cultural and organisational systems? If so, how can it be weaponised and deployed?

The focus of these questions on the adaptation of new platforms to an existing architecture implies the extent to which members of the MNIOE were ill-chosen to investigate the military affordances of digital platforms. As NATO Forces Interviewee 1, a member of the MNIOE, conceded, neither he nor his colleagues knew very much about social media when the MNIOE began, and what little social media policy existed in their organisations was almost entirely focused on how to 'use it carefully'. As a whole, he acknowledged, the 'Military doesn't have anything … Everybody wants to do social media, and the military wants to do it as well…. [but] there is nothing on social media and military doctrine'.[368] The publication of the *Analytical Concept* can be read as an affirmation of this.

Perhaps we can understand why the MNIOE's contributor militaries were so lacking in their ability to respond to digital media or integrate it into their current operational frameworks through an examination of how the conforming cultures of conventional militaries affect responsiveness and creativity. As recent studies suggest, mid-ranking military personnel (Majors, Lieutenant Colonels and Colonels—indeed, those who largely comprised the membership of the MNIOE), by virtue of their rank, their length of service and the instinct for professional conformity this has instilled, are more likely

to be unresponsive, if not resistant, to radical innovations and the creative thinking these require.[369] This is despite the key role that creative thinking plays in the ability of organisations to manage change.[370] In conventional militaries, conformity is prioritised. In this context, heterodoxy in all its forms is regarded with suspicion:

> *A person is not selected to join the military organization unless he can fit into the system, and when he is enlisted or commissioned he is adjusted on a Procrustean bed to ensure his conformity.*[371]

This is especially the case in peacetime, which 'encourages the breeding of officers who rigidly follow rules', and is intensified in militaries with a slow operational pace.[372] Conventional militaries thus endorse conformity as an end in itself, identifying it as both the means to and an emblem of the proper functioning of the hierarchy. For the modern military professional, conformity is demanded for success. Personnel 'do not dare take the initiative as complying with rules and being an obedient subordinate opens up a safe road to the top'.[373] Put simply, 'one progresses up the ranks' by doing as one's predecessors did.[374] As a result, Nazareth contends: 'These conditions have moulded the military forces into the most authoritarian organization that exists with the hierarchical "pecking-order" clearly delineated at every level.' Military systems, and the 'military authoritarian structure' that supports them, valorise and reward conformity, resist heterodoxy, and so operate as 'a deterrent to creative thinking'.[375] Nazareth's postulations are borne out in Leon Young's study of the fate of highly creative officers in the Australian Defence Force (ADF), who are either 'normalised' or exit the service, leaving a core of 'conservative colonel[s]' to occupy crucial positions of authority.[376]

That it was just such a cohort of 'conservative colonels' who were responsible for the MNIOE helps account for some but not all of the *Analytical Concept*'s shortcomings. The second and possibly larger issue that the MNIOE identified was the fundamental mismatch between the centralising, hierarchical command and control structures through which modern militaries organise and communicate, and the decentralised networks that underpin digital culture and operations in the information environment. While conventional militaries routinely acknowledge and in many cases applaud the innovations brought about by the revolution in communications technology, they have struggled to adapt to it or have

resisted the integration of this technology into their own systems. Wedded to a broadcast-era Web 1.0 model of production and distribution, conventional militaries continue to fixate on 'mass producing content for mass distribution and mass consumption … on controlling the production and distribution of information for dutiful, passive audiences'.[377] Yet, as a result of the digital architectures of (audience) participation made possible by technological evolution, passive audiences are in decline, have evaporated altogether, or survive only under authoritarian regimes—including militaries—in which digital systems are tightly policed. The dominance of a single, simple broadcast model thus no longer exists and 'the arrangements, assumptions, models, structures, and economic and political power relationships of the broadcast era have been overthrown'.[378] Many militaries, the ADF among them, have failed to adapt to this cultural revolution and are in danger of excluding themselves from the information environment, or arriving there with inadequate weapons.

Similarly, while the communications revolution has powered a radical transformation in conflict paradigms, marked in the shift from War 1.0 to War 2.0, conventional militaries have yet to adapt to decentralised information flows. The primary focus of War 1.0 was weapons and intelligence—among other characteristics—executed through hierarchical top-down initiatives where the media and public were tangential to the execution itself. In War 1.0 information was protected, secret and intended for internal military consumption only.[379] In contrast, War 2.0 is executed through decentralised structures, driven by bottom-up initiatives in which the media and population play a central role, what Hoskins and O'Loughlin describe as 'diffused war'.[380] Here information may be 'predominantly public, open-source, and intended for external consumption'.[381] Yet, while most conventional militaries officially endorse and are committed to the principles of War 2.0, they have continued to invest in War 1.0-style hierarchical command and control structures, where power flows from the apex to the base, and conformity and obedience are the cultural norm. This system is fundamentally incompatible with the 'distributed network of semiautonomous interlinked nodes' that characterises the operations of contemporary digital and social media, with its horizontal vectors and decentralised distribution of power.[382]

The inability of conventional militaries to embrace fully the communications developments of War 2.0, lies in stark contrast to sophisticated non-state actors like Al Qaeda and ISIS whose social connectivity, made possible

by their decentralised networks, has flourished in their execution of war. The transformation of Al Qaeda's organisational planning is noteworthy as a shining example of adaptation and responsiveness through digital technologies. In the wake of the 9/11 attacks, when US military and intelligence services turned their fire on Osama bin-Laden and his leadership team, Rid and Hecker note, Al Qaeda's 'Command-and-control became impractical'.[383] Large training camps were abandoned and 'it became exceedingly dangerous to communicate, be it face-to-face, by messenger, by mail, by telephone, or by electronic means'.[384] As such, Al Qaeda was forced to adopt new organisational systems to recruit, motivate, train and communicate with its personnel. Among those tasked with solving this problem was Abu Musab al-Suri, one of Al Qaeda's principal strategists, who searched for a method to gather, organise and direct supporters and soldiers for a cause 'which is susceptible to self-renewal and to self-perpetuation as a phenomenon after all its conditions and causes are present and visible to the enemy itself'. That is to say, he was looking for a resilient 'operative system', not an 'organization for operations'.[385] This culminated in the emergence of the non-hierarchical, decentralised 'jihad of individualized terrorism', in which small cells, acting autonomously, initiated 'single acts of terrorism' in the service of 'a common aim, a common doctrinal program'.[386] The success of this method was largely dependent on, and deeply integrated with, the technical affordances of digital media where self-motivated nodal non-state actors weaponised digital and social media networks to enable a sophisticated coordination of both the real and virtual spaces of war.[387]

The failure of most of the conventional militaries under analysis here to integrate and merge these differing spaces of war has, by comparison, rendered them largely ineffectual in the cognitive battlespace relative to non-state actors. Instead, as much as they are critical to operational success, digital and social media are predominantly understood as risk generating. These perceived risks include the conviction that user-generated content is untrustworthy; that social media platforms are hostile environments for reputation management; that social media generates risks to personnel security and operational security; that being active on social media is time and personnel intensive; and that the speed of social media poses a challenge to accuracy and presence.[388] These convictions are clearly reflected in the *Analytical Concept*'s treatment of the 'Risks, Threats and Limitations' of social media, particularly the discussion

of the challenges posed by speed. Here the authors express their concern as to whether conventional militaries will or can initiate or respond to social media posts with the timeliness and frequency of other users. The members of the MNIOE rightly point out that the test of social media timeliness 'poses a challenge to the hierarchical nature of the military'.[389] The *Analytical Concept* proposes two possible responses to this problem: either 'the chain of command has to approve each and every message that goes out in the name of the coalition'—the so-called 'one-star tweet'—or militaries reverse the trend whereby only senior personnel act as spokesperson and instead 'lower levels … speak for the coalition online'. The latter response 'requires a strong reliance on Mission Command—the decentralized execution of the Commander's intent' in the information space, which militaries clinging to the command and control model have so far resisted.[390] While conventional militaries continue to revert to the practices and assumptions embedded in their organisational and cultural norms, there is little hope of them 'truly distributing power (to judge and originate ideas)' because such practice cannot coexist with conventional military chains of command.[391] As long as they hold on to a rigid interpretation of hierarchy that resists the organisational logic of contemporary digital and social media technologies, as long as they refuse to reform existing organisations and systems so that new technical affordances might be accommodated, conventional militaries restrict their ability to operate successfully in the information environment.

The most notable exception to the tendencies identified so far among conventional militaries has been the Israel Defense Forces. The IDF have now successfully integrated social media into their systems and operations, actively embraced mission command in their operations and adapted their systems and structures to the organisational logic of the digital age. Here, the devolved enactment of the commander's intent has extended beyond the military and, as a result, Israel has enjoyed unusual success in mobilising its civil base, both domestic and dispersed, to support its campaigns and promote its core messages via social media. The combination of successful mission command and the more condensed and fluid operation of the hierarchy, with its thinner and narrower levels of bureaucratic approval (outlined in Chapter 6) means that IDF responses to specific events are relevant and timely with close coordination between the bottom-up spontaneity of the social media operators and the top-down direction of command. That the IDF's operations in the information

environment are far closer to those of Al Qaeda or ISIS than to those of any other conventional military offers a clear guide to the ADF. Only by taking lessons from its enemies as well as its friends will it be able to organise itself effectively to compete in the information environment.

If the IDF offers a case study in the organic uptake of social media, the MCDC approach, by contrast, sits at the opposite extreme, reflecting a top-down, command-centred, risk-sensitive, theoretically driven approach, run by personnel with limited experience of, understanding of or intuitive feel for the new media. The IDF experience suggests that if conventional militaries want to realise social media's potential as both a platform and a weapon, they will need to radically reshape their organisational systems. Traditional command structures can put boots on the ground, but they cannot regulate the information that 'now pours onto, from, about and around the battlefield'.[392] The IDF's success over the last decade has rested on its sophisticated integration of communication with warfighting operations, but perhaps more so on its mobilisation of civil society communities in 'a new mode of participative warfare'.[393] This brought together and combined the efforts of professional service personnel, conscripts, reservists, the domestic public and a dispersed international support base in an always-at-war space weaponised by religion, ethnicity, culture and narrative. In this space, shared narratives, sharpened and directed by top-down command messaging, were weaponised from the bottom up by social media warriors posting at will within broadly designated arcs of fire. The digital operators who generate these posts can be managed—in so far as they can be managed at all—only through an attenuated form of mission command. Command simply has to accept that there is limited capacity to exercise control over them or mitigate the risks they pose to reputation. The greater risk, however, is that fear will paralyse militaries from fully engaging with and succeeding in the information environment. Conventional militaries will need to thin their bureaucratic levels of approval and flatten the chain of command to ensure that their top-down messaging augments the social media operator's autonomy, speed and spontaneity. The hierarchy will have to empower, and trust, its digital warriors, whose links to the wider online community make them significant force multipliers.

However, there is no question that the IDF experience is largely unique. For Israelis, every conflict is a fight for survival and the regular flow of personnel into and out of uniform creates uniquely porous civil–military relations. By contrast, for almost 75 years, Western militaries have been engaged in wars of choice, while the abolition of conscription and the move to smaller, professionalised forces, has deepened the divisions between civil and military orders.[394] The 'war on terror' revealed that non-state actors had weaponised the information environment, exploiting the affordances of digital networks to maximise their advantage. This revealed that Western militaries not only lacked the organisational systems and cultural posture needed to compete in this space but also were allocating their resources and concentrating their efforts in the wrong places. The dominant paradigm for operations, developed and exemplified in US military doctrine, comprises a six-phase planning construct, running from Phase 0 ('shape') through to Phase V ('enable civil authority'):

> *Within this paradigm, the central decisive point is assumed to be phase III [major combat operations], and the bulk of the U.S. military's attention for resourcing, modernizing, training, and allocating risk is found there.*[395]

Yet, while the US and its allies tool up for battle, their 'adversaries are working to accomplish their objectives short of open conflict' in the grey zone. To match their competitors, conventional militaries need to shift more of their resources to Phase 0, where the information environment is the centre of operations and the focus is on the struggle for the cognitive terrain, not combat in the physical world. Through active engagement with domestic, dispersed and competitor audiences by way of a coordinated but decentred information campaign utilising all relevant media platforms, conventional militaries must learn how to shape this space of war to their benefit, position their competitors to their advantage, determine the conditions for victory and go on to achieve them.

The need for Western militaries to shape the space of war in their interests brings the question of narrative sharply into focus. As Lawrence Freedman notes, 'For a narrative to have the desired effect it must relate in some way to the experiences, culture and concerns of its intended audience'.[396] Al Qaeda, ISIS and the IDF share potent core narratives about what they fight for and why. Their narratives define the principal actors and events in conflict; they speak to the experiences, cultures and concerns of their members and supporters, and create meanings that reaffirm their identities. As the conflicts in Iraq and Afghanistan illustrate, the wars of choice that Western militaries have pursued over the past half century have largely failed to generate or sustain such potent, identity affirming narratives.[397]

Social media has given Western militaries the tools to dominate the information space. To realise that dominance, they need to adapt their organisational systems and cultures so that their personnel are empowered by the digital environment's 'distributed network of semiautonomous interlinked nodes' They need to shift resources from warfighting into shaping the information battlefield where they can channel public participation, mute—if not entirely silence—their competitors, dictate what victory looks like, and ensure that they have a compelling narrative that reinforces who they are, what they are fighting for, and why. Until they are prepared to embrace these organisational and cultural reforms, they may win the warfighting battles, but they will continue to cede the information domain to their military and non-state competitors and so lose the war.

Acknowledgements

I would like to thank the staff of the Australian Army Research Centre for commissioning this report and for their forbearance in awaiting its delivery. I would like to extend my particular thanks to Dr Albert Palazzo, Stephen Sherwood, Dr Lyndal Thompson and Paul Grey. I wish to thank my interviewees: Major General Marcus Thompson; General Angus Campbell; and those from the Department of Defence in Australia, 77th Brigade in Britain, the Pentagon and the Joint Information Operations Warfare Center in the US, the Spokesperson's Unit in the Israel Defense Forces, the Multinational Information Operations Exchange, the Ministerie van Defensie in the Netherlands, and the Department of National Defense and Canadian Forces in Canada. I also owe a debt of thanks to the intermediaries who facilitated my interviews in Israel and the UK. Susan Hutton expertly transcribed the interviews. Tom Sear carried out some preliminary research, for which I thank him. Terri Davis, Assistant Director Research Ethics for the Department of Defence and Veterans' Affairs Human Research Ethics Committee (DDVAHREC), was a source of sound advice as I navigated the ethics clearance process. I would particularly like to thank her for her sensitivity when my mother died in late 2016 as the approval process was under way. This research was conducted under Protocol 838-16 approved by the DDVAHREC. At Monash University, I wish to thank the former Dean of Arts, Professor Rae Frances, for appointing me as Head of the School of Languages, Literatures, Cultures and Linguistics in January 2017, and the current Dean, Professor Sharon Pickering, for her continuing support.

Endnotes

1 British Army, *Army Information Sub-Strategy (2015–2018)* (2015), formerly at http://www.army.mod.uk/documents/general/20151201_Army_Info_Sub_Strategy-EXTERNAL_V1.pdf, 3, para. 10. This link is no longer active.

2 Author interview, Lieutenant General Angus Campbell, Chief of Army, Canberra, 15 September 2017.

3 Kevin Foster, *Social Media as a Force Multiplier: A Review of the Literature*, February 2017.

4 Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age* (Westport, CT: Praeger, 2009), 1–33. For a definition of Web 2.0 see p. 74.

5 Yascha Mounk, 'Enemy of the Status Quo', *Slate*, 17 February 2017, at http://www.slate.com/articles/news_and_politics/the_good_fight/2017/02/social_media_isn_t_bad_or_good_it_favors_outsiders_regardless_of_their_aims.html (accessed 20 February 2017).

6 See, for example, José van Dijk and Thomas Poell, 'Understanding Social Media Logic', *Media and Communication* 1(1) (August 2013), 2–14.

7 Thomas Elkjer Nissen, *The Weaponisation of Social Media: Characteristics of Contemporary Conflicts* (Copenhagen: Royal Danish Defence College, 2015), 8.

8 Elkjer Nissen, *The Weaponisation of Social Media*, 9. See also Mary Kaldor, *New and Old Wars: Organised Violence in a Global Era*, Third Edition (Cambridge: Polity Press, 2013); Herfried Münkler, *The New Wars* (Cambridge: Polity Press, 2005); Martin Van Creveld, *The Transformation of War* (New York: The Free Press, 1991).

9 Christine Bell, Multi-National Capability Development Campaign (MCDC), *Use of Social Media as an Effector: Analytical Concept for the Use of Social Media as an Effector*, Version 1.0 (Mayen, Germany: MCDC, 2016), 4.

10 The *Department of Defense Dictionary of Military and Associated Terms* defines the information environment as 'The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information' (Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02 (Washington, DC: Department of Defense, 2016), 110.

11 George HW Bush, 'Remarks to the American Legislative Exchange Council, 1 March 1991', *The American Presidency Project* (Santa Barbara: University of California, nd), at http://www.presidency.ucsb.edu/ws/?pid=19351 (accessed 18 August 2018). The American Legislative Exchange Council (ALEC) is 'dedicated to the advancement of free market and limited government principles through a unique "public-private partnership" between state legislators and the corporate sector' (Nancy Scola, 'Exposing ALEC: How Conservative-Backed State Laws Are All Connected', *The Atlantic*, 14 April 2012), at https://www.theatlantic.com/politics/archive/2012/04/exposing-alec-how-conservative-backed-state-laws-are-all-connected/255869/ (accessed 18 August 2018).

12 Robert D Schultzinger, *A Time for Peace: The Legacy of the Vietnam War* (Oxford: Oxford University Press, 2006), 186.

13 Ronald Reagan, 'Address to the Veterans of Foreign Wars Convention, Chicago, 18 August 1980', *The American Presidency Project*, at http://www.presidency.ucsb.edu/ws/?pid=85202 (accessed 19 August 2018).

14 Susan L Carruthers, *The Media at War*, Second Edition (New York: Palgrave, 2011), 136. Bruce Cumings noted that 'getting "Vietnam" behind us' was the central purpose of the administration's and the military's media policy during the First Gulf War (Bruce Cumings, *War and Television* (London: Verso, 1992), 119.

15 George HW Bush, 'The President's News Conference, 30 November 1990', *The American Presidency Project*, at http://www.presidency.ucsb.edu/ws/index.php?pid=19119 (accessed 19 August 2018).

16 George HW Bush, 'Address to the Nation Announcing Allied Military Action in the Persian Gulf, 16 January 1991', *The American Presidency Project*, at http://www.presidency.ucsb.edu/ws/?pid=19222 (accessed 19 August 2018).

17 Thomas Rid, *War and Media Operations: The US Military and the Press from Vietnam to Iraq* (New York: Routledge, 2007), 62–63.

18 For more details on these arrangements see Rid, *War and Media Operations*, 77–82; Carruthers, *The Media at War*, 131–38; Philip M Taylor, *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day*, Third Edition (Manchester: Manchester University Press, 2003), 290–291.

19 Douglas Kellner, 'The "Crisis in the Gulf" and the Mainstream Media', *The Electronic Journal of Communication* 2(1) (1991), at http://www.cios.org/EJCPUBLIC/002/1/00215.HTML (accessed 18 August 2018).

20 John J Fialka, *Hotel Warriors: Covering the Gulf War* (Washington, DC: The Woodrow Wilson Center Press, 1991), 12.

21 Fialka, *Hotel Warriors*, 12.

22 For more on the MRTs see Carruthers, *The Media at War*, 132–135.

23 Bernard Trainor, 'The Military and the Media: A Troubled Embrace', *Parameters* 20(4) (1990), 2.

24 Trainor, 'The Military and the Media', 2.

25 John MacArthur, *Second Front: Censorship and Propaganda in the Gulf War* (Berkeley: University of California Press, 1993), 143.

26 Carruthers, *The Media at War*, 131. As Parrish and Andreacchio noted: 'Schwartzkopf is a typical military officer. Although he'd probably never admit it publicly, he takes a sceptical view of the media. Sure, he'll smile from the platform, but his real feelings surface the instant a reporter gets a little pushy' (Lt. Col. Robert D. Parrish and Col. NA Andreacchio, *Schwartzkopf: An Insider's View of the Commander and his Victory* (New York: Bantam, 1991), 179–180).

27 Fialka, *Hotel Warriors*, 27.

28 Fialka, *Hotel Warriors*, 12.

29 Colonel John Shotwell, 'The Fourth Estate as a Force Multiplier', *Marine Corps Gazette* 75(7) (1991), 72–73.

30 Shotwell, 'The Fourth Estate', 73.

31 Shotwell, 'The Fourth Estate', 73.

32 Fialka, *Hotel Warriors*, 27.

33 Shotwell, 'The Fourth Estate', 75. Notably, the Australian experience of extended exposure to the media produced the opposite result—see Kevin Foster and Jason Pallant, 'Familiarity breeds contempt? What the Australian Defence Force Thinks of Its Coverage in the Australian Media and Why', *Media International Australia* 148 (2013), 22–38.

34 Shotwell, 'The Fourth Estate', 77.

35 Fialka, *Hotel Warriors*, 26–27: '… the corps had nearly ninety-four thousand men and women in the Gulf War—more than in the biggest battles of World War II', http://www.historynet.com/persian-gulf-war-us-marines-minefield-assault.htm (accessed 25 August 2018).

36 Shotwell, 'The Fourth Estate', 79.

37 Shotwell, 'The Fourth Estate', 73. Shotwell's conclusion pre-dates Army's arrival at the same realisation, during the early stages of the deployment to Afghanistan, by more than a decade. Further, even at this point Army's reluctant embrace of the media was driven less by a rediscovered enthusiasm for First Amendment rights than by its recognition that, as the public set little store by Army's truthfulness, it needed 'an independent truth-teller' on hand in the field to counter enemy misinformation. For more on this see Thomas Rid, *War and Media Operations*, 108.

38 '15 Top Journalists Object to Gulf War Curbs', *The New York Times*, 2 May 1991, 17. There were representatives from, among others, the *New York Times*, *Washington Post*, *Wall Street Journal*, *Los Angeles Times*, *Time*, Associated Press, CBS, NBC, ABC and CNN.

39 Jason DeParle, 'Keeping the News in Step: Are the Pentagon's Gulf War Rules Here to Stay?', *The New York Times*, 6 May 1992, 9.

40 '15 Top Journalists', 17.

41 MacArthur, *Second Front*, 8.

42 Fialka, *Hotel Warriors*, xiii.

43 MacArthur, *Second Front*, 213, 216.

44 Colin Powell, *A Soldier's Way* (London: Hutchinson, 1995), 529.

45 Philip Taylor, *War and the Media: Propaganda and Persuasion in the Gulf War*, Revised Edition (Manchester: Manchester University Press, 1998), 208–209.

46 Taylor, *War and the Media*, 262.

47 Cumings, *War and Television*, 122. John Broughton argued that the particular power of the nose-cone footage arose from the viewer's identification with the ordnance: 'The viewer, falling under the thrall of the smart-bomb video, took up a specific, symbolic position, not as abstract, transcendental subject but as concrete, material body' (John Broughton, 'The Bomb's-Eye View: Smart Weapons and Military TV', in Stanley Aronowitz, Barbara Martinsons, Michael Menser and Jennifer Rich (eds), *Technoscience and Cyberculture* (New York: Routledge, 1996), 150).

48 Prominent among the leaflets were the coveted 'safe conduct' passes, designed to look like 25-dinar banknotes 'to attract the soldiers' attention' (Jennifer Gabrys, 'Leaflet Drop: The Paper Landscapes of War', *Invisible Culture: An Electronic Journal for Visual Culture* 7 (2004), 1, at http://www.rochester.edu/in_visible_culture/Issue_7/Issue_7_Gabrys.pdf (accessed 28 August 2018).

49 Taylor, *Munitions of the Mind*, 297.

50 For more on this see Peter W Singer and Emerson T Brooking, *LikeWar: The Weaponisation of Social Media* (Boston: Houghton Mifflin Harcourt, 2018) 4–9. See also Chapter 5.

51 Taylor, *Munitions of the Mind*, 294, 295.

52 Taylor, *Munitions of the Mind*, 295; Cumings, *War and Television*, 109.

53 Phillip Knightley, *The First Casualty: The War Correspondent as Hero and Myth Maker from the Crimea to Iraq*, Third Edition (Baltimore: Johns Hopkins University Press, 2004), 494.

54 Michael R Gordon and Lt Gen Bernard E Trainor, *The Generals' War: The Inside Story of the Conflict in the Gulf* (Boston: Little Brown, 1995), 326.

55 For more on this see William Hammond, 'The Press in Vietnam as an Agent of Defeat: A Critical Examination', *Reviews in American History* 17(2) (1989), 315; Daniel Hallin, *The 'Uncensored War': The Media and Vietnam* (Berkeley: University of California Press, 1989).

56 Cumings, *War and Television*, 104.

57 See Taylor, *Munitions of the Mind*, 294–295; Carruthers, *The Media at War*, 138–140; Knightley, *The First Casualty*, 492–494.

58 Eliot A Cohen, *Gulf War Air Power Survey, Volume III: Logistics and Support* (Washington, DC: Government Printing Office, 1993), II, 135.

59 See Mark Bowden, *Black Hawk Down: A Story of Modern War* (New York: The Atlantic Monthly Press, 1999).

60 Johanna Neuman, *Lights, Camera, War: Is Media Technology Driving International Politics?* (New York: St Martin's Press, 1996), 14.

61 Nik Gowing, *Real Time Television Coverage of Armed Conflicts and Diplomatic Crises: Does It Pressure or Distort Foreign Policy Decisions?* (Cambridge, MA: The Joan Shorenstein Center on the Press, Politics and Public Policy, 1994), 48.

62 Frank J Stech, 'Winning CNN Wars', *Parameters* 24(3) (1994), 38.

63 Stech, 'Winning CNN Wars', 38.

64 David B Stockwell, *Press Coverage in Somalia: A Case for Media Relations to Be a Principle of Operations Other Than War*, Unpublished MA Thesis (Fort Meade, MD: Defense Information School, 1995), 30.

65 Rid, *War and Media Operations*, 93.

66 Lt General Anthony C Zinni and Colonel Frederick M Lorenz, 'Media Relations: A Commander's Perspective', *Marine Corps Gazette*, December 1995, 67.

67 Stockwell, *Press Coverage in Somalia*, 1.

68 Rid, *War and Media Operations*, 95.

69 See Leigh Armistead, *Information Operations Matters: Best Practices* (Washington, DC: Potomac Books, 2010), 47. The US administration's first official definition of information warfare was contained in the Secretary of Defense's *Annual Report to the President and the Congress* from January 1994 in a section on 'C^{4}I Cross-Functional Integration'. The Secretary of Defense, Les Aspin, noted that information warfare 'consists of 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, *Annual Report to the President and the Congress* (Washington, DC: Department of Defense, 1994), 244).

70 Gregory J Rattray, *Strategic Warfare in Cyberspace* (London: MIT Press, 2001), 315.

71 Armistead, *Information Operations Matters*, 48. For a more detailed account of the doctrinal evolution of information operations across the USAF, Army and Navy see William Merrin, *Digital War: An Introduction* (New York: Routledge, 2019), 53–59.

72 John Arquilla and David Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy* 12(2) (1993), 142, 143.

73 Arquilla and Ronfeldt, 'Cyberwar', 141–142.

74 Arquilla and Ronfeldt, 'Cyberwar', 143.

75 Rattray, *Strategic Warfare in Cyberspace*, 323.

76 Department of the Army, *Force XXI Operations*, TRADOC Pamphlet 525-5 (Monroe, VA: HQ United States Army Training and Doctrine Command, 1994), 3-1-3-3.

77 Department of the Army, Field Manual 100-6 *Information Operations* (Washington, DC: Department of the Army, 1996), iv.

78 General Ronald R Fogelman, 'Information Operations: The Fifth Dimension of Warfare', *IWS—The Information Warfare Site* 10(47), at http://www.iwar.org.uk/iwar/resources/5th-dimension/iw.htm (accessed 10 September 2018).

79 Fogelman, 'Information Operations'. Three years after this address, in August 1998, the USAF launched its first information operations doctrine: Air Force Doctrine Document 2-5, *Information Operations* (Washington, DC: Secretary of the Air Force, 1998).

80 Major Gary Pounder, 'Opportunity Lost: Public Affairs, Information Operations, and the Air War against Serbia', *Aerospace Power Journal* 14(2) (2000), 58. Field Manual 100-6 defined information operations as 'Continuous military operations within the MIE [military information environment] that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the GIE [global information environment] and exploiting or denying an adversary's information and decision capabilities' (Department of the Army, Field Manual 100-6, 2–3). A more succinct version of this was provided in the 1997 version of the *Department of Defense Dictionary of Military and Associated Terms*, which described it as 'action taken to affect adversary information and information systems while defending one's own information and information systems' (quoted in Rid, *War and Media Operations*, 120).

81 Pounder, 'Opportunity Lost', 66.

82 Quoted in Pounder, 'Opportunity Lost', 66.

83 Pounder, 'Opportunity Lost', 67.

84 Pounder, 'Opportunity Lost', 62–63.

85 These figures are from Howard Kurtz, 'NBC's News Machine Marches to War', *The Washington Post*, 21 April 1999, at https://www.washingtonpost.com/archive/lifestyle/1999/04/21/nbcs-news-machine-marches-to-war/4375009f-56a3-4d54-916e-824cfcfe9302/?noredirect=on&utm_term=.cb71eae67e35 (accessed 28 October 2018).

86 James Kitfield, 'Command and Control the Messenger', *National Journal* 31(37) (1999), 2547.

87 For an overview of media-military-Defence relations see Robert Harris, *Gotcha! The Media, the Government and the Falklands Crisis* (London: Faber and Faber, 1983); Kevin Foster, *Fighting Fictions: War, Narrative and National Identity* (London: Pluto Press, 1999), 34–35. The reporter who identified the landing site was the *Guardian*'s David Fairhall (see David Fairhall, 'The Next Round Won't Be Plain Sailing', *The Guardian*, 28 April 1982, 13). For official commentary on the use of retired service officers as expert commentators see House of Commons Defence Committee, *The Handling of Press and Public Information During the Falklands Conflict*, Volume I (London: HMSO, 1982), xlix.

88 Pascale Combelles Siegel, 'Operation Allied Force: The Media and the Public', in Larry Wentz (ed.), *Lessons from Kosovo: The KFOR Experience* (Washington, DC: Department of Defence Command and Control Program, 2002), 191.

89 Dr Jamie P Shea, 'The Kosovo Crisis and the Media: Reflections of a NATO Spokesman' in Larry Wentz (ed.), *Lessons from Kosovo*, 167, 168. NATO's briefings offer an exemplary illustration of mediatisation in which the media assume 'an active performative involvement and constitutive role' in the conduct of war (Simon Cottle, *Mediatized Conflict: Developments in Media and Conflict Studies* (Maidenhead: Open University Press, 2006), 9.

90 Quoted in Pounder, 'Opportunity Lost', 67.

91 Shea, 'The Kosovo Crisis', 173.

92 The information had to be 'good, plenty and fast'; only then, in the words of Jamie Shea, could you 'give them [the journalists] the news before they give you the news'. See Rid, *War and Media Operations*, 99–100.

93 Quoted in Pounder, 'Opportunity Lost', 67.

94 Kitfield, 'Command and Control the Messenger', 2547.

95 Alastair Campbell, 'Communications Lessons for NATO, the Military and the Media', *The RUSI Journal* 144(4) (1999), 33.

96 Donald Matheson and Stuart Allan, *Digital War Reporting* (Cambridge: Polity Press, 2009), 32.

97 Quoted in Matheson and Allan, *Digital War*, 32.

98 Quoted in Matheson and Allan, *Digital War*, 32.

99 Campbell, 'Communications Lessons', 66.

100 Shea, 'The Kosovo Crisis', 160.

101 Taylor, *Munitions of the Mind*, 309.

102 For more on this see 'NATO Facing E-mail and Web Attacks', *Info World* 21(14) (5 April 1999), 5.

103 Matheson and Allan, *Digital War*, 36.

104 Ellen Goodman, 'The First Internet War', *Boston Globe*, 8 April 1999, A19; Merrin, *Digital War*, 22.

105 Taylor, *Munitions of the Mind*, 308. Taylor claimed that 'The internet was to Kosovo what television had been to the Korean war' (Taylor, *Munitions of the Mind*, 308).

106 Richard Norton-Taylor, 'Serb TV Station Was Legitimate Target, Says Blair', *The Guardian*, 24 April 1999, at https://www.theguardian.com/world/1999/apr/24/balkans3 (accessed 20 April 2020). See also Steven Erlanger, 'Survivors of NATO Attack on Serb TV Headquarters: Luck, Pluck and Resolve', *The New York Times*, 24 April 1999, at https://archive.nytimes.com/www.nytimes.com/library/world/europe/042499kosovo-belgrade.html (accessed 20 April 2020).

107 In Taylor's definition, asymmetric warfare 'essentially means that militarily strong nations like the United States, which can unleash overwhelming firepower, are nonetheless vulnerable in certain areas that weaker opponents can exploit. Information in the global media "space" is one such area, unless the voice of the enemy can be silenced' (Taylor, *Munitions of the Mind*, 309).

108 Serbia saw the first deployment of the carbon graphite bomb, 'which sprays electrical power stations with a dust that causes instant short circuits'. When it was dropped on five power plants on 3 May 1999: 'Power was cut almost instantly across almost 70% of the country, blanking out military computers and radars and communications systems' (Martin Walker, '"Soft Bomb" Knocks out Power Plants', *The Guardian*, 4 May 1999, at https://www.theguardian.com/world/1999/may/04/martinwalker1 (accessed 20 April 2020).

109 Shea, 'The Kosovo Crisis', 164.

110 Shea, 'The Kosovo Crisis', 164.

111 Quoted in Pounder, 'Opportunity Lost', 58.

112 Pounder, 'Opportunity Lost', 57.

113 Michael R Gordon, 'Civilians Are Slain in Military Attack on a Kosovo Road', *The New York Times*, 15 April 1999, 1; Blaine Harden, 'The Teetering Balkans', *The New York Times*, 15 April 1999, 1. The incident was also front-page news in the *Los Angeles Times* (Joel Havemann, 'Convoy Deaths May Undermine Moral Authority', *Los Angeles Times*, 15 April 1999, 1).

114 Shea, 'The Kosovo Crisis', 162–63. Alistair Campbell concurred with this assessment: 'If a bomb went astray, the Serb media machine could round up a few chosen journalists at the Hyatt in Belgrade, take them down to the scene, and get the story running. Pictures. Therefore news … And we had only words to hit back with … Just words though. No pictures. No news' (Campbell, 'Communications Lessons for NATO', 34).

115 Pounder, 'Opportunity Lost', 57.

116 Dana Priest, 'NATO Concedes Its Bombs Likely Killed Refugees', *The Washington Post*, 20 April 1999, 19.

117 Michael Elliott, 'Casualties of War', *Newsweek*, 26 April 1999, 27.

118 Priest, 'NATO Concedes', 19.

119 Wesley K Clark *Waging Modern War: Bosnia, Kosovo and the Future of Combat* (New York: Public Affairs, 2001), 444.

120 Rid, *War and Media Operations*, 99.

121 Shea, 'The Kosovo Crisis', 167.

122 Quoted in Pounder, 'Opportunity Lost', 66.

123 Pounder, 'Opportunity Lost', 60.

124 Sergeant Marilee Phelen, a former USAF Europe PAO, claimed that IO planners 'were more interested in "media manipulation" than dissemination of factual information' (quoted in Pounder, 'Opportunity Lost', 64).

125 Quoted in Pounder, 'Opportunity Lost', 64–65.

126 Rid, *War and Media Operations*, 115.

127 Quoted in Pounder, 'Opportunity Lost', 60.

128 Rid, *Media Operations*, 128.

129 Rid, *Media Operations*, 107, 108.

130 Howard Kurtz, 'All on Board for the Attack', *The Washington Post*, 9 October 2001, at https://www.washingtonpost.com/archive/lifestyle/2001/10/09/all-on-board-for-the-attack/7e8b5fbd-035a-4c5a-97c3-00a919e379e5/ (accessed 22 April 2020).

131 Rid, *Media Operations*, 105.

132 Rid, *Media Operations*, 106.

133 Tammy L Miracle, 'The Army and Embedded Media', *Military Review* 83(5) (2003), 42. Reeder helped write the public affairs chapter on the coalition forces' land component command public affairs mission in Afghanistan for the Center for Army Lessons Learned.

134 Rid, *Media Operations*, 106; Miracle, 'The Army and Embedded Media', 42.

135 The 'Coalition of the Willing' ultimately comprised forces from 48 countries, only three of which, besides the US, contributed troops to the invasion of Iraq, namely the UK, Australia and Poland. Principal responsibility for the development and implementation of the public affairs guidance lay with the Assistant Secretary of Defense for Public Affairs, Victoria (Torie) Clarke.

136 Office of the Assistant Secretary of Defense for Public Affairs, *Public Affairs Guidance on Embedding Media during Possible Future Operations/Deployments in the U.S. Central Commands [sic] (CENTCOM) Area of Responsibility (AOR)* (Washington, DC: Department of Defense, [2003]), para. 2.A.

137 Secretary of Defense, *Public Affairs Guidance on Embedding Media*, para. 3.G.

138 Secretary of Defense, *Public Affairs Guidance on Embedding Media*, para. 2.C.2.

139 Secretary of Defense, *Public Affairs Guidance on Embedding Media*, para. 2.C.3.

140 Secretary of Defense, *Public Affairs Guidance on Embedding Media*, para. 6.A.; 6.A.2.

141 Secretary of Defense, *Public Affairs Guidance on Embedding Media*, para. 2.A.

142 John Kampfner, *Correspondent: War Spin*, BBC 2, 18 May 2003. Transcript at http://news.bbc.co.uk/nol/shared/spl/hi/programmes/correspondent/transcripts/18.5.031.txt (accessed 22 April 2020).

143 Julia Day, 'US Steps up Global PR Drive', *The Guardian*, 30 July 2003, at https://www.theguardian.com/media/2002/jul/30/marketingandpr.terrorismandthemedia (accessed 22 April 2020).

144 Douglas Quenqua, 'White House Prepares to Feed 24-Hour News Cycle', *PR Week*, 24 March 2003, 1.

145 David Miller, 'The Propaganda Machine', in David Miller (ed.), *Tell Me Lies: Propaganda and Media Distortion in the Attack on Iraq* (London: Pluto Press, 2004), 81.

146 Quenqua, 'White House Prepares', 1.

147 Miller, 'The Propaganda Machine', 82.

148 United States Air Force, Air Force Doctrine Document 1, *Air Force Basic Doctrine* (Washington, DC: US Air Force, 2003), 31.

149 Quoted in Rid, *War and Media Operations*, 120; US Air Force, *Air Force Basic Doctrine*, 31.

150 US Air Force, *Air Force Basic Doctrine*, 31.

151 For a breakdown of how the reporters were distributed among the different service arms see Andrew P Cortell, Robert M Eisinger and Scott L Althaus, 'Why Embed? Explaining the Bush Administration's Decision to Embed Reporters in the 2003 Invasion of Iraq', *American Behavioral Scientist* 52(5) (2009), 670.

152 Cortell, Eisinger and Althaus, 'Why Embed?', 670, 672.

153 Susan Brockus, 'Coming to You "Live": Exclusive Witnessing and the Battlefield Reporter', *Journal of Communication Inquiry* 33(1) (2009), 34.

154 Carruthers, *The Media at War*, 229.

155 Thomas Ricks, *Fiasco: The American Military Adventure in Iraq* (London: Penguin, 2006), 85.

156 For more on the role of CENTCOM in sustaining the strategic message and managing reporters see Kampfner, *Correspondent: War Spin*.

157 Faisal Bodi, 'Al Jazeera's War', in David Miller (ed.), *Tell Me Lies*, 245.

158 Sheldon Rampton and John Stauber, *Weapons of Mass Deception: The Uses of Propaganda in Bush's War on Iraq* (New York: Penguin, 2003), 199.

159 Bodi, 'Al Jazeera's War', 249.

160 Rampton and Stauber, *Weapons of Mass Deception*, 199. Simson Garfinkel alleged that the NSA and the CIA were involved in the DDoS attack. See Simson Garfinkel, 'Al Jazeera Hacker Sentenced', *MIT Technology Review*, 14 November 2003, at https://www.technologyreview.com/s/402294/al-jazeera-hacker-sentenced/ (accessed 18 October 2018).

161 See Bill Katovsky and Timothy Carlson, *Embedded: The Media at War in Iraq* (Guilford, CT: Lyons Press, 2003), 182.

162 Robert Fisk, 'Al Jazeera accuses US of harassment in row over "bias"', *The Independent*, 30 July 2003, at https://www.independent.co.uk/voices/commentators/fisk/al-jazeera-accuses-us-of-harassment-in-row-over-bias-98200.html (accessed 18 October 2018).

163 Jane Perlez, 'At Least 3 Journalists Die in Blast at Baghdad Hotel', *The New York Times*, 8 April 2003, at https://www.nytimes.com/2003/04/08/international/worldspecial/at-least-3-journalists-die-in-blast-at-baghdad.html (accessed 14 October 2018).

164 Claire Cozens, 'Al-Jazeera claims military "cover up"', *The Guardian*, 9 April 2003, at https://www.theguardian.com/media/2003/apr/08/iraq.iraqandthemedia2 (accessed 14 October 2018).

165 Ricks, *Fiasco*, xvi. For more on Iraq's descent into chaos see Megan Stack, 'Forgive Us Our Trespasses', 'All Things Light, and All Things Dark' and 'There Would Be Consequences', in Megan Stack, *Every Man in this Village Is a Liar: An Education in War* (Melbourne: Scribe, 2011), 52–62, 191–202, 203–216.

166 Donald Macintyre, 'Iraqi PM Bans Al-Jazeera for "inciting hatred"', *The Independent*, 8 August 2004, at https://www.independent.co.uk/news/world/middle-east/iraqi-pm-bans-al-jazeera-for-inciting-hatred-50712.html (accessed 2 November 2018).

167 Carruthers, *The Media at War*, 234.

168 Tim Gopsill, 'Target the Media', in David Miller (ed.), *Tell Me Lies*, 251.

169 Ministry of Defence, *Green Book*, Version 5.0 (London: Ministry of Defence, 2008), 7.

170 John Donvan, 'For the Unilaterals, No Neutral Ground', *Columbia Journalism Review* 42(1) (2003), 35.

171 Shahira Fahmy and Thomas J Johnson, 'Embedded versus Unilateral Perspectives on Iraq War', *Newspaper Research Journal* 28(3) (2007), 102–103.

172 Donvan, 'For the Unilaterals', 35.

173 Justin Lewis, Rod Brookes, Nick Modsell and Terry Threadgold, *Shoot First and Ask Questions Later: Media Coverage of the 2003 Iraq War* (New York: Peter Lang, 2006), 109.

174 The Marines were convinced that the militia who had hijacked Osman and Nerac's vehicle were using both to launch suicide attacks against the American troops. For more detail see, 'How I Tracked down Terry Lloyd's Killers', *Evening Standard*, 21 October 2006, at https://www.standard.co.uk/news/how-i-tracked-down-terry-lloyds-killers-7187633.html (accessed 19 October 2018).

175 Gopsill, 'Target the Media', 256.

176 Donvan, 'For the Unilaterals', 35.

177 Gopsill, 'Target the Media', 252.

178 Brockus, 'Coming to You "Live"', 34.

179 John Durham Peters, 'Witnessing', *Media, Culture and Society* 23(6) (2001), 719.

180 Project for Excellence in Journalism, *Embedded Reporters: What Are Americans Getting?* (Washington, DC: Project for Excellence in Journalism, 2003), 2.

181 Carruthers, *The Media at War*, 231.

182 William Merrin defines 'full spectrum dominance' as the simultaneous combination of 'informational/electromagnetic and real-world dominance' (Merrin, *Digital War*, 58).

183 Rid and Hecker, *War 2.0*, 29. Web 2.0 was a term coined by Tim O'Reilly in 2004. See Tim O'Reilly, 'What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software', *O'Reilly*, 30 September 2005, at https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (accessed 7 September 2019).

184 Brendan I Koerner, 'Why ISIS Is Winning the Social Media War', *Wired*, April 2016, at https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/ (accessed 13 March 2020). Koerner examines the media's capacity to breed contagion, drawing a series of connections between the hijacking epidemic of the late 1960s / early 1970s and the media operations of ISIS.

185 Rid and Hecker, *War 2.0*, 10.

186 Arquilla and Ronfeldt, 'Cyberwar', 143. For more on Al Qaeda's and ISIS's information advantage see Lisa Blaker, 'The Islamic State's Use of Online Social Media', *Military Cyber Affairs* 1(1) (2015); James P Farwell, 'The Media Strategy of ISIS', *Survival: Global Politics and Strategy* 56(6) (2014), 49–55; Joseph Shaheen, *How Daesh Uses Adaptive Social Networks to Spread Its Message* (Riga: NATO Strategic Communications Centre of Excellence, 2016), at https://www.stratcomcoe.org/network-terror-how-daesh-uses-adaptive-social-networks-spread-its-message; Singer and Brooking, *LikeWar*; Charles Winter, 'The Battle for Mosul: An Analysis of ISIS Propaganda', in Ofer Fridman, Vitaly Kabernik and James C Pearce (eds), *Hybrid Conflicts and Information Warfare: New Labels, Old Politics* (Boulder: Lynne Rienner, 2019).

187 Rid and Hecker, *War 2.0*, 128.

188 Maryanne Kelton, Michael Sullivan, Emily Bienvenue and Zac Rogers, 'Australia, the Utility of Force and the Society-Centric Battlespace', *International Affairs* 95(4) (2019), 860.

189 Sanda Svetoka, *Social Media as a Tool of Hybrid Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2016), 4, at https://www.stratcomcoe.org/social-media-tool-hybrid-warfare (accessed 9 August 2019).

190 MCDC, *Use of Social Media as an Effector*, 4. The MCDC has since been superseded by the Capability Development Directorate. See http://www.act.nato.int/who-we-are

191 See for example http://www.defence.gov.au/Social Media/; https://www2.werkenbijdefensie.nl/nieuws/social-media; and https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2008/2008-official-use-social-media.html. For more on risk aversion and fear see Sarah Maltby, 'Imagining Influence: Logic(al) Tensions in War and Defence', in Mikkel Fugl Eskjær, Stig Hjarvard and Mette Mortensen (eds), *The Dynamics of Mediatized Conflicts* (London: Peter Lang, 2015), 165–184; Sarah Maltby, Helen Thornham and Daniel Bennett, 'Capability in the Digital: Institutional Media Management and Its Dis/Contents', *Information, Communication and Society* 18(5) (2015), 1–22.

192 US Air Force, *Air Force Basic Doctrine*, 31.

193 Rid and Hecker, *War 2.0*, 54.

194 Sean Lawson, 'The US Military's Social Media Civil War: Technology as Antagonism in Discourses of Information-Age Conflict', *Cambridge Review of International Affairs* 27(2) (2014), 227.

195 Mike Spector, 'Cry Bias, and Let Slip the Blogs of War', *The Wall Street Journal*, 26 July 2006, B1 at https://web.archive.org/web/20061005035939/http://online.wsj.com/public/article/SB115388005621517421-FmiVf9l3loQ4cYnDSnAAHhLyIDo_20070725.html (accessed 22 January 2017). For more on the culture of milblogging and one of its most prominent figures, Bill Roggio, see Paul McLeary, 'Blogging the Long War', *Columbia Journalism Review*, March/April 2008, 36–40.

196 For more on Milblogging.com see Melissa Wall, 'The Taming of the Warblogs: Citizen Journalism and the War in Iraq', in Stuart Allan and Einar Thorsen (eds) *Citizen Journalism: Global Perspectives* (New York: Peter Lang, 2008), 37.

197 For these figures see Lawson, 'The US Military's Social Media Civil War', 232. Melissa Wall points out that there was also a large number of blogs about life in occupied Iraq written by Iraqis: 'so many Iraqi-written blogs now exist that they are indexed by the aggregator Iraq Blog Count' (Wall, 'The Taming of the Warblogs', 34).

198 United States Army, *Operations Security*, Army Regulation 530-1 (Washington, DC: Pentagon, 2005), 5, at https://fas.org/irp/doddir/army/ar530-1-2005.pdf (accessed 22 January 2017).

199 'The END of Military Blogging', *BlackFive*, 2 May 2007, at http://www.blackfive.net/main/2007/05/new_opsec_regul.html

200 Noah Shachtman, 'Army Squeezes Soldier Blogs, Maybe to Death', *Wired*, 2 May 2007, at https://www.wired.com/2007/05/army-bloggers/. Fans of *BlackFive* and the work of the milbloggers included General David Petraeus. See Noah Shachtman, 'Petraeus Hearts Milblogs', *Wired*, 14 May 2007, at https://www.wired.com/2007/05/petraeus_hearts

201 Shachtman, 'Army Squeezes Soldier Blogs'.

202 United States Army, 'Army Operations Security: Soldier Blogging Unchanged', 2 May 2007, at https://fas.org/irp/agency/army/blog050207.pdf (accessed 23 January 2017). See also Noah Shachtman, 'Army to Bloggers: We Won't Bust You. Promise', *Wired*, 3 May 2007, at https://www.wired.com/2007/05/army_to_blogger (accessed 23 January 2017).

203 US Army, 'Army Operations Security: Soldier Blogging Unchanged'. It goes on to note: 'Much of the information contained in the 2007 version of AR 530-1 already was included in the 2005 version of AR 530-1. For example, Soldiers have been required since 2005 to report to their immediate supervisor and OPSEC officer about their wishes to publish military-related content in public forums.

Army Regulation 530-1 simply lays out measures to help ensure operations security issues are not published in public forums (i.e., blogs) by Army personnel.'

204 Wall, 'The Taming of the Warblogs', 37–39.

205 For more on this see Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013), 6–7; Richard A Clarke and Robert K Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), 12–16.

206 Lawson, 'US Military's Social Media Civil War', 233. See also Robert Gates, 'Memorandum: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations', 23 June 2009, at http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf (accessed 24 January 2017).

207 Noah Shachtman, 'Military May Ban Twitter, Facebook as Security "Headaches"', *Wired*, 20 July 2009, at https://www.wired.com/2009/07/military-may-ban-twitter-facebook-as-security-headaches (accessed 24 January 2017).

208 Shachtman, 'Military May Ban Twitter, Facebook'.

209 Noah Shachtman, 'Army Orders Bases to Stop Blocking Twitter, Facebook, Flickr', *Wired*, 10 June 2009, at https://www.wired.com/2009/06/army-orders-bases-stop-blocking-twitter-facebook-flickr/ (accessed 24 January 2017). The original ban on access to 13 sites, including MySpace and YouTube, was initiated by STRATCOM in 2007 purportedly 'to stop the heavy drain the media-intensive sites put on the military network' (Leo Shane III, 'Military Considers Ban on Twitter, Facebook', *Stars and Stripes*, 31 July 2009, at http://www.stripes.com/news/military-considers-ban-on-twitter-facebook-1.93709 (accessed 24 January 2017).

210 Lawson, 'US Military's Social Media Civil War', 231.

211 Deputy Secretary of Defense, 'Directive Type Memorandum (DTM) 09-026—Responsible and Effective Use of Internet-based Capabilities', 25 February 2010, at http://www.slideshare.net/DepartmentofDefense/dtm-09-026 (accessed 24 January 2017).

212 James Dao, 'Military Announces New Social Media Policy', *The New York Times*, 26 February 2010, at https://atwar.blogs.nytimes.com/2010/02/26/military-announces-new-social-media-policy/?_r=0 (accessed 24 January 2017).

213 Deirdre Collings and Rafal Rohozinski, *Bullets and Blogs: New Media and the Warfighter* (Carlisle Barracks, PA: US Army War College, 2009); Mark Drapeau and Linton Wells II, *Social Software and National Security: An Initial Net Assessment* (Washington, DC: National Defense University, 2009). For a handy survey of the enthusiastic embrace of social media by the US military's junior officers see Rid and Hecker, *War 2.0*, 72–78.

214 Office of the Chief of Public Affairs, *The United States Army Social Media Handbook* (Washington, DC: US Army Office of the Chief of Public Affairs Online and Social Media Division, 2016), at https://www.army.mil/e2/rv5_downloads/socialmedia/army_social_media_handbook.pdf (accessed 25 January 2017). This link is no longer active.

215 *United States Army Social Media Handbook*, 4. It was supplemented by the Social Media Education and Training site, hosted by the Chief Information Officer of the Department of Defense, which provides guides to blogging, Facebook, Twitter, Flickr and YouTube and an array of service-specific advice, at http://dodcio.defense.gov/Social-Media/Social-Media-Education-and-Training/

216 United States Army, 'Army Social Media Policies and Resources', at https://www.army.mil/socialmedia/ (accessed 13 March 2020).

217 The training comes under the auspices of the Chief Information Officer. See 'DoD Social Media Hub' at https://dodcio.defense.gov/Social-Media/ (accessed 13 March 2020).

218 United States Army, *Social Media Protection: A Handbook for Privacy and Security Settings* (2019), at https://www.army.mil/e2/downloads/rv7/socialmedia/social_media_protection.pdf (accessed 13 March 2020).

219 Michael S James and Marisa Taylor, 'Marine Sgt. Gary Stein Gets "Other Than Honorable" Discharge over Anti-Obama Facebook Comment', *ABC News* [online], 25 April 2012, at http://abcnews.go.com/US/marine-sgt-gary-stein-honorable-discharge-anti-obama/story?id=16216279 (accessed 25 January 2017).

220 Cheryl Rodewig, 'Geotagging Poses Security Risks', *U.S. Army*, 7 March 2012, at https://www.army.mil/article/75165/Geotagging_poses_security_risks (accessed 25 January 2017).

221 Lawson, 'US Military's Social Media Civil War', 237–238.

222 Jeremy Hsu, 'The Strava Heat Map and the End of Secrets', *Wired*, 29 January 2018, at https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/ (accessed 24 April 2020).

223 Liz Sly, 'U.S. soldiers are Revealing Sensitive and Dangerous Information by Jogging', *The Washington Post*, 29 January 2018, at https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html (accessed 24 April 2020).

224 Nikhil Sonnad, 'The Chinese Military is Afraid Wearables Will Reveal Its Secrets', *Quartz*, 12 May 2015, at https://qz.com/402353/the-chinese-military-is-afraid-wearables-will-reveal-its-secrets/ (accessed 24 April 2020).

225 'Chinese PLA Bans Soldiers from Social Media', *World of Defense*, 1 June 2011, at http://worldofdefense.blogspot.com.au/2011/06/chinese-pla-bans-soldiers-from-social.html (accessed 25 January 2017).

226 Celine Ge, 'PLA on Call: China's Military Orders Anti-Spy Software for Soldiers' Smartphones', *South China Morning Post*, 20 April 2016, at http://www.scmp.com/news/china/diplomacy-defence/article/1937085/pla-call-chinas-military-orders-anti-spy-software (accessed 25 January 2017).

227 Ge, 'PLA on Call'. In February 2016, PLA soldiers were warned not to use car-hailing apps, like Uber, because the phone's GPS location detection service could reveal secret military facilities. See Gloria Chan, 'Warning Shot: Soldier Alerts PLA to Military Threat from Car-Hailing Apps', *South China Morning Post*, 15 February 2016, at http://www.scmp.com/news/china/diplomacy-defence/article/1913367/warning-shot-soldier-alerts-pla-military-threat-car (accessed 25 January 2017).

228 Department of Defense, *Strategy for Operations in the Information Environment* (Washington, DC: Department of Defense, 2016), 4, at https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (accessed 25 January 2017).

229 Department of Defense, *Strategy for Operations in the Information Environment*, 8–9.

230 Department of Defense, *Strategy for Operations in the Information Environment*, 13.

231 For more on this see Emerson T Brooking and PW Singer, 'War Goes Viral', *The Atlantic*, November 2016, at https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/ (accessed 13 March 2020); Koerner, 'Why ISIS is Winning the Social Media War'.

232 The link to the original NATO website, http://www.act.nato.int/mcdc, has since been disabled.

233 MCDC, *Use of Social Media as an Effector*, 4.

234 Author interview, Robert Presler, Director, Information Operations, Office of the Secretary of Defense, The Pentagon, 14 December 2017.

235 Office of the President of the United States of America, *National Security Strategy of the United States of America* (Washington, DC: United States President, 2017), 34–35.

236 Author interview, US Officer 2 (name withheld), The Pentagon, 14 December 2017.

237 United States Government, *National Defense Authorization Act for Fiscal Year 2018*, Public Law 115-91—12 December 2017 (Washington, DC: United States Government), Stat. 1742, s. 1637, a1A, a1B.

238 National Defense Authorization Act, s. 1637, a3D, a3E, a3F.

239 Author interview, name withheld, US Joint Information Operations Warfare Center, San Antonio, Texas, 15 December 2017.

240 Author interview, name withheld, US Joint Information Operations Warfare Center.

241 Author interview, US Officer 2.

242 Author interview, name withheld, US Joint Information Operations Warfare Center.

243 Author interview, name withheld, US Joint Information Operations Warfare Center.

244 Author interview, name withheld, US Joint Information Operations Warfare Center.

245 Author interview, name withheld, US Joint Information Operations Warfare Center.

246 Author interview, US Officer 2.

247 Tony Hall, *Report by Tony Hall on Review of Media Access to Personnel* (London: Ministry of Defence, 2007), 6, para. 30, at http://webarchive.nationalarchives.gov.uk/20121026065214/http://www.mod.uk/NR/rdonlyres/B6BBBA4B-02ED-45AC-84EF-A4AD4AB7DAA1/0/HallReport.pdf (accessed 27 January 2017).

248 Tony Hall, *Review of Media Access to Personnel*, 7, para. 34.

249 Hall was appointed Director-General of the BBC in 2013.

250 Tony Hall, *Review of Media Access to Personnel*, 20, Annex A.

251 Tony Hall, *Review of Media Access to Personnel*, 2, 3, paras 8, 10.

252 Tony Hall, *Review of Media Access to Personnel*, 3, para. 11.

253 Rid and Hecker, *War 2.0*, 89.

254 Anthony King, 'Understanding the Helmand Campaign: British Military Operations in Afghanistan', *International Affairs* 86(2) (2010), 311.

255 BBC, 'Helmand "Not a Losing Campaign"', *BBC News*, 25 June 2009, at http://news.bbc.co.uk/2/hi/uk_news/8117988.stm (accessed 20 March 2020). This was not the view of other analysts.

256 Robert Egnell, 'Lessons from Helmand, Afghanistan: What Now for British Counterinsurgency?', *International Affairs* 87(2) (2011), 297 (ISAF was the NATO-led International Security Assistance Force.)

257 See Sean Rayment, 'Briish Troops Are Left without Medics', *The Telegraph*, 16 September 2007, at https://www.telegraph.co.uk/news/uknews/1563279/British-troops-are-left-without-medics.html (accessed 20 March 2020); Luke Baker, 'British Government Criticised over Afghanistan Equipment', *Reuters*, 14 July 2009 (accessed 20 March 2020).

258 Mark Townsend, 'Troops Say They Lack the Right Kit to Fight in Helmand', *The Guardian*, 9 August 2009, at https://www.theguardian.com/uk/2009/aug/09/afghanistan-soldiers-deaths-compensation-equipment (accessed 20 March 2020).

259 See Stephanie Kennedy, 'British Government Faces Afghanistan War Fallout', *Correspondents Report*, ABC Radio, 19 July 2009, at https://www.abc.net.au/correspondents/content/2009/s2629675.htm (accessed 24 April 2020); Richard Norton-Taylor and Patrick Wintour, 'MPs' Report to Say Helicopter Shortage Puts Troops at Risk in Afghanistan', *The Guardian*, 16 July 2009, at https://www.theguardian.com/politics/2009/jul/15/helicopters-brown-committee-afghanistan (accessed 24 April 2020).

260 Rid and Hecker, *War 2.0*, 94. For criticism from the top brass see James Sturcke, 'General Sir Richard Dannatt: In His Own Words', *The Guardian*, 8 October 2009, at https://www.theguardian.com/uk/2009/oct/07/general-sir-richard-dannatt-words (accessed 20 March 2020).

261 For more on this see Rid and Hecker, *War 2.0*, 95.

262 Rid and Hecker, *War 2.0*, 95.

263 Tony Hall, *Review of Media Access to Personnel*, 3, para. 14.

264 Nick Gurr, *Defence Communications Strategy* (London: Ministry of Defence, 2009 [2007]), 1, para. 1.

265 Gurr, *Defence Communications Strategy*, 2, para. 6.

266 Gurr, *Defence Communications Strategy*, 4, para. 9d.

267 Ministry of Defence, *Online Engagement Guidelines* (London: Ministry of Defence, 2009), para. 5 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27933/20090805UMODOnlineEngagementGuidelinesVersion10.pdf (accessed 27 January 2017).

268 Ministry of Defence, 'MoD Launches Personal Online Security Awareness Campaign', *Gov.UK*, 1 June 2011, at https://www.gov.uk/government/news/mod-launches-personal-online-security-awareness-campaign (accessed 27 January 2017).

269 Nick Hopkins, 'MoD Releases YouTube Videos Warning of Careless Talk on Social Media Sites', *The Guardian*, 15 June 2011, at https://www.theguardian.com/uk/2011/jun/14/ministry-defence-facebook-youtube-warning (accessed 27 January 2017). The first of the four videos is at https://www.youtube.com/watch?v=AiGD2t-H1Lw.

270 Ministry of Defence, 'MoD Scoops Gold for Social Awareness Campaign', *Gov.UK*, 27 March 2012, at https://www.gov.uk/government/news/mod-scoops-gold-for-social-media-awareness-campaign (accessed 27 January 2017).

271 Ministry of Defence, 'Think Before You Share Online', *Gov.UK*, 21 October 2013, at https://www.gov.uk/guidance/think-before-you-share (accessed 27 January 2017). See also Ministry of Defence, *Personal Online Security* (London: Ministry of Defence, 2013), at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251555/onlineSecurity20131018b.pdf (accessed 27 January 2017).

272 British Army, *Army Information Sub-Strategy*, 1, para. 1.

273 British Army, *Army Information Sub-Strategy*, 2, para. 8.

274 British Army, *Army Information Sub-Strategy*, 3, para. 10.

275 Christian Hill, 'Army's Press Team Locked in an Embrace with the "Dark Arts" Squad', *The Guardian*, 11 September 2014, at https://www.theguardian.com/media/greenslade/2014/sep/11/ministry-of-defence-war-reporting (accessed 27 January 2017). See also Christian Hill, *Combat Camera: From Auntie Beeb to the Afghan Frontline* (London: Alma Books, 2014).

276 Hill, 'Army's Press Team'.

277 Hill, 'Army's Press Team'.

278 See Caroline Wyatt, 'Psy-Ops: Tuning the Afghans into Radio', *BBC News*, 27 October 2012, at http://www.bbc.com/news/world-south-asia-20096416 (accessed 27 January 2017). For internet penetration rates in Afghanistan see Ruth Rennie, Sudhindra Sharma and Pawan Sen, *Afghanistan in 2009: A Survey of the Afghan People* (San Francisco: The Asia Foundation, 2009), 137–145, at http://asiafoundation.org/resources/pdfs/Afghanistanin2009.pdf (accessed 27 January 2017).

279 Tom Coburg points out that Tatham went on 'to head the Defence division of SCL, the now defunct parent of data miner Cambridge Analytica' (Tom Coburg, 'A Secretive Propaganda Unit is Manipulating Our Social Media. But It's Not Russian', *The Canary*, 17 November 2019, at https://www.thecanary.co/exclusive/2019/11/17/a-secretive-propaganda-unit-is-manipulating-our-social-media-but-its-not-russian/ (accessed 23 March 2020).

280 Wyatt, 'Psy-Ops'.

281 Wyatt, 'Psy-Ops'.

282 For more on 77th Brigade see '77th Brigade: Influence and Outreach', *The British Army*, at https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/ (accessed 24 March 2020).

283 Jonathan Beale, 'Army Sets up New Brigade for "Information Age"', *BBC News*, 31 January 2015, at http://www.bbc.com/news/uk-31070114 (accessed 28 January 2017).

284 Harry Lye, 'British Army Announces New Cyberwarfare Division', *Army Technology*, 1 August 2019, at https://www.army-technology.com/news/british-army-cyber-warfare-division/ (accessed 26 March 2020). For more details on the six groups see 'Groups within 77th Brigade', *The British Army*, at https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/groups/ (accessed 24 March 2020).

285 Kim Sengupta, 'New British Army Unit "Brigade 77" to Use Facebook and Twitter in Psychological Warfare', *The Independent*, 31 January 2015, at http://www.independent.co.uk/news/uk/home-news/return-of-the-chindits-mod-reveals-cunning-defence-plan-10014608.html (accessed 28 January 2017); Ewan MacAskill, 'British Army Creates Team of Facebook Warriors', *The Guardian*, 31 January 2015, at https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade (accessed 28 January 2017).

286 Beale, 'Army Sets up New Brigade for "Information Age"'.

287 Carl Miller, 'Inside the British Army's Secret Information Warfare Machine', *Wired*, 14 November 2018, at https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military (accessed 20 March 2020). *Grange Hill* was a hugely popular BBC children's television series set in a 'typical' London secondary school, the eponymous Grange Hill. It comprised 31 series and ran from 1978 to 2008.

288 '77th Brigade: Influence and Outreach'.

289 Miller, 'Inside the British Army's Secret Information Warfare Machine'.

290 'Groups within 77th Brigade'.

291 Author interview, 77th Brigade Personnel 1 (name withheld), Denison Barracks, Hermitage, Berkshire, 7 June 2017.

292 Author interview, 77th Brigade Personnel 1.

293 'Groups within 77th Brigade'.

294 'Groups within 77th Brigade'. The two cells and four teams are Division IA&O Cell; Brigade IA&O Cell; IA&O Teams; Information Warfare Team; Tactical Engagement Team; and IA Training and Advisory Team.

295 The Information Warfare Team (IWT) provides 'the Information Activity component of the IA&O Team, an IWT provides an Information Warfare capability to the Field Army and wider Defence' ('Groups within 77th Brigade').

296 Miller, 'Inside the British Army's Secret Information Warfare Machine'. The targeting of competitors was guided by the targeting process which, Giulio Di Marzio notes, 'is developed through five important steps … Decide, Detect, Track, Deliver and Assess' (Giulio Di Marzio, 'The Targeting Process … This Unknown Process', *NRDC-ITA Magazine* 13 (11 September 2009), 12, at https://www.nato.int/nrdc-it/magazine/2009/0911/0911d.pdf (accessed 21 March 2020). Elsewhere, the joint targeting process is identified by the Joint Chiefs of Staff and others as a six-phase process: end state and commander's objectives; target development and prioritisation; capabilities analysis; commander's decision and force assignment; mission planning and force execution; assessment. For more on this see Deployable Training Division—Joint Staff J7, *Integration and Synchronization of Joint Fires*, Fourth Edition (Suffolk, VA: J7 Deputy Director for Joint Training, 2018), at https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/int_and_sync_jointfires.pdf?ver=2018-09-18-102801-350 (accessed 21 March 2020).

297 Author interview, 77th Brigade Personnel 2 (name withheld), Denison Barracks, Hermitage, Berkshire, 7 June 2017.

298 *Department of Defense Dictionary of Military and Associated Terms*, 155.

299 Author interview, 77th Brigade Personnel 1.

300 Author interview, 77th Brigade Personnel 2.

301 Author interview, 77th Brigade Personnel 1.

302 Jonathan Owen, 'British Army Ramps up Information Warfare Capability to Meet 21st-Century Threats', *PR Week*, 6 August 2019, at https://www.prweek.com/article/1593186/british-army-ramps-information-warfare-capability-meet-21st-century-threats (accessed 26 March 2020).

303 Ben Farmer, 'Woolwich Attack: Troops Advised Not to Wear Uniform outside Bases', *The Telegraph*, 23 May 2013, at http://www.telegraph.co.uk/news/uknews/crime/10075476/Woolwich-attack-troops-advised-not-to-wear-uniform-outside-bases.html (accessed 28 January 2017).

304 Ekin Karasin, 'British Soldiers are Told to "Scrub" Facebook Accounts of All Uniform Pictures and to Jog in Pairs for Fear of New Lee Rigby-Style ISIS Attacks', *Mail Online*, 25 July 2016, at http://www.dailymail.co.uk/news/article-3705665/British-soldiers-told-scrub-social-media-accounts-uniform-pictures-jog-pairs-fear-new-Lee-Rigby-style-attacks-ISIS.html (accessed 28 January 2017).

305 'Social Media Guidance', *The British Army*, at https://www.army.mod.uk/digital-communications/social-media-guidance/ (accessed 26 March 2020).

306 British Army, *#DigitalArmy: Using Social Media in the British Army* (2018), 5, at https://indd.adobe.com/view/4a92013b-c1f0-4e86-a710-f2ca0604a36d (accessed 26 March 2020).

307 British Army, *#DigitalArmy*, 3.

308 Partnership for Conflict, Crime, and Security Research, 'Social Media in the Armed Forces', *Evidence Briefing*, Economic and Social Research Council, October 2016, at http://www.esrc.ac.uk/files/news-events-and-publications/evidence-briefings/social-media-in-the-armed-forces/ (accessed 28 January 2017).

309 Reuven Gal and Stuart A Cohen, 'Israel: Still Waiting in the Wings', in Charles C Moskos, John Allen Williams and David R Segal (eds), *The Postmodern Military: Armed Forces after the Cold War* (New York: Oxford University Press, 2000), 224.

310 *Tsahal*, the name by which the Israelis know their military, is the Hebrew acronym for *Tsva ha-Hagana le-Yisra'el*, which translates as 'The Army of Defence for Israel'.

311 Miluim website, at http://www.miluim.aka.idf.il/894-he/Miluim.aspx (accessed 28 March 2020). Women's service in the reserves is voluntary.

312 Yoram Peri, 'Intractable Conflict and the Media', *Israel Studies* 12(1) (2007), 88, 87.

313 Rebecca Schiff, 'Civil-Military Relations Reconsidered: Israel as an "Uncivil" State', *Security Studies* 1(4) (1992), 646.

314 Gal and Cohen, 'Israel: Still Waiting in the Wings', 224.

315 Author interview, IDF Interviewee 1 (name withheld), Tel Aviv, 13 June 2017.

316 Hasan Al-Rizzo, 'The Undeclared Cyberspace War between Hezbollah and Israel', *Contemporary Arab Affairs* 1(3) (2008), 392, 399.

317 Al-Rizzo, 'The Undeclared Cyberspace War', 398.

318 For more on this see Adi Kuntsman and Rebecca L Stein, *Digital Militarism: Israel's Occupation in the Social Media Age* (Stanford: Stanford University Press, 2015), 24.

319 Rid and Hecker, *War 2.0*, 101. Rid and Hecker offer a handy synopsis of IDF–media relations from independence to the Second Intifada in 2000. The relationship, they argue, falls into four main periods: independence to the 1973 Yom Kippur War; the Yom Kippur War to the 1982 Lebanon War; the Lebanon War to the 1993 Oslo Accords; and the Oslo Accords to the outbreak of the Second Intifada in 2000. For more detail on the characteristics of each period see Rid and Hecker, *War 2.0*, 104–105. Michal Shavit brings this picture up to date with a detailed analysis of the evolution of the IDF's media and information operations policies from 2000 to 2014 in *Media Strategy and Military Operations in the 21st Century: Mediatizing the Israel Defence Forces* (London: Routledge, 2017).

320 Shavit, *Media Strategy and Military Operations in the 21st Century*, 2.

321 Shavit, *Media Strategy and Military Operations in the 21st Century*, 2, 57.

322 Shavit, *Media Strategy and Military Operations in the 21st Century*, 85.

323 Schejter and Cohen note that in 2009, 91.8 per cent of Israeli households possessed a mobile phone (Amit Schejter and Akiba Cohen, 'Mobile Phone Usage as an Indicator of Solidarity: Israelis at War in 2006 and 2009', *Mobile Media and Communication* 1(2) (2013), 174–95). By 2013, 'Israel was said to lead Europe and the United States in smartphone usage' (Kuntsman and Stein, *Digital Militarism*, 108).

324 Amos Harel, 'Soldier Killed, 3 Missing after Navy Vessel Hit off Beirut Coast', *Haaretz*, 16 July 2007, at https://web.archive.org/web/20060718032259/http://haaretz.com/hasen/spages/738695.html (accessed 30 January 2017).

325 Rid and Hecker, *War 2.0*, 119. For the Hezbollah broadcast see Hezbollah, 'Hezbollah Shooting on Israeli Warship INS *Hanit*', *YouTube*, 21 July 2006, at https://www.youtube.com/watch?v=lR4KlJk5q0U (accessed 28 January 2017). The video has been viewed more than 60,000 times. The sailors aboard *Hanit* were even quicker off the mark, using their mobile phones from the ship to call and text their families to reassure them that they were fine.

326 Kuntsman and Stein, *Digital Militarism*, 25. I have altered Kuntsman and Stein's spelling of 'Hizballah' to 'Hezbollah' in this and all further quotations for the purposes of consistency.

See also Sabrine Saad, Stéphane Bazan and Christophe Varin, 'Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a New Strategic Battlefield', https://www.researchgate.net/publication/229005501_Asymmetric_Cyber-warfare_between_Israel_and_Hezbollah_The_Web_as_a_new_strategic_battlefield (accessed 30 January 2017).

327 Shavit, *Media Strategy and Military Operations in the 21st Century*, 106.

328 The government and the IDF had failed to achieve any of the goals they had set for themselves at the war's outset. They had identified three principal objectives—to rescue two kidnapped IDF soldiers, to destroy Hezbollah and to force the cessation of rocket attacks from southern Lebanon on northern Israel—but achieved none of them. The inquiries included the high-profile Winograd Commission, the State Comptroller's report on the treatment of the press, and a report from the Israeli Press Council, alongside classified military inquiries into various aspects of the IDF's performance.

329 Rid and Hecker, *War 2.0*, 121–122.

330 Rebecca L Stein, 'Impossible Witness: Israeli Visuality, Palestinian Testimony and the Gaza War', *Journal for Cultural Research* 16(2–3) (2012), 137. I have altered Stein's spelling of 'Hizballah' to 'Hezbollah' in this and all further quotations for the purposes of consistency. See also Marvin Kalb and Carol Saivetz, 'The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict', *The Harvard International Journal of Press/Politics* 12(3) (2007), 43–66.

331 Shavit, *Media Strategy and Military Operations in the 21st Century*, 137.

332 Shavit, *Media Strategy and Military Operations in the 21st Century*, 138, 139. The Spokesperson's Office, later the Spokesperson's Division, is now the Spokesperson's Unit: 'The purpose of the IDF Spokesperson's Unit is to report on the accomplishments and activities of the IDF to the Israeli and international public, to nurture public confidence in the IDF, and to serve as the IDF's primary professional authority on matters of public relations and distribution of information to the public' ('IDF Spokesperson's Unit', *Israel Defense Forces* blog, nd, at https://www.idfblog.com/about/idf-spokespersons-unit/ (accessed 3 February 2017). This link is no longer active.

333 Shavit, *Media Strategy and Military Operations in the 21st Century*, 138, 139.

334 David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century* (New York: Basic Books, 2017), 51.

335 Shavit, *Media Strategy and Military Operations in the 21st Century*, 142; Asher Schechter, 'The Social Intifada: How Millennials and Facebook Beat the Almighty Israeli Army', *Haaretz*, 5 May 2014, at http://www.haaretz.com/israel-news/.premium-1.589032 (accessed 3 February 2017).

336 Alison Hoffman, 'The "Kids" Behind IDF's Media', *Tablet*, 20 November 2009, at https://www.tabletmag.com/jewish-news-and-politics/117235/the-kids-behind-idf-media (accessed 3 February 2017).

337 Shavit, *Media Strategy and Military Operations in the 21st Century*, 145.

338 Patrikarakos, *War in 140 Characters*, 53.

339 Patrikarakos, *War in 140 Characters*, 55.

340 Shavit, *Media Strategy and Military Operations in the 21st Century*, 146.

341 Shavit, *Media Strategy and Military Operations in the 21st Century*, 147.

342 Shavit, *Media Strategy and Military Operations in the 21st Century*, 147. See also Yaakov Lappin, 'IAF strike kills Hamas military chief Jabari', *The Jerusalem Post*, 14 November 2012, at http://www.jpost.com/Defense/IAF-strike-kills-Hamas-military-chief-Jabari (accessed 3 February 2017).

343 IDF Spokesperson (@IDFSpokesperson), 'Ahmed Jabari: Eliminated', *Twitter*, 14 November 2012, at https://twitter.com/search?q=IDFSpokesperson (accessed 2 February 2017). This link is no longer active.

344 Israel Defense Forces (@IDF), 'We recommend that no Hamas operatives …', *Twitter*, 14 November 2012, at https://twitter.com/idf/status/268780918209118208?lang=en (accessed 2 February 2017).

345 Alqassam Brigades(@Alqassambrigade), *Twitter*, 14 November 2012. The al-Qassam Brigades Twitter account is suspended.

346 Shavit, *Media Strategy and Military Operations in the 21st Century*, 148.

347 Thomas Zeitzoff, 'Does Social Media Influence Conflict? Evidence from the 2012 Gaza Conflict', *Journal of Conflict Resolution* 62(1) (2018), 29–63. See in particular 46–49.

348 Noam Cohen, 'In Gaza Conflict, Fighting with Weapons and Postings on Twitter', *The New York Times*, 21 November 2012, at http://www.nytimes.com/2012/11/22/world/middleeast/in-gaza-conflict-fighting-with-weapons-and-postings-on-twitter.html (accessed 2 February 2017).

349 Yaakov Lappin, 'Gaza terrorists fire two rockets at Tel Aviv', *Jerusalem Post*, 16 November 2012, https://www.jpost.com/defense/gaza-terrorists-fire-two-rockets-at-tel-aviv (accessed 2 February 2017).

350 Lappin, 'Gaza terrorists' (accessed 2 February 2017).

351 Israel Defense Forces (@IDF), 'What would you do if rockets were striking your country?', *Twitter*, 16 November 2012, at https://twitter.com/idfspokesperson/status/269419585101512704 (accessed 2 February 2017).

352 Kuntsman and Stein, *Digital Militarism*, 33–34.

353 Israel Under Fire (@IsraelUnderFireLive), 'About', *Facebook*, nd, at https://www.facebook.com/pg/IsraelUnderFireLive/about/?ref=page_internal (accessed 2 February 2017).

354 Reuven Ben-Shalom, 'Hasbara, Public Diplomacy and Propaganda', *The Jerusalem Post*, 12 June 2014), at http://www.jpost.com/Opinion/Op-Ed-Contributors/Hasbara-public-diplomacy-and-propaganda-358211 (accessed 28 February 2017).

355 Matthew Hall, 'Israeli Propaganda Hits Social Media', *The Sydney Morning Herald*, 18 July 2014, at http://www.smh.com.au/it-pro/government-it/israeli-propaganda-war-hits-social-media-20140717-ztvky.html (accessed 3 February 2017). Notably, the structure of the volunteer groups mimicked that of the Interactive Media Branch in the Spokesperson's Unit.

356 Leibovich had spent the preceding eight years as the IDF's official spokesperson to the international media. For an interview with her see Sue Tomchin, 'Going on the Digital Offensive', *Jewish Woman Magazine*, Winter 2015, at https://www.jwmag.org/sslpage.aspx?pid=3851#sthash.1evGaqfY.dpbs (accessed 4 February 2017). This link is no longer active.

357 Dara Kerr, 'How Israel and Hamas Weaponized Social Media', *C-Net*, 13 January 2014, at https://www.cnet.com/au/news/how-israel-and-hamas-weaponized-social-media/ (accessed 4 February 2017).

358 Israel Defence Forces (@IDF), *Twitter*, at https://twitter.com/idf?lang=en; Israel Defence Forces (@idfonline) (accessed 9 August 2019), *Facebook*, at https://www.facebook.com/idfonline/ (accessed 9 August 2019).

359 IDF Spokesperson's Unit, 'Social Media', https://www.idfblog.com/join/ (accessed 4 February 2017). This link is no longer active.

360 IDF Interviewee 1, Tel Aviv, 13 June 2017.

361 IDF interviewee 1, 13 June 2017.

362 IDF interviewee 1, 13 June 2017.

363 IDF interviewee 1, 13 June 2017.

364 'Allied Command Transformation's mission is to contribute to preserving the peace, security and territorial integrity of Alliance member states by leading the warfare development of military structures, forces, capabilities and doctrines … From its inception in 2003, Allied Command Transformation demonstrated the importance placed by NATO Nations on the roles of transformation and development as continuous and essential drivers for change' (Allied Command Transformation, 'Who We Are', *NATO Headquarters, Supreme Allied Commander Transformation*, at https://www.act.nato.int/who-we-are (accessed 9 August 2019).

365 See Allied Command Transformation, 'Who We Are', at https://www.act.nato.int/who-we-are. The link to the original NATO website, http://www.act.nato.int/mcdc, has since been disabled.

366 MCDC, *Use of Social Media as an Effector*, 4.

367 MCDC, *Use of Social Media as an Effector*, 4.

368 Author interview, NATO Forces Interviewee 1 (name withheld), Mayen, Germany, 12 October 2017.

369 See Allen and Gerras, 'Developing Creative and Critical Thinkers', *Military Review* 89(6) (2009), 77–83; Toomas Möls, 'Critical and Creative Thinking: Are Innovation and Initiative Welcome in the Military?', *ENDC Proceedings* 13 (2010), 7–17; Brigadier J Nazareth, *Creative Thinking in Warfare* (Atlanta: Lancer Publishers, 2013); Gabriel Serbu, 'The Dangers of Anti-Intellectualism in Contemporary Western Armies', *Infantry* 99(4) (2010), 44–47; Leon Young, 'The Conservative Colonel': How Being Creative Killed Your Career in the ADF', *Australian Defence Force Journal* 203 (2018), 47–56.

370 Marilyn Higgins and James Morgan, 'The Role of Creativity in Planning: The "Creative Practitioner"', *Planning Practice and Research* 15(1–2) (2000), 117–127.

371 Nazareth, *Creative Thinking in Warfare*, 81, 82.

372 Milan Vego, 'On Military Creativity', *Joint Forces Quarterly* 70(3) (2013), 84.

373 Möls, 'Critical and Creative Thinking', 31.

374 Young, 'The Conservative Colonel', 52.

375 Nazareth, *Creative Thinking in Warfare*, 81–83.

376 Young, 'The Conservative Colonel', 50.

377 Merrin, *Digital War*, 112.

378 Merrin, *Digital War*, 113.

379 See Rid and Hecker, *War 2.0*, 10.

380 Andrew Hoskins and Ben O'Loughlin, *War and Media: The Emergence of Diffused War* (Cambridge: Polity, 2010), 2.

381 Rid and Hecker, *War 2.0*, 10.

382 Chris Hables Gray and Ángel J Gordo, 'Social Media in Conflict: Comparing Military and Social-Movement Technocultures', *Cultural Politics* 10(3) (2014), 251–261, 252.

383 Rid and Hecker, *War 2.0*, 188.

384 Brynjar Lia, *Architect of Global Jihad: The Life of Al-Qaeda Strategist Abu Mus'ab Al-Suri* (New York: Columbia University Press, 2008), 420.

385 Lia, *Architect of Global Jihad*, 420, 17.

386 Lia, *Architect of Global Jihad*, 393; Brynjar Lia, 'Doctrines for Jihadi Terrorist Training', *Terrorism and Political Violence* 20(4) (2008), 533.

387 Rid and Hecker point out the close parallels between al-Suri's vision of global jihad, and the organisational logic of Web 2.0: 'both assumed entrepreneurial individuals as part of a global community of like-minded activists, self-motivated participation, decentralized networks, self-administration, a common purpose, and global collaboration' (*War 2.0*, 193).

388 See MCDC, *Analytical Concept*, 16–18; Maltby, Thornham and Bennett, 'Capability in the Digital'; Sarah Maltby and Helen Thornham, 'The Digital Mundane, Social Media and the Military', *Media, Culture and Society* 38(8) (2016), 1153–1168.

389 MCDC, *Analytical Concept*, 16–18.

390 MCDC, *Analytical Concept*, 17.

391 Hables Gray and Gordo, 'Social Media in Conflict', 255.

392 Merrin, *Digital War*, 196.

393 Merrin, *Digital War*, 196.

394 For more on this see Charles C Moskos, John Allen Williams and David R Segal (eds), *The Postmodern Military: Armed Forces After the Cold War* (New York: Oxford University Press, 2000).

395 Paul Scharre, 'American Strategy and the Six Phases of Grief', *War on the Rocks*, 6 October 2016, at https://warontherocks.com/2016/10/american-strategy-and-the-six-phases-of-grief/ (accessed 17 August 2019).

396 Lawrence Freedman, 'The Possibilities and Limits of Strategic Narratives', in Beatrice De Graaf, George Dimitriu and Jens Ringsmose (eds), *Strategic Narratives, Public Opinion and War: Winning Domestic Support for the Afghan War* (New York: Routledge, 2015), 18.

397 See Baxter Oliphant, 'The Iraq War Continues to Divide the U.S. Public, 15 Years After It Began', *Fact Tank: Pew Research Center*, 19 March 2018, at https://www.pewresearch.org/fact-tank/2018/03/19/iraq-war-continues-to-divide-u-s-public-15-years-after-it-began (accessed 17 August 2019); William Maley, 'The War in Afghanistan: Australia's Strategic Narratives', in De Graaf, Dimitriu and Ringsmose, *Strategic Narratives, Public Opinion and War*, 81–98.

About the Author

Dr Kevin Foster

Associate Professor Kevin Foster is Head of the School of Languages, Literatures, Cultures and Linguistics at Monash University in Melbourne. Educated in the UK, Canada and Australia, he has conducted original research with the Australian, British, Canadian, Dutch, US and Israeli militaries. He has published widely on the representation of war, military-media relations, the cultural history of the military, national identity and combat photography. His work has appeared in a range of national and international journals. He is the author/editor of a number of books including *Don't Mention the War: the Australian Defence Force, the Media and the Afghan Conflict* (2015). His latest monograph, *Anti-Social Media: Conventional Militaries in the Digital Battlespace*, will be published in 2021.