PHD

Contemporary Conflict and the Online Information Environment

An examination of American military engagement with Web 2.0

Revie, Roy

Award date:
2015

Awarding institution:
University of Bath

Contemporary Conflict and the Online Information Environment: An examination of American military engagement with Web 2.0

Roy Revie

A Thesis Submitted for the Degree of Doctor of Philosophy

University of Bath – Department of Social and Policy Sciences

December 2014

Table Of Contents

Thanks to my family who have supported and inspired me in a million ways since forever. And to Susan, whose patience, encouragement, help and faith this would have been impossible without.

This thesis examines developments in American military thought, organisation and practice in response to the conditions of Digital Age conflict – the contemporaneous rise of Web 2.0 and of forms of conflict (counterinsurgency and counter-terrorism) associated with the 'Global War on Terror' (GWOT). The research focuses on areas of military activity under the categories of special operations, information operations and intelligence. These are identified as those most effected by new Web technology and GWOT-era warfare, and significant developments of interest are identified and examined. I explore how Digital Age conflict is conceived of as a 'problem field' from the military perspective; and then examine how developments in areas from discourse to practice cohere to form an 'apparatus' through which this 'problem' is addressed.

The research area is one in which access is a challenge, as such the research relies primarily on open source documentary data, collated and analysed in a way which provides significant insight to an opaque area of military practice. The thesis includes an analysis of military doctrine, propaganda websites, psychological operations practice, and cutting-edge R&D programmes. It is demonstrated that as well as being challenged by Digital Age conflict, the US military is empowered in the areas of strategy, intelligence and communication to develop new practices which enhance their ability to operate in the contemporary environment.

Ultimately, the thesis argues, developments in the US military response to Web 2.0 mean that traditional understanding of military communication in terms of linear 'propaganda' messages must be augmented with an approach which understands military communication power through a holistic examination of the multiplicity of practices which collect, process, and distribute information within the Web 2.0 information environment. This form of emerging "CY-OPS" activity has wide-ranging consequences for our understanding of the Web as a social space.

List Of Abbreviations

AFRICOM – Africa Command (US)
AFRL – Air Force Research Laboratory
ARSOF – Army Special Operations Forces
C4ISR – Command, Control, Communication, Computers, Information, Surveillance, Reconnaissance
CASOS – Computational Analysis of Social and Organizations Systems Center
CENTCOM – Central Command (US)
CIA – Central Intelligence Agency
CIC – Cultural Intelligence Cell
CJCS – Chairman of the Joint Chiefs of Staff
COCOM – Combatant Command
COIN – Counterinsurgency
CORE – Common Operational Research Environment
CSCC – Center for Strategic Counterterrorism Communication
CVE – Counter-Violent Extremism
CVP – Credible Voices Program
CYBERCOM – Cyber Command (US)
CY-OPS – Cyber-Psychological Operations
DARPA – Defense Advanced Research Projects Agency
DET – Digital Engagement Team
DOD – Department of Defense (US)
DSB – Defense Science Board
DTNA – Dynamic Twitter Network Analysis
EUCOM – European Command (US)
EZLN – Ejército Zapatista e Liberación Nacional (Zapatista Army of National Liberation)
FARC – Fuerzas Revolucionarias de Colombia (Revolutionary Armed Forces of Colombia)
FM – Field Manual
FSA – Free Syrian Army
ICCCD – International Conference on Computational Cultural Dynamics
ICTs – Information and Communication Technologies
IED – Improvised Explosive Device
IIA – Inform and Influence Activities *or* Interactive Internet Activities
IO – Information Operations
ISAF – International Security Assistance Force
JIC – Joint Integrating Concept
JIEDDO – Joint Improvised Explosive Device Defeat Organization
JP – Joint Publication
JSOC – Joint Special Operations Command
JTF – Joint Task Force
FBO – Federal Business Opportunities
FOI – Freedom Of Information
GAO – Government Accountability Office

GCHQ – Government Communication Headquarters (UK)
GWOT – Global War On Terror
HSCB – Human Sociocultural Behavioural (Modeling Program)
MILDEC – Military Deception
MISO – Military Information Support Operations (see also PSYOPS)
MIS – Military Information Support
MISG – Military Information Support Group
MISOC – Military Information Support Operations Command
MIST – Military Information Support Team
MOD – Ministry of Defence (UK)
NAVSPECWARCOM – Naval Special Warfare Command
NIOC – Navy Information Operations Command
NORTHCOM – Northern Command (US)
NSA – National Security Agency (US)
ONR – Office of Naval Research
OODA – Observe, Orient, Decide, Act
OPSEC – Operational Security
ORA – Operational Risk Analyzer
OSD – Office of the Secretary of Defense
P2P – Peer-to-Peer
PA – Public Affairs
PACOM – Pacific Command (US)
PR – Public Relations
PSYOPS – Psychological Operations
QDR – Quadrennial Defense Review
R&D – Research and Development
RDT&E – Research, Development, Test and Evaluation
RMA – Revolution in Military Affairs
RWIP – Regional Web Interaction Program
SBIR – Small Business Innovation Research
SMA – Strategic Multi-Layer Assessment
SMISC – Social Media In Strategic Communication
SNA – Social Network Analysis
SNARC – Social Network Analysis Reachback Capability
SOCOM – Special Operations Command (US)
SORDAC – Special Operations Research, Development & Acquisition Center
SOUTHCOM – Southern Command (US)
STTR – Small Business Technology Transfer
TRADOC – Training and Doctrine Command (US Army)
TRMP – Trans Regional MISO Program
TRWI – Trans Regional Web Initative
TTP – Tactics, Techniques and Procedures
USAF – United States Air Force
USMC – United States Marine Corps

UW – Unconventional Warfare
VOIP – Voice of Internet Protocol
W-ICEWS – Worldwide Integrated Crisis Early Warning System

1. Digital Age Conflict: The US Military, ICTs, and Public Communication

1.1. From Embedding to Abu Ghraib: Outlining the Research Problem

In December 2003, 9 months after the US-led invasion of Iraq and 7 months after President Bush had declared "mission accomplished" on the deck of the *USS Abraham Lincoln*, a report was released by the British Ministry of Defence (MOD) favourably assessing the media-management practices of coalitions forces (MOD, 2003). This had been based on a system of 'embedding' journalists within individual combat units, and a network of shiny media "Information Centres" across the conflict zone. Embedding represented the outcome of a refinement in the military-media relationship over the previous 40 years (Rid, 2007), and was seen to establish a situation where the mass media were relatively happy with access to the battlefield, publics received more direct news footage than ever, and the military got the sort of compliant coverage they wanted – with the MOD report noting that 90% of reporting was "neutral or positive" towards coalition activity.

Something happened in the following years however that means when historians look back at the wars in Iraq and Afghanistan it is not this embedded footage that will be the most memorable, or the most important. Instead of the camaraderie of coalition forces, their technical and strategic superiority, and Western armour rolling across the desert in the swift advance on Baghdad, the images of most significance may prove to be the grainy mobile phone footage of Saddam Hussein's execution, the gruesome torture photos from Abu Ghraib, and the numerous videos posted online of beheadings, military abuses, and other 'unofficial' versions of the war. Fuelled by the rise of cheap recording devices, proliferating internet connectivity, and conditions of asymmetric conflict, these images signalled the end of the fine-tuned relationship between Western states, media and publics during conflict and presented an altogether more messy communication environment in which the increase in power of information to significantly affect outcomes is matched by its uncontrollability.

This shift outlines the situation at the heart of the research presented in this thesis: one in which changing information communication technologies (ICTs) characterised by the rise of Web 2.0, and the changing forms of warfare characterising the age of the Global War on Terror[1] (GWOT) present important questions to our understanding of the relationship between state power, citizens, and communication during times of conflict. In the conditions of the GWOT, where the "battle for hearts and minds" of global and local populations become key state concerns, a number of practical and strategic challenges are presented to government and military communicators. The contemporaneous conditions of the rise of new ICTs under the rubric of *Web 2.0* – convergent, social and new media; ubiquitous recording technology; free and effectively limitless data storage and reproduction; anonymity and a breakdown of information and communication hierarchies

[1] While the terminology of the "Global War on Terror" has since been dismissed as a George W Bush-era mistake, many of the attendant concepts and elements of strategic thought remain. Here it is taken to refer generally to the period since September 11th, 2001, through the Afghan and Iraq wars, to the drone

– produce a disruptive and challenging information environment with a changing relationship to conflict itself (Rid and Hecker, 2009:vii).

This research is situated in this dual context of GWOT-era conflict and the Web 2.0 information environment, which I call *Digital Age conflict,* and examines how the US military (as the most powerful military actor in the world) is adapting. In doing so, the research takes an investigative approach to studying military doctrine, discourse, structures and practice; uncovering and presenting important developments in the areas of military intelligence, research & development, and psychological operations. The research presented includes analyses of a network of psychological operations websites, clandestine programmes to influence online debate, the use of Web 2.0 in intelligence and special operations practice, and military research programmes at the cutting-edge of research into online influence.

In exploring the changes of Digital Age conflict it becomes clear that existing approaches to the study of military-public communication are insufficient. They focus too narrowly on *the representation* of conflict in *mass* media, or specific media-management practices, when what is required is an approach that allows us to understand the break down in the division between conflict and its representation and the effects of military communication activity on a broader global *information environment.* As such, this thesis develops a theoretical and methodological approach to the study of state communication power drawing on Foucault, and examines how a variety of military practices cohere to form a *propaganda apparatus* addressing the particular challenges of Digital Age conflict. This allows a coherent description of these diffuse practices to be produced, as well as developing an approach to the analysis of military communication practice which allows understanding and insight to be produced in a manner which captures the complexity of communication in the Web 2.0 era.

1.2. Chapter Outline

This chapter proceeds with a discussion of the relationship between ICTs, communication and war – highlighting the importance of the research area and introducing contemporary warfare as one part of the context of Digital Age conflict. I move on in **Chapter 2** to the theoretical background of state communication power and propaganda, and discuss the necessity of a new approach to the analysis of this area. The latter part of this chapter discusses the Web 2.0 aspect of Digital Age conflict as the second important contextual element. **Chapter 3** builds from this theoretical work to a method for the analysis of US military adaptation, outlining an approach drawing on the concept of *governmentality,* which examines how powerful actors discursively construct a "problem field" – in this case of Digital Age conflict – which guides the development of an *apparatus* through which the 'problem' is addressed. The chapter then discusses the more practical aspects of the research – including the substantial challenges of elite-focussed research in an area of military activity characterised by hostile contrast between the researcher and subject.

Chapter 4 presents a formal outline of the problem field as conceived by military actors – exploring evolving thought in the GWOT, particularly in relation to special operations, military intelligence, and psychological operations (PSYOPS). This examination guides the

focus of the further chapters, which address those subjects and areas of activity identified as key sites of interest in military thought. **Chapter 5** addresses developments in PSYOPS practice within the two most active military commands in the GWOT – the US Special Operations and Central commands, examining a network of fake-news websites, programmes insinuating PSYOPS activities into foreign civil society, and both clandestine and overt approaches to influencing online discussion forums. Turning our attention to the area of military research and development (R&D), **Chapter 6** examines a number of military programmes sponsoring research throughout industry and academia, developing a knowledge base for Web 2.0 intelligence and PSYOPS practices, which highlights current and potential future developments in the research area. **Chapter 7** concludes by discussing the development of this propaganda apparatus, assessing the effects on the information environment and highlighting important elements in the study and analysis state communication power.

1.3. War, Communication and Technology: The Emergence of Digital Age Conflict

In addressing the question of military adaptation to a changing context the immediate requirement is for this context to be outlined. This section begins this process by exploring the 'conflict' part of Digital Age conflict (the communication element is addressed in detail in section 2.3), examining how theorists and practitioners have understood the changing nature of the conflicts which characterise the GWOT. In addressing key writings on military strategy, organisational adaptation, and military-media relations, this section traces the relationship between US military activity, communication, and technology from the time of the Vietnam War to the present day. It becomes clear that this relationship is not just a matter of individual communicative acts, but of communication as an infrastructure or environment which has profound effects in enabling and constraining particular forms of military activity. As such, examining this area allows the development of an understanding of communication, technology, and conflict as intertwined and mutually-influential, as well as an appreciation of the particular context of contemporary military practice.

1.3.1. Communication and Conflict From Vietnam to the Revolution in Military Affairs

Communication technology has always played a key role in conflict, from semaphore to satellite (Taylor, 1995), yet it is only in the relatively recent period of mass media information about conflict and mass democratic political participation that public communication itself became a defining feature (see Qualter, 1985:ix) – making information a central strategic element. The salience of public communication in wartime increases with the quantity, quality and speed of information from conflict zones and, in the literature, the second half of the 20th century – with the proliferation of quality news footage from Vietnam and other conflict, the rise of cable and then satellite news, and latterly the Internet – is seen as the period in which the relationship between conflict and its mediation became a key element in understanding the practice and outcomes of warfare (see e.g. Betz, 2012; Rid, 2007; Belknap, 2001).

The development of contemporary military information strategy, with a definite emphasis on media relations and public opinion, can be traced back to the Vietnam war period, which was seen as a turning point in American (and thus wider Western) treatment of the media on the battlefield (Rid, 2007). In Vietnam the media were perceived as largely unconstrained by military power (roving around the battlefield, filming what they liked, broadcasting without constraint) and consequently they were seen by many in the military and political establishment to have "lost the war" by turning American popular opinion against it (see Elegent, 1981). The truth of these accusations is disputed (e.g. see Herman and Chomsky, 1994:169) and to speculate involves a number of counter-factuals – but they key point is that the lack of military and government influence in the information environment was *seen* to be a key reason for American failure, and is still discussed as the "Vietnam Effect" within contemporary US defence circles (Samuels, 2002:59, cited in Biernatzki, 2002:10; see also Betz, 2012:56). Thus between the end of the Vietnam war and the present day there have been a number of key developments in the military-media relationship in which government and military actors began to see media, information and public opinion as an increasingly important element in the conduct of war (Webster, 2003:59).

The key drivers of this adaption were developments in the technological and political context of war. In the world of politics, there was an increasing mediatisation of political activity and life. The media became not just a secondary but a fundamental concern in political decision making. This is process that began with 'mass society' theory in the US in the early 1900s (see page 17), and can be seen in the rise of a culture of political publicity which has reached its apogee in the contemporary phenomena of 'spin' and PR in politics (e.g. Corner, 2007; Sussman, 2012). In this respect, Thrall describes the domestic political imperatives of conflict in the US as the primary reason "for the growth of press controls" over coverage of US military activity in the latter part of the twentieth century (Thrall, 2000:5). The recognition of this mediatisation of politics (see Hjarvard, 2008; Mazzoleni and Schulz, 1999; Brown, 2003), coupled with increased political control over military activity led to government actors "responding to what they perceive to be the growing certainty that the media, if left to their own devices, will turn public opinion against even those conflicts that initially draw great support" (Thrall, 2000:6)[2]. This fear is understood to have led to greater focus on media management and PR, as well as a casualty-aversion and preference for fast wars of overwhelming force.

Beyond the watershed moment for the access of journalists reporting on the ground during conflict, Vietnam also represented a key turning point in military thought regarding the scale of US military deployments. The failure of the war and the huge cost in human life and resources was seen by a new generation of American military leaders as signalling the end of the viability of large-scale ground wars. Where public and political will for such wars was seen to be lacking, military theorists sought a means to continue American military dominance, or at least autonomy. This search converged with a developing focus on advanced technology – with the rise of advanced ICTs and hi-tech sensors and weaponry being conceived of as the future basis of US military dominance, a paradigm

[2] It should be noted that the media 'turning the public against' war need not be a conscious effort by the media in this case – as wars go on and casualties rise, mistakes are made, aims and outcome become unclear and media emerges showing the reality of war, pubic opinion may inevitably shift.

which came to be known as the Revolution in Military Affairs (RMA) (see Hirst, 2005: Lawson, 2008:185-319; Der Derian, 2009). The RMA was seen as the key project underlying "military strategies to project, sustain and deepen US geopolitical power in the post-Cold War period", and centred on technologies of "'stealth,' 'precision' targeting, networked computing, and satellite geo-positioning" (Graham, 2010:154). The paradigm grew in influence from the 70s (Lawson, 2008) and by the 90s was drawing on the most effective uses of modern technologies in commerce, treating the battlefield as a "giant, integrated 'network enterprise' – a 'just-in-time' system of cyborg warriors" (Graham, 2010:155). By exploiting American supremacy in the field of technological innovation, new advanced weapons and "network-centric warfare" concepts which integrated all battlefield activity under a command and control concept known as C4ISR[3] (Rizwan, 2000:1) was understood as underpinning US military dominance on the battlefield, linking everything from intelligence and logistics through to advanced targeting. This was envisaged as producing an efficient, clinical and lightening quick form of warfare. Crucially, one outcome of RMA for those concerned with the "Vietnam Effect" was that "it reduce[d] the risk of undertaking military operations – the risk for US forces, that is" (Graham, 2010:155), thus offering US military power greater flexibility and autonomy of action in the age of proliferating mass media and a casualty-averse public.

While the RMA was conceived of as a strategic approach to achieving 'full spectrum dominance' (Shalikiashvili, 2006; see also Graham, 2010:156), the paradigm also entailed a fundamental ethical dimension. Advanced targeting and intelligence paradigms presented war as 'clean', free of mass civilian casualties and unnecessary destruction. Der Derian (2009) explores the implications of this through the concept of 'virtuous war' – a term which plays on the dual meaning of *virtue* and *virtual* – meaning that advanced sensors, targeting tools, and weaponry produce a form of war which, when combined with new techniques of media management, appeared from one side at least to be relatively bloodless. Shaw describes a type of "risk-transfer war" (2005:75), in which the risks to western-politicians of a casualty-averse domestic public are transferred (as the risk of death) to populations in the warzone – whose remoteness and lack of access or proximity to the global information environment means that they could be sacrificed for the appearance of speedy, efficient war. Of course this is not to say that military or political actors consciously think in terms of "sacrificing" civilians, but that RMA produces a relationship between war and public communication in which certain facets of conflict become obscured, opening avenues of action which might not otherwise exist.

This form of warfare also entails specific forms of media management – a process which becomes much more deeply integrated within planning and operations. Maltby writes that complex media management strategies, beyond crude censorship or 'messaging' as an afterthought to military activity itself, developed based on "minimizing access to the battle space (and hence information) while maximizing control through other means, specifically the employment of manoeuvres that are difficult for the media to verify" (Maltby, 2012:2, see also Thrall, 2000, and Tatham, 2008 for a military point of view)[4]. This RMA-enabled

[3] Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance

[4] Note, Maltby is focusing on only one element of military communication practice – 'media management' – in the context of Digital Age conflict, as we will see, journalists accessing the warzone become the least of the military communicators' worries as information proliferates from other uncontrollable sources.

information-management paradigm led to a military thought which "projects a technological and ethical superiority in which … media dissimulation, global surveillance, and networked warfare combine to deter, discipline, and if need be, destroy the enemy" (Der Derian, 2009:xi). 'Virtue' in this case becomes, further, a dimension of Western hegemony (Der Derian, 2009:xxxi), as those without access to the technology (the 'virtual') are excluded from 'virtue' in the ethical sense – a concept underlined by the seemingly anachronistic clash between the US government's drone assassination program (clinical, hi-tech, dispassionate) and militants' use of suicide bombers (indiscriminate, low-tech, fanatical).

However, the reality of the RMA never quite matched the rhetoric – in its 90s heyday (where the Gulf, Kosovo and Balkans wars saw the paradigm applied to various degrees) there were still highly-public civilian casualties, 92% of the bombs dropped on Iraq in 1992 were 'dumb' bombs (i.e. not guided by laser or GPS technology), and even by the second Iraq war in 2003 this number was still around 40% (Gardner, 2009). Two events are illustrative of the failure of the RMA to live up to the promise of clinical supremacy and the negation of the pressures of adverse public opinion. Firstly, the US precision bombing of the Amiriyah air-raid shelter in Baghdad in 1991, killing 408 civilians in what is considered the most lethal massacre in the history of air warfare (Peterson, 2002) – showing that the 'fog of war' could not be completely eradicated and high-profile mass-casualty events remained a challenge to the unilateral pursuit of war. The second is the infamous *Black Hawk Down* incident in Mogadishu – in which US soldiers became engaged in a prolonged urban battle, the gruesome pictures of which resulted in a withdrawal of U.S. forces from Somalia, due largely to the effects of negative domestic public opinion (Thornton, 2007:10). This development catalysed vigorous debate about the 'CNN effect' of conflict imagery once again driving foreign policy decision making (see e.g. Robinson, 2002; Livingston, 1995; Belknap, 2001). Armistead, editor of the *Journal of Information Warfare,* goes as far as to write that "with the use of a $600 video camera, Aideed changed forever U.S. foreign policy in the region", describing the Somali warlord as a "true information warrior" who overcame a distinct military disadvantage through the "effective use [of the] mass media to his advantage [to influence] the flow of events" (Armistead, 2004:16).

The underlying issues these events exemplify - the persistence of military atrocities in producing negative public opinion, the relative-impotence of many advanced military technologies in the urban warfare scenario (see Graham 2010: 156-159), and the growing unruliness of information from the battlefield in the age of widespread consumer recording devices – were portents of the vulnerability of the public communication element of RMA doctrine. The final blow came, however, after 9/11 and the initial phases of the wars in Afghanistan and Iraq, where the RMA "received a sobering reality check in Baghdad's urban sprawl beginning in late 2003" with the birth of the insurgency (Rid and Hecker, 2009:37). However the importance of relationship between ICTs, public communication and conflict which RMA thinking embraced remains a key element in military thought, strategy and practice – and represents a key area of analysis in understanding contemporary conflict.

1.3.2. The Counter-Revolution in Military Affairs: Counterinsurgency and Global "Population-Centric" Warfare

The challenges presented to RMA thought and practice in the wars following 9/11 (see Burke, 2011, Scahill, 2013) were significant. While the integrated system of sensors, communication systems and high-tech weapons was designed to destroy any military enemy quickly, cleanly and effectively – thus limiting the need for too much public communication activity – the wars the US and its allies quickly became involved in did not feature conventional military enemies. The '9/11 wars' (Burke, 2011) required patience and cultural understanding, and relied as much on human intelligence and communication between all levels of society (often low- or no-tech) than it did on the various aspects of C4ISR. Even the early phase of the 2003 Iraq War did not conform to the type of wars which RMA thinking anticipated, after quickly destroying Iraqi armoured divisions in a conventional war, things got more complicated: the first US casualties in Iraq came during a drive-by shooting by civilian-clothed Fedayeen fighters firing from a civilian vehicle (Rid and Hecker, 2009:130), a portent of the complications of fighting an enemy who refused to conform to the systems which RMA was designed to prosper within. The real significance of the changes became clear during the occupations of Afghanistan and Iraq, both of which became sites of large-scale insurgency. Western forces found themselves having to move beyond the paradigm of the RMA, learning how to fight a counterinsurgency (COIN) war in which, instead of being banished by technological superiority, the element of perception and public communication became central to victory. Rather than being enemy-centric or territorial, the new COIN strategy was *population-centric* (Gentile, 2009), and the public took on central strategic importance (see e.g. Kilcullen, 2006; US Army/Marine Corps – *FM 3-24*, 2006; Payne, 2011; Nagl, 2009).

Insurgency in Iraq and Afghanistan did not represent an entirely new sort of conflict – the tactics of insurgency and counterinsurgency had characterised many of the conflicts (outside of the two World Wars) of the twentieth century, from Mao's revolution to the anti-colonial struggles in Africa and Asia (see e.g. Nagl, 2005; Horne, 2006; Mackinaly, 2009). Indeed, COIN represented a return of some Vietnam-era approaches and, from the perspective of many in the military, the repetition of many of the mistakes of the 60s (see e.g. Payne, 2011; Gentile, 2011; DSB, 2009). However in the contemporary context the rise of insurgencies against militaries based on RMA ideas and presumption of the utility of advanced ICTs for overwhelming force has been presented as a "*counter-revolution* in military affairs in which the established weapons of modern guerrilla warfare (hijackings, car bombs, suicide bombers, small arms and portable rocket launchers)" together with the dispersal of combatants amongst the people "effectively counteract many of the supposed gains from advanced weapons systems and communications networks" (Downey and Murdock, 2003:71). On the ground in Iraq and Afghanistan a shift to COIN warfighting for Western forces meant a reconceptualization of the terrain. No longer was the battle conceived if as one of military vs. military for control of territory or infrastructure, but one for "human terrain" in which the population became the essential referent for all activity (Marr et al, 2008). In conditions of insurgency the entire population of a combat zone become militarily significant as it is split into three groups "insurgent supporters; government supporters; and the (largest group by far) neutrals" – insurgent and counterinsurgent compete for the neutrals "for their acceptance of authority, for legitimacy" (Rid and Hecker, 2009:1; see also US Army/Marine Corps – *FM 3-24*, 2006:A-

5). In this situation, where victory or defeat is judged in terms of perception, the importance of communication and information is paramount.

The counter-revolution in military affairs was contemporaneous with another key accelerant for the role of communication in warfare: the proliferation of advanced ICT. The handheld camcorder used by Aideed in Mogadishu multiplied into millions of smartphones with instant access to YouTube. Rid and Hecker contend that while historically most new ICTs (from semaphore to the radio) have benefited regular armed forces (basically in direct proportion to their wealth) now it is "new media that shape warfare[, and the] technology has increased the options for irregulars much more than it has for governments or armies" (Rid and Hecker, 2009:viii). A number of asymmetries in cost-benefit are produced. For example: secure online communication offers insurgents free, safe, instant, communication not previously available before. Where regular armies could already afford such a capacity, they not only lose their monopoly in this area, but also a traditional means of intelligence gathering (eavesdropping), and are exposed to the dangers of losing control of their own information, of which the WikiLeaks exposure of the Afghan and Iraq 'war logs' is a key example (see New York Times, 2010). In empowering non-state actors to communicate, gather intelligence, and solicit for funds and recruits, Web 2.0 has been described as a *tool* which non-state groups such as insurgents or terrorists can use as a 'force multiplier', and an *environment* which these groups can use to built momentum and support operations, such that New York Police Commissioner Raymond Kelly famously described the Internet as the "new Afghanistan" (Nichols and Honan, 2007).

Of course, in discussing the role of Web 2.0 in these cases of insurgency we must note that due to the poor network and technological penetration – at least during the early stages of the GWOT – there was little direct engagement with local people via social media or the Internet in Iraq and Afghanistan. However – given the situation of these insurgencies within a global information environment there are key immediate outcomes regarding public communication and forward-thinking military actors recognised that these technologies would soon proliferate in warzones, and began to integrate Web 2.0 and COIN thinking both at the theatre and broader strategic level.

1.3.3. Insurgency in the Global Information Environment

With the development of COIN in Iraq and Afghanistan, perhaps the most important conceptual shift in US military thought was the changing relationship between "kinetic" activity and its effects. Kinetic activity (military jargon for the use of violence) is traditionally seen as the primary means of achieving strategic goals such as the destruction of enemy brigades, the capturing of territory, or the killing of key figures. The "information" element of conflict plays a secondary role, trying to affect how this activity is reported or perceived by local or global audiences. However, when the strategic focus of operations is "population-centric", there is a shift in focus from kinetic operations to those based on communication – essentially "everything that the military does and says in theatre becomes a defacto information operation: all actions and words create *informational effects* on the perceptions of the population, whether intended or not" (Collings and Rohozinski, 2006:1). Information Operations refers here to a doctrinal term for a group of military practices relating to military communication, examined in chapter

4, but the broader point here goes beyond military doctrine. In simple terms: the impact of military activity on the world of information and communication is more significant in the COIN environment than the impact on the physical world[5]. When your enemy is not a conventional military and the battlefield is for 'hearts and minds' of populations, kinetic-focussed RMA practices and the attendant relationship with communication and public opinion go out the window.

This feature is emphasised on the contemporary battlefield full of Aideeds, "where anyone armed with a hundred dollar digital camera and access to the Internet can become an 'information warrior'" (Collings and Rohzinski, 2006:ix). The networked nature of recording devices mean any event can potentially be recorded and have "information effects" beyond the immediate physical environment, influencing perceptions both in the conflict zone and in the wider world. This produces a much more complex operating environment for military activity "encompassing an overarching battle of ideas fought at the local level over the "hearts and minds" of the indigenous population", within an information environment where that local battle both influences and is influenced by external information due to the scope of global communication networks (Collings and Rohozinski, 2006:ix). This is recognised by Murphy[6] who writes that "it is apparent from both current military operations and the environment in which they occur that information and influence as applied to military success will become increasingly important while significantly more complex" (Murphy, 2012:47) – referring to the "transparency of the information environment" due to Web 2.0, meaning that "military operations will not only have the ability to shape the information environment, but also in turn risk being shaped by it" (Murphy, 2012:48). Research presented in this thesis demonstrates how in the fields of strategic thinking, intelligence and military communication, this information environment and military activity shape and influence each other.

The rise of Web 2.0 at the same time as COIN means that insurgency in the Digital Age is not consigned to local areas of operation. Rather, it becomes a diffuse and global affair – the human terrain is not "confined by the same physical borders as the theatre of operations [, as] the media environment allow[s] a potentially worldwide audience to witness what happen[s]" creating a globally-dispersed "active audience" for the insurgency (Rid and Hecker, 2009:7). The information effects produced in COIN conflicts are not constrained by the borders of the battlefield, with publics outside of the conflict zone playing key roles and globalising the 'population-centric' nature of conflict. From the military perspective, this creates a 'soft spot' insurgents attempt to attack – the "open flank" of militaries in the GWOT era: domestic support for operations (Rid and Hecker, 2009:2; see also Mackinaly, 2009:85, Hammes, 2009:28, Betz, 2008:3). Global and domestic publics become strategic targets for insurgents because they offer the possibility of limiting the autonomy of militaries through, for example: elections (such as the withdrawal of Spanish troops from Iraq in 2004 (Jefferey, 2004)); protests (such as those calling for an end to drone strikes in Pakistan (Al Jazeera, 2011)); or through the legal

[5] This concept is known as "Effects Based Operations" in the UK, in which every military maneuver is judged in terms of what it communicates to various target audiences in order to pursue a desired cognitive end-state (see Taverner, 2007:141)

[6] Then-director of the Information in Warfare Group at Center for Strategic Leadership at the US Army War College

system (for example the use of 'universal jurisdiction' to pursue Israeli officials for war crimes (Bowcott, 2011)). Similarly, militaries involved in counterinsurgencies and their political backers have their own power base in domestic opinion, requiring the support of political and other elite audiences in order to succeed. As such, the population of the global information environment can be seen as enabling or limiting counterinsurgent military actors meaning that, like in-theatre public opinion, it becomes instrumentalized in military strategic thinking.

In this context a number of military-linked analysts have situated the conflicts in Afghanistan and Iraq within a broader situation of "global insurgency" (see Betz, 2008; Mackinlay, 2009; Kilcullen, 2005). Through presenting a broad understanding of Islamist insurgency – including in some respect everyone from Al Qaeda members to Islamist politicians to disenfranchised and poor Muslim communities to disaffected diasporas (Makinlay, 2009:79, see also Kilcullen, 2005) – Mackinlay argues that global insurgencies take on "whispy, informal patterns, without territory and without formal command structures that are not easily touched by the kinetic blows of a formal military campaign" (Mackinlay, 2009:6). These are further empowered by the "information anarchy" of Web 2.0 in which "information asymmetry [becomes] an uncontrollable nightmare" for the counterinsurgent (Mackinlay, 2009:95) – allowing non-state actors the same potential communicative-reach as governments, and for images of conflict to proliferate beyond the bounds of military information control in ways which can have an impact on global public opinion. Mackinaly does not advocate an international military campaign to tackle this perceived menace, rather he recognises that for the most part COIN is a fundamentally political and social project (Mackinaly, 2009:5), noting the example of British counter-extremism policy which - taking in social, criminal justice, and intelligence projects - is basically a domestic counterinsurgency campaign (Mackinlay, 2009:7-8, see also Sabir, 2014).

As a fundamentally more socially-embedded form of war – the relationship between ICTs, public communication, and conflict in the contemporary strategic environment is of enhanced significance. Betz refers to a dimension of the GWOT which takes place in the "virtual, informational realm in which belligerents content with words and images to manufacture strategic narratives which are more compelling than those of the other side" (Betz, 2008:1), and the rhetoric of a "battle of ideas" and global "hearts and minds" is a key feature of post-9/11 military discourse (see Echevaria, 2008; Payne, 2009; Waller, 2007; Corman et al, 2008). This rhetoric signifies an important shift in thinking relating to the information and communication, with an architect of US military information strategy describing how the global information environment has "become a battlespace" in which ICTs are used "to deliver critical and influential content in order to shape perceptions, influence opinions, and control behaviour" (Kuehl in Armistead, 2004:xvii). We can also see this in the thinking of the key symbolic enemy in the GWOT – with Ayman Al-Zahwari[7] saying "we are in a battle, and … more than half of this battle is taking place in the battlefield of the media" (al-Zawahiri, 2005). In providing a heightened level of connection between events on the ground and a global audience through Web 2.0-enabled

[7] Here he is chastising Al Qaeda in Iraq leader Abu Musab al-Zarqawi for beheading too many people on video and thus alienating potential followers, demonstrating the strength of the link between the "kinetic" and "non-kinetic" in insurgent thought, too.

information recording and dissemination the "connection between the popular perception of the war and the physical battlefield is much more immediate and therefor more volatile" (Betz, 2008:9) – making it a key area of military concern and significant adaption.

The concept of 'global insurgency' suggests the impact of the global information is not simply contemporaneous with insurgency, but is a key contributing factor to the nature of contemporary conflict with important strategic implications. This is recognised by insurgents at least as much as it is by Western military thinkers. Betz writes that insurgents who are overmatched militarily seek to shift "the centre of gravity… away from populations defined by territory to the 'virtual dimension' where identities are more fluid" (Betz, 2012:54) and where "propaganda of the deed" such as terrorist attacks or relatively minor attacks on counterinsurgent forces can have greater impact. For example we can see IED attacks filmed and posted online as seeking to amplify the physical effects of attacks in the information domain (building a narrative of vulnerability, encouraging insurgent allies and soliciting recruits), and the role of similar videos emerged as a key element in soliciting funds for rebel groups in Syria (Abdul-Ahad, 2013), showing both a strategic and logistics role. Hammes notes that in the contemporary information environment "the tactical, operational, and strategic levels of war merge. One reason that [insurgents] videotape almost every attack is because they understand that while the attack is tactical, the resulting video is a crucial element of their strategic information campaign" (Hammes, 2009:27). In this understanding the connection provided by Web 2.0 ICTs to broader audiences means that these audiences become more interested in the war in terms of direct access to information, but also that these audiences become a strategic interest themselves.

The understanding of global insurgency evidently draws political dissent, social dissatisfaction, and other non-military areas into military consideration. In this regard, strategic developments echo more locally-based COIN thought and practice, which is self-consciously social and political. The Army's influential COIN Field Manual notes that "COIN operations can be characterized as armed social work. It includes attempts to redress basic social and political problems while being shot at" (US Army/Marine Corps – *FM 3-24,* 2006:A-7). It also follows the development of post-Cold War thought in the US military which sought to adapt thinking to the complex and politically- and socially-complicated 'new wars' of the globalised world (Kaldor, 1999). Influential amongst these theories is Arquilla and Roenfeld's[8] concept of *social netwar* – which draws on the examples of the Zapatista EZLN in Mexico, the Chechen guerrillas in the first Chechen war, and the International Campaign to Ban Landmines to argue that asymmetric conflict, networks of irregular actors, and a global interconnected information environment mean there is a new "comprehensive information-oriented approach to social conflict" (Arquilla and Ronfeldt, 1997:4-6, see also Hammes (2006) on *Fourth Generation Warfare*) in which militarily or otherwise structurally weak actors can challenge major powers. In social netwar "outcomes of conflicts increasingly depend on information and communications", the use of "soft power" (Nye, 2004), and the rise of information operations, "perception

[8]Arquilla and Ronfeldt are influential military futurists, their book *In Athena's Camp* featured "a list of key readings about information-age conflict that circulated at high levels of the Pentagon" in the mid 90s (Arquilla and Ronfeldt, 1997:4), they have both published work for the RAND Corporation, and Arquilla is Chair of the Department of Defense Analysis at the Naval Postgraduate School and continues to be an influential writer on information warfare (see e.g. Arquilla, 2013)

management" and "psychological disruption" (Arquilla and Ronfeldt, 2001:2). Thus we can that the rise of asymmetric actors as challenges to US military dominance and new communication considerations are not completely *sui generis* – but draw on paradigms developed since at least the 90s which see new technological and social factors as driving changes in the strategic environment.

1.4. The Socio-Technical Battleground of Digital Age Conflict

The important point which this thesis draws from this changing military context is that in the contemporary conflict situation US military thought addresses the challenges of Web 2.0 and population-centric or asymmetric conflict as deeply intertwined. They are "*socio-technical* changes which have been transforming warfare, as opposed to the merely technological ones" (Betz, 2012:60, see also Hammes, 2009:30, 32) – and thus practical and strategic responses are also fundamentally socio-technical. The contemporary relationship between communication, conflict, and public opinion is one in which the elements are increasingly linked – with public opinion not just seen as a potential limit to military autonomy (as in the 'Vietnam syndrome' narrative), but also as a vital 'terrain' to be contested, a potential 'force multiplier' for actors in conflict, and ultimately a 'battlespace' in which conflicts can be won and lost. Similarly, ICT should not be understood in this context simply as a set of tools – but as creating an 'information environment' which combatants attempt to influence and shape as an integral part of military strategy.

The particular aspects of Web 2.0 technology which produces the challenge of Digital Age conflict are addressed in detail in section 2.3, and the contemporary military approach is examined throughout this thesis. What this introduction demonstrates, however, is the contemporary importance of examining the technology-communication-conflict relationship – in a context where military theorists present it as entailing an increased interest in military communication practices and driving military strategic thought and practical development into areas which are fundamentally *social.* In the course of this research, the implications of this way of thinking are demonstrated: the rise of a form of *population-centric* military intelligence interested in broad social and political discourse and deep psychological insight; the development of a strategic approach to the GWOT conducted by special operations forces in which military activity is deeply imbricated in important areas of social life; and the emergence of a Web 2.0 propaganda apparatus bringing together new forms of intelligence and psychological operations which is increasingly pervasive.

In introducing this context the US military has largely been presented as caught in the currents of changing information flows, a victim of circumstance. However, as the next chapter discusses through the concept of state communication power, state and military actors have historically played a key role in influencing and shaping the communication environment, and continue to do so. This thesis goes on to examine how this role continues today, as Web 2.0 and military activity interact in a dynamic way in Digital Age conflict – offering challenges but also presenting opportunities for new technologies, practices, and relations of communication to be developed.

2. State Communication Power, Propaganda, and the Web 2.0 Information Environment

The focus of this research on US military development in the contemporary media and conflict environment situates it in a body work which studies state and military communication practices as they relate to broader publics. This type of work addresses what I will call *state communication power*, and examines the organisation, processes, technologies, practices, and effects of this power[9]. The use of the term *power,* rather than simply *communication,* distinguishes this type of work from that which studies communication acts or particular forms of communication in isolation (e.g. see Cialdini (2007) on persuasion; Corman *et al* (2013) on narrative), instead addressing the processes which structure communication at a broader level, within it's social and political context. In addressing state communication power this work contends that official control over access to warzones, domestic media law, journalistic norms, economic levers, military practice, and telecommunications policy are as important to understanding mediated state-citizen relations as studying individual communicative acts – requiring that we address these broader areas to understand contemporary communication and conflict.

In addressing the context of Digital Age conflict this thesis presents a situation in which complicated socially- and politically-embedded forms of warfare and new complex networked communication systems combine to produce significant change. New actors are empowered to challenge states' communication practices, new techniques and platforms of communication become important, and new forms of social and political activity have a significant impact on the conduct of conflict. Lianos writes that the "organisation and the nature of power cannot remain immutable and subject to atemporal criteria while sociality transforms itself in a radical way" (Lianos, 2003:418), neither can the analysis of power remain static, and a conception of how it operates must be attuned to the social, technological and political context. With this in mind, this chapter presents a discussion of contemporary state communication power on which the research methodology and analysis is based, drawing on the work of Michel Foucault. It then moves on to discusses how the concept of *propaganda* can guide research in this area. The second half of the chapter then discusses various approaches to the study of state communication power and propaganda, before examining developing work on the challenges of Web 2.0 to that power, and to its analysis. This discussions allows a concept of the *information environment* to be developed as the referent for the study of contemporary military activity, and for this research to be situated in its theoretical and disciplinary context.

2.1. State Communication Power – Foucault, Power and Propaganda

[9] The use of this term should not be taken to imply any claim about the existence of a *particular type* of power (i.e. "communication power", cf. Castells, 2009), rather (as will be discussed in this chapter) it is based on the recognition that the power of communication must be understood more broadly than inhering in particular communicative acts.

2.1.1. Foucault and Power

The discussion of state communication power begins here with an engagement with the theory of Michel Foucault, whose understanding of power as multi-faceted and produced through a network of social relations, structures, and technologies has been particularly useful for those seeking to examine power in the context of Digital Age conflict (see e.g. Reid, 2009; Graham, 2012; Galloway and Thacker, 2007). However this thesis is not interested in an exegesis of Foucault (e.g. see Collier, 2009) - the world is not a code which Foucault cracked. Rather, his thinking, in interrogating contemporary power as a complex, dynamic and socially situated phenomenon provides us with useful concepts to borrow and adapt. As will be shown here (and the methodological discussion which follows in chapter 3), a theory of power drawn from Foucault allows us to proceed in a manner which coheres with thinking about the contemporary information environment and the particular concerns and practices of irregular conflict.

Grounding the approach in a Foucauldian notion of power is a fundamentally *practical* step, one which allows the development of a methodological and theoretical framework suitably adaptable to understand the subject at hand. In the research area, approaches abound which seek to make broad claims about the impact of technology on the nature of power (see e.g. Castells, 2007, 2009; Bramen, 2006) or conflict (see e.g., Verilio, 2000; Der Derian, 2013; De Landa, 1991, Hammond, 2007) in order to present a novel conception of these phenomena. However, they are often based on generalisation through drawing grand conclusions from a necessarily limited engagement with the empirical world (no theorist can study *everything*). Rather than focussing on power or conflict at this meta-level, this thesis focuses on the activities of one distinct actor (the US military) in one distinct area (Digital Age conflict) of techno-social relations. This form of analysis, in allowing us to examine a *particular site* of contemporary state communication power allows us to develop an understanding grounded in experience, and thus engage with the theoretical work in an empirically-informed manner.

For Foucault, power can only be studied, indeed it only exists, in action – it is a social relation rather than an entity in its own right (Foucault, 1994:135), and is produced and reproduced through myriad relationships, activities, and "underpinned by permanent structures" (Foucault, 1994:135)[11]. This conception of power allows a more nuanced understanding than those in which "domination is though to inhere in visible regimes of cruelty or injustice" (Brown, 2006:67), and also displaces the pluralist notion of power being visible only in "situations of conflict between competing … overt preferences" (Lukes, 2005:5). Rather, power is understood as existing throughout all social activity, as both the product and producer of particular social relations. In Foucault's view, power is understood in terms of "its irrigation of the social order as opposed to an image positioning power on top of, visibly stratifying, or forcibly constraining its subject" (Brown, 2006:67). It is productive as well as restrictive: "it incites, it induces, it seduces, it makes easier or more difficult … [only] in the extreme: it constrains of forbids absolutely

[11] This notwithstanding, the terms "powerful" and "power" are often spoken about – including in this thesis – as something which one can be or hold or accumulate. This is a shorthand – with a "powerful" actor being one who is situated advantageously within various power relations. For example, the police officer has power only insofar as they are part of a series of structured political and social relations which reproduce that power, the loss of power when they transgress some boundary ("hand over you badge and gun") or when social conditions structuring these relations break down (revolution) illustrates this well.

… to govern, in this sense, is to structure possible field of action of others" (Focuault, 1994:138). Understood as such, the key to the analysis of any set of relations of power lies in examining the structures, technologies, and practices which make up relations within that particular area.

The analysis of power adopted here is based on an approach which appreciates power's "dispersion, circulation, and microphysical mechanics, its often automatic rather than intentional workings, and its detailed imbrication with knowledge" (Brown, 2006:64), as it works to structure relations in a particular field of action. Thus when examining military communication power we should attend not only to the ideological elements (e.g. statements of policymakers, the content of Psychological Operations broadcasts) or the material ones (e.g. the use of capital to hire PR people, the development of communication technologies) – but also to the *ad hoc* changes taking place on the ground; the development of new concepts which guide practice; the relationship of the military to developing knowledge in the area; and, the many other practices which structure access to, norms and flows of communication. In addition, we should extend our analysis to attend to the dynamic nature of contemporary military practice, addressing the *processes* of communication as well as its content, and the *collection* of information as much as its dissemination.

This understanding of power coheres with our understanding of the online communication environment – as discussed in section 2.4, flows of information in Web 2.0 are not hospitable to linear understandings of communication cause and effect associated with the rhetorician or the advertising campaign. Successful communicators must take account of and operate through influencing flows of convergent information and cultivate influence and credibility within networks of social media communication rather than simply broadcast well-written messages. In this respect, Boyer has noted that "Foucault was already thinking at the level of networks" (Boyer, 2011:96) – taking into account the complexities of process and the multiplicity of nodes of power. Indeed, while much technological utopian thinking about networks suggest that their non-hierarchical nature means power in the Internet communication environment is constantly up for grabs, Galloway and Thacker argue that the rise of the network form "in no way implies an absence of power relations. In fact, it prescribes them" (Galloway and Thacker, 2007:7). As such, a concept of power which suggests we pay heed to these structural or spatial aspects is vital. Recognition of this is found in many of the military developments studied in this thesis – from the cultivation of Facebook audiences as both recipients and conduits of military PSYOPS material, to significant funding for academic research on memes and viral communication.

The latter example suggests an important link between power and knowledge, a key and influential element of Foucault's theory (which he calls *knowledge/power,* Foucault, 1980, see also Mehta and Darrier, 1998:111; Hall, 2001:74-75). Work based on the link between knowledge and power has been influential in social science and cultural studies since Foucault, sometimes leading to extremes of interpretation in certain post-structuralist work in which critique, politics and knowledge seem to become no more than a matter of 'discourse' (for criticism see e.g. Lukes, 2005:492; Philo and Miller, 2000; cf. Finlayson, 2001). The understanding of the links between knowledge and power presented in this paper is a more practical one: neither knowledge nor power exist in a vacuum, knowledge

is put to work in certain structures and strategies of power, and in turn has an impact on how power relations develop (Hall, 2001:76). As such, we can see state communication power as working through not just individual ideological statements, but in many forms: through using knowledge about others ('intelligence') to guide strategies; through disciplining and limiting the range of public debate (such as the UK government's refusal to "comment on intelligence matters" (Turk, 2014)); the promotion of certain forms of knowledge over others (such as the instrumentalization of Communication Studies to assist military propaganda in post WWII American academia (Simpson, 1996)); the shaping of the language and norms of public debate to favour particular viewpoints (e.g. see Halliday, 2010) or privilege specific forms of argumentative proof (Massumi, 2005:10); and the enclosure of issues within particular governmental logics rendering them amenable to specific types of state intervention (of which the 'securitization' school of International Relations is a key example, see e.g. Williams, 2003).

Recognising the strong link between knowledge and power in this way allows us to extend the analysis of military communication beyond the realm of the ideologue – to one in which power is reproduced through the work of everyone from the editor, to the statistician (Weizman, 2011), to the latest technological guru (e.g. see Robins and Webster, 1999:141; Lawson, 2009). Indeed, the research presented here demonstrates that when military actors are considering information and communication strategy, the futurists, technologists, statisticians, and social network analysts occupy many more seats around the table than the ideologues (e.g. see Bolier, 2003; Collings and Rohozinski, 2009).

This understanding of power based on Foucault will be further developed in the methodology chapter, where we will see that as well as offering us a hammer to smash power into little pieces, his theory gives us a guide to studying those pieces coherently as they apply to a particular *problem field,* that of Digital Age conflict. It also gives us some conceptual glue to assemble the fragments and study them as a propaganda *apparatus* which structures power relations in this field. In the military context, the term "intelligence" directly refers to knowledge instrumentalised for war (Horn, 2003:4) – perhaps the supreme example of power/knowledge. As well as paying significant attention to changing intelligence practice, this thesis draws attention to the implications of the privileging of certain approaches to information gathering and processing such as social network analysis and identification of forms of influence; the implication of the insinuation of military-produced information into broader news ecologies; and the key links between the military and developing academic knowledge in computing and ICT. All of which underline the important links between knowledge and state communication power.

2.1.2. Power, Publics and Populations

In studies of power which draw on Foucault, the role of the state is often an ambiguous one. Brown notes that "if power operates through norms, and not only through law and force, and if norms are borne by words, images and the built environment then popular discourses, market interpellations, and spatial organization are as much a vehicle for power as are troops, bosses, prime ministers, and police" (Brown, 2006:66). This thesis takes this to be the case. However, it asserts that in the context of conflict the power of the later (troops and prime ministers) over the former (words and space) is an element which

has historically been very significant and continues to be so. This is a result of military actors' structural position within systems of legitimacy and authority (i.e. as primary sources of information about conflict), as well as their 'objective capacities' (Foucault, 1994:135) such as huge training and R&D budgets and employment of communication professionals – not to mention their central role in the application of violence itself.

The adoption of Foucault within the research context must be understood not as power-without-the-powerful, but as a way of addressing and understanding complex power relations as they structure a given field. The state and military apparatuses of a society do not hold power *per se,* but through historical contingency and constant effort to protect the structures and practices which reproduce that power. This research, in examining the state reaction to changing socio-technological context, takes this recognition as the foundation of analysis. Given the huge efforts government and military actors undertake to protect their communication advantage, it is evident that they see this power as contingent too.

However, if state communication power is a shorthand for power which inheres in relationships, we must address the question of *who* these relationships are with. An interest in the public as the addressee of state communication power is at the foundation of both the sociology of communication as an academic pursuit, and the development of the fields of public relations and modern propaganda (see e.g. Lippmann, 2008[1922]; Lasswell, 1927). This work is grounded in the development of "mass society" theory in America, which developed in response to the emergence of a mass, urban, educated population which was, through the development of information technology (the radio, telegraph, and modern printing press) able to communicate and access information as never before (see Qualter, 1985:ix). The influential theorist Walter Lippmann wrote, typically of the concerns at the time, that the emergence of such a mass threatened the breakdown of social order through the increased capacity of mass communication to connect publics to national and global politics. For Lippmann, democratic ideology would lead the public to suppose that they should be involved and political decision making and the extent of this involvement, which had previously been limited by lack of literacy or access to political information, posed serious challenges to the status quo (Lippmann, 2008[1922]) [12].

In response to this challenge Lippmann's contemporaries Edward Bernays and Harold Lasswell (key figures in the development of public relations and academic communication research respectively) asserted the necessity for new forms of elite communication practice (PR and Propaganda – the former invented as a euphemism for the later) to manage this new restive mass. Lasswell wrote that "in a world in which 'impersonality has supplanted personal loyalty to leaders" and 'literacy and the physical channels of communication have quickened the connection between those who rule and the ruled … most of that which formerly was done by violence and intimidation must now be done by argument and persuasion" (Lasswell, 1927 in Robins et al, 1987:2). The necessity of the use of propaganda was asserted in order to control "the mass", seen to possess a new and dangerous "wilfulness", they must be "seduced" by an enlightened elite (Lasswell, 1927 in Robins et al, 1987:2-3). Thus, the dawn of mass democratic participation based on mass

[12] Lippmann's legacy is contested, interpreted variously as one of elitism or one of deep concern with democratic representation, see Curry Jansen (2008).

communication was met by the rise of theoretical and practical attempts to manipulate this mass public in order to protect the autonomy of the states and elites and suppress social antagonism (see Miller and Dinan, 2008).

Lippmann was right about democratic ideology and the value of public opinion, and Qualter notes that "the legitimacy of public opinion led inevitably to the development of techniques to manipulate it" (Qualter, 1985:6). He argues that prior to the modern age "it did not really matter what people thought. No machinery existed through which any public opinion could be aggregated or articulated, or in any formal way be brought to bear on policy" (Qualter, 1985:5). This situation is turned on its head in the contemporary world of polls, surveys and petitions, and of mass democratic experience of politics based on publicity and spin (Corner, 2007). Whether it is listened to or not, the *notion* of public opinion is now central to political discourse (see e.g. Jacobson, 2008:360; Hanson, 2008:111; Slaughter, 2009). One of the key questions then, in studying state communication power, is how it produces and structure the relationships of influence between states and publics. States generally, and militaries engaged in conflict in particular, have the essentially bureaucratic concern of self-legitimation and the reproduction of the basis of their power (Brown, 2006:79). In this regard, Habermas has argued that the very idea of "the public" was "called into form by the instrumentalization of the press by early modern states in the effort to solidify governance" (Boyer, 2011:89). Thus we can conceive of the public as not simply something to be ameliorated or manipulated by the state, but something internal to the processes of contemporary state power in the contemporary age of mass democratic participation and publicity. The "public" is the addressee of state communication power, its medium (as power is reproduced through social relations), and the state's "legitimating fiction" (Boyer, 2011:89).

This is particularly important in a situation which sees the concerns of the mass society theorists writ large: with the informed, connected, and vocal masses now operating at a *global* level empowered by Web 2.0 ICTs. Here the 'wilfulness' of the Arab Spring is understood as the harbinger of this new age (see e.g. Cottle, 2011, Wallin, 2012; Seib, 2012). Taking this element of state communication power into account leads us to an appreciation of the ways in which public opinion is bypassed (e.g. through lobbying, Miller and Dinan, 2009), contested (through PR campaigns, political rhetoric, or military information operations), and instrumentalized (engaged with to sustain political legitimacy, seen as key in judging the progress of war in terms of both popular support at home and "hearts and minds" abroad). The relations between militaries and publics have particular resonance in Digital Age conflict – where military strategy is often referred to as "population-centric". While one must be wary of making theoretical hay from the fertility of military linguistic novelty, this evokes the Foucauldian idea of *population,* a key concept in understanding the operation and implications of particular regimes of power.

For Foucault, the concept of population does not just refer to a mass of individuals within a particular area, but specifically to *how* groups of individuals are brought together and coherently addressed within particular strategies of power (see Foucault, 2007:37,45,108; 1994:245, see also Kapferer, 2010:128). From the view of power, populations can be seen as pools of potential opinion, actions, and knowledge which can be accumulated, analysed, and acted upon in the abstract (Foucault, 2007:37;45) – seen for example in the statistical

management of crime rates or unemployment, as well as the legitimacy granted to (and imparted by) opinion polls. This affects the way being conceived of as part of a particular population has an impact on individuals subject to that power – for example in the data about individuals that the powerful deem important to guide strategy, or the different forms of activity deemed reasonable in interaction with that population. At the most violent end of the GWOT spectrum, we can see how particular military strategy conceives of certain populations - in warzones such as Afghanistan, Yemen and Pakistan - in terms of how their activities look from the viewpoint of a drone or other persistent surveillance – as "signature strikes" target alleged insurgents with missiles based not on specific intelligence, but on a general assessment of their movements via aerial surveillance[13] (Rhode, 2012).

At a more subtle but pervasive level, we can see how being conceived as part of the "human terrain" in a counterinsurgency strategy has serious effects on how populations are related to by military power: variously "lived amongst", targeted for action from intelligence collection to PSYOPS to violence, and "contested" by militaries and insurgents. It is clear then, that *how* strategies of government conceive a population is significant to the outcomes for those included within this conception (Dillon and Lobo-Guerrero, 2008:267, see also Reid, 2009). Throughout this thesis, the understanding of the implications for the subjects of military communication and intelligence practices is guided by the assessment of how military approaches address them in terms of particular attributes, activities, and interests - often with stark consequences in terms of the invasiveness of military activity and the potential outcomes in both the communicative and physical realms.

2.1.3. Propaganda and the Politics of Information

Propaganda is a controversial term which cannot be avoided when discussing state communication power. However, it must be thoroughly examined and unpacked before it can be used with any precision. It is a concept which carries significant ethical and ontological baggage: it is associated with totalitarian regimes, 'dirty tricks', lies, censorship, and is most commonly used to dismiss any communication of a form or content with which the respondent happens to disagree. US military public affairs doctrine emphasises that the Department of Defense (DOD) does not do "propaganda", which it defines as "*any form of adversary communication*, especially of a biased or misleading nature, designed to influence opinions, emotions, or attitudes, or behavior of any group in order to benefit the sponsor" (US DOD – *JP 3-61,* 2010:I-2, emphasis added). It is a term, then, which is used to discredit opponents, often used imprecisely and relates more to the viewpoint of the user of the term than the features of the communication to which they refer. It is also possible to think of 'good' propaganda such as public health or safety campaigns (O'Shaughnessy, 2004:15), further demonstrating the confusion that applying ethical or agent-based definition to the term. As such, many propaganda theorists have stated the importance of dispensing with the notion that the term carries any normative

[13] That is, in the regions most directly affected by the GWOT the population is addressed (both conceptually and literally) as one in which moving across the terrain in a manner an insurgent might do (say, travelling in a pick up truck with fighting-aged men) can make a life-or-death difference in how military power addresses you.

or ethical judgement *a priori* (see e.g. O'Shaughnessy, 2004; Taylor, 1995; Ellul, 1974) – an approach which is adopted here.

For many researchers, having dispensed with ethical criteria, propaganda instead becomes a matter of the *intention* of the communicator (see O'Shaughnessy, 2004:1-18, and Jowett and O'Donnel, 2006:3-16 for a discussion of various definitions) – involving the *instrumental* use of communication or information by one party to influence the opinions or behaviours of another[14]. Beyond this, various instrumental uses of communication have been studied – including those which attempt to define propaganda in relation to matters of content or form, relying on judgements regarding the truth value of messages, the use of rhetorical tropes, and the relationship to reason (e.g. O'Shaughnessy, 2004:4). However, this is a superficial way to examine propaganda, obscuring the key point of its instrumentality: all elements of the content and form of propaganda are judged by the propagandist on the basis of their utility to the purposes of persuasion. In a common sense understanding, propaganda *can* be based on lies or emotional manipulation, but most messages are not so crude, as to be caught lying diminishes the credibility of the speaker and thus the effectiveness of further communication (see e.g. Kinniburgh and Denning, 2006:9; DOD – *JP 3-13.2,* 2011:II-11). Furthermore, a conception of propaganda based on *content* or *form* fails to capture perhaps the key concern of the PR practitioner or military public affairs specialist – that information likely to undermine the official viewpoint never gets out. Censorship, both formal and informal, is a key element of any system of propaganda.

Already in recognising the complexity of intentionality we can see elements of legitimacy, consistency, and authority joining those of form and content as potential aspects of propaganda. Furthermore, in producing effective communication campaigns, it is important to note that propagandists require access to information about audiences (what the military calls "target audience analysis", e.g. US Joint Warfighter Command, 2010), an understanding of the process of communication and the dynamics of particular platforms (such as research on viral communication (see page 178)), and intelligence as to the likely effect communication will have on the broad information or conflict environment. As such, propaganda is understood in this thesis as a broader social practice, in which structures of access to information, different communication practices, and the link of power to knowledge play a much more significant role than the content of any individual message.

As such, propaganda is understood, following Robins, Webster and Pickering, as a "matter of the politics of information" (Robins et al*,* 1987:8). This conception situates the analysis beyond any simple study of content. Instead it allows for the analysis of propaganda as a systematic feature of contemporary society working through all areas where communication and information have impact on social and political experience (Robins and Webster, 1999:134).

Robins and Webster argue that the study of propaganda can best proceed by attending to the "panoply of industries and apparatuses" that act to produce state communication power in a particular situation – a system of elements, from the "intuitions of active persuasion" such as PR companies and spin doctors, to systems of censorship,

[14] Ultimately, behaviour is the key goal as opinions themselves do not alter the world – Ellul sees propaganda's aim as the creation of *orthopraxy* rather than ortho*doxy* (Ellul, 1973:27).

surveillance, and the commercialisation of information (Robins and Webster, 1999:141). As we have seen in relation to the development of counterinsurgency and population-centric conflict, and will be further demonstrated in throughout this thesis, in a situation where terms such as "hearts and minds" and "psychological operations" are central to military activity, propaganda is not an additional or peripheral element of conflict concerned only with its representation. Rather, it is a "a *constitutive* aspect" (Robins et al, 1987:8) of conflict, and of broader social experience (see also O'Shaughnessy, 2004:142; Sussman, 2012, cf, Corner, 2007). As such, we develop an understanding beyond propaganda conceived as a matter of content or form – it is understood as a system which structures power relations in a particular situation.

Conceiving propaganda in these broad terms allows us to proceed based on the concept of power developed in this chapter. It provides a way of conceiving the operation of state communication power in a particular field of social activity. This research adopts the Foucauldian concept of an *apparatus* as a way of understanding the multiple structures, technologies, practices, and organisations that structure power relations in a particular field. The concept – fully outlined in section 3.1 – offers a means of describing and understanding the range of elements of "the politics of information" as they apply to the particular *problem field* I have outlined as Digital Age conflict – and thus allows us to examine the range of diffuse military activity in a coherent way as a *propaganda apparatus.* In adopting a broad notion of propaganda which compliments the Foucauldian conception of power, the study develops deep insight by producing a *broad study* of a multiplicity of practices within a relatively *narrow area.*

In taking a holistic view we come to understand, for example, how the censor (who controls what information remains outside of the public domain) or the surveillor (either the monitor of public opinion or the analyst of target audiences) play as important a role in the instrumentalization of information by powerful actors as does the spokesperson or the corporate flak. Jansen notes that the word 'censor' derives from the Latin title for the job which entailed both 'censorship' and 'taking of censuses' such that as a single concept it can be understood as "a mechanism for gathering intelligence that the powerful can use to tighten control over people or ideas that threaten or disrupt established social order" (Jansen, 1988:14). The links between surveillance and public communication, between intelligence and psychological operations studied in the later chapters of this thesis demonstrate that this link between these various aspects of state information work - that is, between elements of a propaganda apparatus - is not just a historical curiosity.

2.2. Manufacturing Consent: the Critical and the Practical Approach

Due to the contemporary nature of the area of analysis, studies of relevance to this thesis - dealing with various aspects of Web 2.0 and conflict - are drawn into the discussion and analysis throughout the paper, and come from disciplines including geography (e.g. Graham, 2010), war studies (e.g. Rid, 2007), and sociology (Bakir, 2010). However, the work which has historically been most strongly identified with the study of propaganda and the communication of states in conflict are the areas of critical communication studies and practitioner-based analyses of military communication. This section examines this

work before moving on to discuss studies which outline the challenge of Web 2.0 to our understanding of state communication power, and then introducing the concept of the *information environment* as the referent for understanding military communication activity in this thesis.

2.2.1. Critical Communication Studies

In addressing state communication power the area of critical communication studies has been influential in investigating the ways in which states have utilised public communication during conflict. The focus on *critical* communication – meaning studies which focus on the activities of powerful state or corporate actors within Western media systems and interrogate their activities, generally approaching state communication power from a hegemonic perspective (see e.g. Herman and Chomsky, 1988; Philo and Berry, 2004) – is important here. In focussing on the role of state actors in conflict, critical communication studies takes the view that their *communication* power must be seen in the context of their general monopoly on other forms of power (violence, economic, political, etc.) in conflict. Thus the approach to the study of propaganda is not one of pluralism or competing interests (cf. Patrick and Thrall, 2007), but of substantial structures and networks of power acting in a coherent way over a field, examining the broader structural factors and long-term practices and relationships which allow powerful actors to use media platforms to their advantage.

A very influential text in the field of critical communication studies is the work of Herman and Chomsky (1988 [1994]), whose "propaganda model" offers a powerful tool for examining how state and capitalist power works to systematically influence mass media content. The work demonstrates how an analysis of power understood as working through a variety of "filters" to shape mass media production can convincingly predict structural outcomes in terms of media content through an analysis based on a systemic notion of communication power. The model aims to explain the content of mainstream media news, outlining how the events and opinions that exist in the world – of which all mediation is necessarily selective - pass through a number of 'filters' in this selection process, such that the ultimate output of mass media presents a view of the world which is broadly sympathetic to powerful interests. In the model, elite power over the media works through the various filters, including: ownership of the press (the interests of owners are reflected in content); flak (by which powerful interests can have a disciplining effect on the media through phenomena such as lobbying, campaigning or *de facto* financial sanction); and through "dominant ideology", in which values of the powerful, and news culture more generally, are internalised by journalists or editors and reflected in the content they produce .

Herman and Chomsky's study examined coverage of the US wars in South East Asia and Central America in the 1970s and 1980s, and demonstrated that the filters allowed the powerful to "fix frames of reference and agendas, and to exclude inconvenient facts from public inspection" (Herman and Chomsky, 1994:xiv). The propaganda model has since proved effective in studying many of the effects of state and elite power on mass media content, particularly during times of conflict (see e.g. Klaehn and Mullen, 2010). However as mass media content *per se* is not the focus of this research we can also look at broader utility of the approach. This lies in the fact that the model represents state power as

operating in a variety of ways through particular filters to influence mediation - the point where all of the events and opinions in the world are chosen from and presented as a highly selective subset of information we call "news". Analysing state communication power in this way allows us to develop an understanding of how a multiplicity of practices, constraints, structures, and actors come together in a systematic way to produce relatively coherent outcomes over a field – the mass media – through which power relations are reproduced.

The influence of the propaganda model theory can be seen directly in a number of critical communication studies which attend to the analysis of particular filters within the field of mass communication, or else allows us to understand studies of particular "filters" which we can situate within a broader understanding of state or capitalist power as acting in a coherent way across that field[15]. These have shown how various factors in news production effect media content: works from journalists and academics about the constraints of military media management (see, e.g. Thomson, 1992; Maltby, 2012) have given an insider view of the effects these practices have on news reporting; others have outlined how constraints of time and resources have led to a number of practices – such as reliance on PR copy or official comment (Davies, 2008) – which have an impact on the content of mainstream news. Media scholars have explored how production values, the systematic privileging of official sources (Philo and Berry, 2004), and a dominant culture of liberal-institutionalism amongst journalists which favours a particular interpretation of "objectivity" (Edwards and Cromwell, 2005) make up other filters which impact how news is interpreted and presented by journalists.

A much more direct form of influence which powerful groups can have on public information is explored in another area of critical communication research. The rise of the practice of public relations (PR) to become a sophisticated and pervasive global industry (Ewen, 1998; Miller and Dinan, 2008) has been shown to produce significant impact in the mass media. At the extreme, such studies have shown how PR companies have worked for governments in producing fake news stories to justify war – with the infamous claim that Iraqi troops were dumping babies from incubators onto the floor of a Kuwaiti hospital, spun by PR firm Hill & Knowlton (Rampton and Stauber, 2003:69), echoing the classic atrocity propaganda of the "barbaric Huns" of the first world war (Wilson, 1979). In this case, studies move beyond the role of "filtering" to examine additional *inputs* to the mass media system – a key area of interest when we consider the Web 2.0 communication environment is one characterised as an 'attention economy', where the active promotion of information becomes an important factor beyond the 'filters' of mediation.

Evidence points towards an increasing convergence of military, PR, government and mass media in the contemporary age, for example: through the blurring of the lines between news and public relations output (see Miller and Dinan: 2009); the employment of a PR firm by the US military to run fake news stories in Iraqi newspapers (Bamford, 2005); the US State Department campaign, conceived by an advertising industry veteran and run by a PR company, to 'sell' America to the Muslim world after 9/11 (Plaisance, 2005); and the elevation of 'spin' to the *sine qua non* of domestic party politics (Corner, 2007). Thus an

[15] Which is to say, not all the studies referenced here are explicitly based on the propaganda model, but in attending to particular 'filters' they can inform a view of the elite-media relationship based on an understanding derived from the model.

understanding of the active and pervasive role which professional communicators play in shaping mass media content has become a key element in understanding state communication power. As we turn our attention in this research to the world of Web 2.0 – our understanding of how these activities have an impact on *mass* media provides context for assessing their impact in the *new* media environment.

These studies demonstrate the utility of an approach to the analysis of state communication power based on an understanding of the multiplicity of ways that power works through media systems. When we take account of all the ways in which state power can exert influence through communication in times of conflict, it becomes clear that propaganda must be understood as a complex process: evidenced in everything from the subtle self-censorship of the ownership-shy journalist to the most egregious falsehood promoted by PR specialists. Thus, the understanding of state communication power and propaganda does not lie in unmasking some form of elite conspiracy, or the ability to micro-manage public opinion, but in investigating how the outcome of a vast array of power relations (from that between owner and editor, to that between rhetorician and their public) and structural factors (those of financial viability, ability to hire PR specialists, or of authority within a particular discourse) lead to a situation in which communication works, broadly, to support and reproduce power relations in a particular field.

2.2.2. A Lesson From the Professionals - Military and Policy Approaches to Propaganda

In the context of contemporary conflict, state communication power has generally been studied through two relationships: that between Western military power and domestic publics, and that with publics in the conflict zone. The later form of communication has largely remained outside the realm of critical media studies, likely due to the fact that the major relationship between Western nations and those in conflict zones is mediated not by mainstream news, but by the bomb and the bullet. However, there *are* studies in the area of military communication practice which add to our understanding of communication power during conflict. The type of work which analyses military and state communication power in detail is, most frequently, that written from the perspective of state power. For example, we find works on communication in warzones written by Information Operations practitioners (e.g. Armistead, 2004; 2007); work on military-media communication by military spokespeople (Tatham, 2006) or military-linked academics (Rid, 2007; Taylor, 1999)[16]; and studies of changing diplomatic practice from the perspective of the preservation of a Western foreign policy elite (Slaughter, 2011; Potter, 2002).

There are a small number of studies which examine the area of military communication from the outside (e.g. Brown, 2003; Miller, 2003; Pamment, 2012; Brunner and Dunn Cavelty, 2009) but in general those authors working from state institutions are most able to offer insight as they do not face the significant problems of access that an outsider does.

[16] Rid works in the War Studies department and King's College London, a key intellectual hub for British and American military thinking. Taylor was a visiting professor at the UK Defence Academy (the hub of UK MOD further education and doctrine development).

This proximity to power does not diminish the utility of the work for understanding the processes of state power, in fact once situated within a broader understanding of communication power, work by these institutional authors provides key insight for the research presented in this thesis (it made up most of the on understanding the problem field of Digital Age conflict). Consideration of this work also allows us to add an understanding of the process of state communication power from the perspective of the practitioners or institutions involved.

A more general point which we can take from this body of work, however, is the key understanding it gives us of the way state communication practices develop in the context of social, political and technological change. Taylor, for example, examines how British military communication practices developed throughout the twentieth century in response to new developments in technology and warfare (Taylor, 1999) as well as social factors such as the changing role of "elite" and "mass" opinion in democratic theory (Taylor, 1999:35-58), different paradigms of the role of the media in wartime (Taylor, 1999:151), and of the development of public relations (Taylor, 1999:243). Other work in this area has produced insight through focussing on more discrete elements of communication in warfare: Macdonald for example studies how images have been used in government and military communication campaigns, showing the driving force of new techniques and technologies in producing new strategies (Macdonald, 2007, see also Winkler and Dauber, 2014); in another area Tatham has focuses on the role of Arab satellite TV channels in military communication practice (Tatham, 2006), and the work of Rid and Hecker (2009) has been influential for this thesis in describing the research context of 'Digital Age conflict'.

This form of analysis, which examines state communication practice as a process of adaptive development driven by changes in social norms, technology, and warfare offers key insight. I draw on this work at length in examining how the changing strategic and technological contexts of the GWOT and Web 2.0 have been understood by both academic and institutional actors – providing insight into the social and technological context of military communication practices. Such insider-analyses also draw our attention to the more mundane, if equally important, element in studying state communication practice of looking at the institutional "enablers and obstacles" to changing practices (Rid, 2007:8). They outline the importance of paying attention to the bureaucratic context of change as well as the social: for example approaches to US diplomatic communication can be seen as influenced by the ideological viewpoint of those running the State Department (Lord, 2006); and approaches to military-media relations are influenced by the changing historical experience of officers (Rid, 2007:9-10). Thus we take from more state-centric analyses two key additions to our understanding of state communication power: the bureaucratic element in understanding how communication practices develop; and the importance of technological and social context in driving these practices.

Military-linked studies provide vital data for this research as they provide key insider context on military developments often inaccessible to the outsider. They are also often blunt in their description of the instrumental role of communication, seeing no need to sugar-coat that the fact that they are involved in "psychological operations" or a "war of ideas" (Waller, 2007). Studies of military communications practices from the outside have, in contrast, sometimes suffered from starting from a more neutral or theoretically naïve

point of view. For example, Maltby's in-depth study of UK military-media communications practices finds that military "media operations is actually a form of impression management performed in interaction with media organizations in an attempt to influence the definition others will come to formulate of military activities" (Maltby, 2012:39). Similarly, Li's analysis finds that a computer game produced by the US military as a recruitment tool called *America's Army* is not a good example of the Habermasian ideal type public sphere (Li, 2004). Elsewhere, Carr's analysis diagnoses a contradiction between US State Department policy on promoting both "Internet Freedom" in Iran and the propaganda value of tweeting in Farsi (2013:633), however this gap between the rhetoric of US foreign policy and the reality is surely a political issue rather than a matter of acadamic insight, showing the dangers of taking policy itself as an analytical basis. In these cases, adopting some of the honest cynicism of military-based analysts – understanding from the outset that when the military uses its resources that it is likely for some instrumental purpose (see e.g. Miller and Sabir, 2012) – saves a lot of time and allows the analysis to proceed from a more advanced position.

There is clearly a disciplinary distinction to be made between the tradition of critical communication studies and that of state-centric and insider accounts of state communication power. The former is critical of power and deeply concerned with its social impact; the later critical only, usually, in the sense that it is concerned with the *effectiveness* of conflict communication, and is more concerned with the impact of society on the practices of powerful actors than vice versa. However in a world where the distinction between conflict communication and more general public communication are rapidly converging a consideration of both areas helps build an understanding of the complexities of contemporary state communication power.

Both bodies of work also demonstrate the importance of attending to the social and technological context of communication, and the currently rapidly changing context is the catalyst for the research presented here. This shifting context gives rise to a situation where we must look beyond the focus of critical communication studies on "mass media", and build on the insight gained from examining changing contexts and practices found in institutional analyses. The following section examines work which has addressed the role of Web 2.0 in the context of Digital Age conflict. This chapter then concludes by introducing an approach which replaces the focus on "mass" media with one which examines impact on the "information environment" – and bridges the gap between critical and institutional studies by examining military and new media practice in an integrated and dynamic way.

2.3. New Media Disruption – Web 2.0 Challenges to State Communication Power and its Analysis

A substantial literature has developed in the last decade addressing the changing nature of public communication due to the rise of Web 2.0. In exploring key areas of interest, conceptual development, and antagonism in relation to Web 2.0 and state communication power, this section presents a context in which both military activity *and its analysis* are challenged by a new socio-technical context. This section develops the concept of the

information environment as the theoretical focal point for the research, as well as engaging with work from military and government elites and associated writers which allows us to explore how *they* view the 'problem field' of Digital Age conflict as a vital first step in examining military development and practice in this area. As we will see, there is often little to separate military thought (and even military *doctrine*) and cutting-edge academia in this area – highlighting it as a key area of military activity, and a vital area in the analysis of contemporary state communication power.

This section draws on discussion of the challenges of new ICTs by authors engaging with the issues from a range of perspectives: those which seek to enhance or protect state power (e.g. Gowing, 2009); which try to dispassionately examine new challenges (e.g. Hoskins and O'Loughlin, 2010); and which explore alternative 'counter-hegemonic' possibilities enabled by new ICTs (e.g. Bakir, 2010). 'Web 2.0' (a term coined by O'Reilly, 2005) is the common referent for these works, and is a concept which describes the proliferation of connective and recording technology such as smartphones and tablets; accessibility of publishing through the Web via blogs; broadened access to information through free news and reference platforms; and growing network forms such as P2P file sharing and VOIP programmes. These elements move beyond the old media (and 'Web 1.0') world of "few content producers and many, relatively passive, content receivers or consumers" (Anderson, 2003, in Bakir, 2010:2), to a new situation of "mass self-communication" (Castells, 2009:55). In popular usage Web 2.0 is generally synonymous with terms such as "new media" and "social media" – where platforms like YouTube, Facebook, Twitter, The Pirate Bay, Flickr, and others have produced new ways of broadcasting content, sharing media, forming social relationships, and accessing news about the world. Cumulatively, they have profound effects on the way individuals engage with information in the public domain. As this section demonstrates, the effect on state and military communicators is similarly profound.

2.3.1. "Information Doers" as New Media Insurgents

The most striking feature of the Web 2.0 information environment is that, in providing cheap access to publishing platforms (blogs, Twitter, Flickr, YouTube, etc.) and cheap forms of content production (smartphones), the number of people who can publish information for the world to access relatively freely is hugely multiplied from the pre-Web (and even pre-Web 2.0) era. Gowing, a key establishment thinker[17], describes the challenge of Web 2.0 to elites as driven by "a fast proliferating and almost ubiquitous breed of 'information doers'... [who], empowered by current, cheap, lightweight, 'go anywhere' technologies … have an unprecedented mass ability to bear witness" (Gowing, 2009:1). He sees this group as leading a "wave of democratisation and empowerment that shifts and redefines the nature of power in crisis" (Gowing, 2009:9-10). Echoing earlier

[17] Nik Gowing, a BBC journalist, wrote the influential *Black Swans and a 'Skyful Of Lies'* (Gowing, 2009) with a view to advising key government and military actors on maintaining their advantage in the changing communication environment. It has been influential in communication policy circles – being mentioned as a key text at Information Operations Global 2012, promoted by the head of the British Army (Richards, 2010), and appearing on the reading list of the UK Government's Stabilisation Unit (a group focussing on international development and counterinsurgency, Stabilisation Unit, 2012). It also synthesises a number of concerns outlined elsewhere by state and military communicators (see e.g. Mullen, 2009; Glassman, 2008; Murphy, 2009).

mass society theorists, Gowing sees this challenge as threatening "the processes of democratic governance" (Gowing, 2009:9), although it is clear from his analysis that what is really threatened is the existing practices of Western government and military elites rather than democracy itself. Another analyst writes, more frankly, that new ICTs mean that "the hegemonic group is unable to use the organs of the State for coercion" (Fisher, 2003:4) as effectively, underlining the structural challenge new technologies represent.

'Information doers' rely on Web 2.0 platforms which enable access to the information environment for an expanded range of actors - what Manuel Castells calls the age of "mass self-communication" (Castells, 2009:55). Even in Web 1.0, publishing (especially to any significant audience) was largely monopolised by large media companies who could afford web designers, servers and domain names. Web 2.0 offers free, easy publishing to anyone with an internet connection through sites like WordPress, Tumblr and Twitter. While hierarchies of audience and authority undoubtedly remain in Web 2.0 (Auer, 2011), and the 'big content' producers still hold significant power (Hindman, 2010), the environment is much more open to impact from amateurs, especially where content is produced which resonates with a significant audience – "going viral" due to the quality of the content or the inherent interest of (usually visual) media captured of a newsworthy event.

We can think of the array of camera-phones held aloft recording significant events, or the dispersed individuals who record or publish vital information about a news event - such as the Twitter user who drew attention to the US special forces helicopter going to assassinate Osama Bin Laden in Abottabad (Anand, 2011), the banker who caught the deadly assault by a police officer on a member of the public at the G20 in London on camera (Ward, 2012), or the legion of citizen journalists documenting vital events such as the protests of the Arab Spring and the Syrian civil war (e.g. see Lynch et al, 2014) - as particularly influential 'information doers'. There is also a secondary layer of Web 2.0 "doers" focussed on analysis, seen in the expanded array of commentators, analysts, and opinion shapers that new media produces, challenging mainstream media's influence of opinion formation. For example, the influential Foreign Policy magazine list of "top 100 twitterati" includes key figures from the political and military establishment, alongside bloggers, and theorists (Foreign Policy, 2012). A US military report into ICTs notes that the access to influence online is "now constrained primarily by imagination and tenacity, rather than access to communications technology or financial assets" (DSB, 2008:401), which doctrine notes gives many more actors the "ability to share information in near real time, anonymously and/or securely" (DOD - *JP 3-13,* 2012:1-1, see also US Army TRADOC - *Pamphlet 525-7-8,* 2010:10).

The increased ability of information doers to have an impact at the level of international relations and warfare has been the subject of concern of a number of influential theorists. Arquilla and Ronfeldt, for example, see it driving "a new epoch – and spectrum – of conflict" in which super-empowered nonstate actors can take on state power (Arquilla and Ronfeldt, 1997:1). Similarly, the US policy advisor Anne-Marie Slaughter has suggested that '"super-empowered individuals" can have such an impact through networked forms of sociality that they can "do things that [previously] only states could do" (Slaughter in Null, 2011, see also Dunn Cavelty and Brunner, 2007:8). These observations show concern at the power of specific new actors who are able to challenge state communication power at the institutional level – often conflating access to broadcasting tools with deeper levels

of influence and impact. US doctrine talks of adversaries using "the commercial marketplaces as their combat developer" (US Army TRADOC (2010), *Pamphlet 525-7-8,* 11) in using Web 2.0 ICTs to access mass audiences. It is clear that the example of Osama Bin Laden releasing his videos online to back up his propaganda of the deed casts a long shadow over the thought of state thinkers in this area: with Richard Hollbrooke famously asking how a "guy in a cave outcommunicate[d] the world's leading communication society" (Hollbrooke, 2001), haunting those concerned with strategic thinking in Digital Age conflict.

However in the long term, the more diffuse examples of data which emerges from a *long tail* of 'information doers' rather than 'super-empowered' ones seems to characterise Web 2.0 more distinctly. It is not Al Qaeda's videos which haunt US strategists, but the possibility of attack. On the other hand, information doers change the strategic environment making it less predictable. Where everyone "from traditional nation-states to noncombatants, transnational corporations, criminal organizations, terrorists, hacker unions, mischievous hackers, and the unwitting individual who intends no malice … combine to *create a condition of perpetual turbulence*" through their access to recording and broadcasting technology, there is a true shift in strategic thought and military planning, with doctrine even referring to any of these creators of "turbulence" (including the "unwitting individual") as "adversar[ies]" due to the seriousness of the threat this unpredictability poses (US Army TRADOC -*Pamphlet 525-7-8,* 2010:iii). In this sense, it is *Black Hawk Down* and Abu Ghraib-type data undermining US military strategy rather than super-empowered users which really haunts decision-makers.

Prominent new information actors such as WikiLeaks or the new media presence of non-state actors like Al-Shabaab or the Taliban (Alonso, 2012) have pre-Web 2.0 precedents. For "groups who relied on (and therefore understood) the mass media to propagate their demands and stances to the wider public, thereby exerting pressure on decision-makers" (Bakir, 2010:12) such as terrorist groups, NGOs, citizen pressure groups, political opposition, and the like, a line can be drawn from the paper PR campaign or the communiqué, to the use of broadcasting, then websites (Dartnell, 2006) and now social media. Indeed, the Unabomber received massive publicity for his political program based in a terrorist campaign long before Bin Laden sent videos from his "cave" (Young, 2012). Similarly, whistle-blowing and the exposure of hidden information has precedent in driving public debate in conflict – a frequent analogy used in relation to WikiLeaks is that of the Pentagon Papers (e.g. Mulrine, 2011). This is not to say these features are insignificant in Web 2.0, or even that the shifts are merely quantitative – the impact of WikiLeaks in terms of international debate, institutional culture, the sheer amount of material made public, and global repercussions distinguish their activities from those of previous leakers. Similarly, the group of Internet activists known as Anonymous could not be conceived of outside of the context of Web 2.0 anonymity and shifting understandings of identity and influence (Coleman, 2012). However, in the context of emergent data and convergent information flows (discussed in next section) – it is the sheer *quantity* of 'information doers' which has the most fundamental impact to the information environment, rather than the few prominent political or social actors with a Web 2.0 programme.

Bakir calls this more general feature the impact of the "digitally active masses" (Bakir, 2010:12). This can be seen in the influence of 'information doers' through Web 2.0's optimisation of a 'long tail' of potential witnesses to an event, and of commentators and knowledgeable amateurs which mean that the accumulated interest and commentary of disparate individuals can produce a closer approximation of the 'truth' of an event than mainstream media often manages. This is increasingly done in a systematic way through the use of real time indexing tools like Twitter's 'hashtag' protocol, or collaborative news curation tools such as Storify (Sheridan, 2012). Gowing describes this as "hundreds of millions of electronic eyes and ears [which] are creating a capacity for scrutiny and new demands for accountability" (Gowing, 2009:10) far beyond the means and structural limitations of the mainstream media. The example of the blogger Brown Moses (see e.g. Radden Keefe, 2013), who uses open source data posted by internet users in Syria and crowd-sourced expertise from his Twitter followers to forensically investigate the claims of rebels, the Syrian government, journalists and Western policy-makers demonstrates the potential impact digitally active individuals, drawing on a mass pool of content and distributed expertise, can have. Such actors challenge the foundation of traditional state communication power – making it difficult for the financial, political, military and legal power of the state to be translated into communication power. They also challenge the traditional media forms on which propaganda model era communication studies rely – bypassing the "filter" function of mainstream media and creating an information economy characterised by abundance (see e.g. Hansen, 2008:1; Fuchs, 2009:96) in which new phenomena such as virality and campaigning can push stories to prominence[18].

2.3.2 Convergence, Emergence, and Chaos

The impact of information doers on the traditional media draws our attention to another concept crucial to understanding the dynamics of the new information environment, that of *convergence*. It is a concept which sees the shift in our understanding of significant actors echoed in a radical shift in how information travels and has an impact. Convergence signals a radical breakdown between the 'old media' and 'new media' environments. The 'old' world was characterised by linear information flows and rigid hierarchies: from official spokespeople and news agencies, via mainstream media, to a mass and reasonably fixed audience with limited sources of information to choose from. In the new Web 2.0 environment information moves in a much more fluid and unpredictable way. It circulates rather than travels in a linear fashion, and the lines between audiences and content producers become blurred.

The concept of convergence describes a media environment in which the multi-media nature of news information links all platforms of content into a mutually reinforcing web of information. This is evident in everyday communication experience: people consume news through smartphones, tablets, PCs, radios, TVs, and newspapers – and these platforms are linked in new and important ways. There are news shows based on social media commentary (e.g. Al Jazeera's *The Stream*); newspapers incorporating twitter feedback and setting publication priorities based on online metrics (Newman, 2009); user-

[18] For example the "Kony 2012" campaign, in which a concerted social media effort drew global attention to the role of the Lord's Resistance Army in central Africa, demonstrates a new form of Web 2.0-enabled PR, and another type of 'information doer' (Jenkins, 2012).

generated content as a key element of many news stories; and for all their challenges the mainstream media platforms (newspapers and TV) still play a key role in driving online news discourse (Meraz, 2009). Even US Army doctrine lists "flash mobs, blogs, social networking … dating sites [and] virtual online gaming" as technologies which complicate their operating environment (US Army TRADOC (2010), *Pamphlet 525-7-8,* 10). Jenkins describes convergence as "the flow of content across multiple media platforms, the cooperation between multiple media industries, and the migratory behaviour of media audiences who will go almost anywhere in search of the kinds of entertainment experiences they want" (Jenkins, 2008:2). While entertainment is the focus of Jenkins' analysis, we can see the same dynamics in political information and news-consumption: convergence represents a new relationship between news production, content, and consumption – it is the "active audience" of communication research (Hall, 1981) taken to the level of sources, platforms, content production and re-mediation (Chouldry, 2008; Bolter and Grusin, 2000).

Convergence represents a new form of media consumption which is information and interest-driven rather than dependent on the availability of content within a specific pattern of consumption (i.e. the newspaper one reads, the TV channel one watches), thus undermining the role of traditional information gatekeepers and opinion leaders. Information has never been entirely linear and the audience has generally been shown to be active in searching out information of interest to them (see West and Turner, 2000), however Web 2.0 information flows make this task very much simpler, as ease of access through ICTs, and new habits of information sharing (through hyperlinks, 'sharing' content, etc.) mean that we approach a 'convergence culture', "where old and new media collide, where grassroots and corporate media intersect, where the power of the media producer and the power of the media consumer interact in unpredictable ways" (Jenkins, 2008:2). Given the reliance of almost all domestic-focussed military communication practice on relations with the mass media this has serious implications for military propaganda activities.

Hoskins and O'Loughlin describe the shift in information flows in this environment as "a scattered *flux* whereby individuals at many points […] send content back and forth, acting and reacting to one another and creating unforeseen patterns and feedback loops" (2010:122). This shift in information flows – of unpredictability, and of increased importance of feedback – mark another important change in mass communication, especially as it concerns state actors. Information flows are characterised by 'multidirectionality' as opposed to hierarchy or control (Potter, 2002:4) and once it is 'out there', information can be remixed, repurposed, and managed or manipulated by various actors (Bakir, 2010:1). In such circumstances it becomes difficult to conceive of official 'messaging' or 'spinning' as a linear process. Instead, official communication must be understood as taking place *within* these convergent flows of information in a space where control is effectively challenged, if not totally relinquished.

McNair describes the unpredictable information flows of convergence as central to the 'chaos' which characterises the contemporary information environment, saying that "there is a practically infinite range of outcomes to which [efforts to influence publics] may lead, and a high likelihood of failure in any attempt to ensure 'dominant decoding'" (McNair, 2006:49). Once a statement is made, that is, it can reach anyone, anytime, either

unadulterated or having been remixed repeatedly, in any number of contexts, from hostile to reinforcing. This interpretation overstates the impact of convergence, seeing it as fundamentally over-riding all forms of hierarchy and power in the communication environment. Theoretically of course, there are "infinite" outcomes of any message being communicated, but any given message on an important theme – and here we are concerned with conflict – can generally be broken down into two types of interpretation: one which reinforces the position of the actor in the conflict doing the communicating, and one which does not. There are infinite *possible* interpretations, but the *probability* of these interpretations is not evenly distributed. If a military spokesperson sends out a Tweet about a particular event in a conflict, the chances are that almost all interpretations will be relevant to that event or wider military implications. Indeed, the consequences of quintessential Web 2.0-enabled publishing of the Abu Ghraib torture photos were largely predictable – "the abuse of prisoners was not unpredictable as a phenomenon in war … nor was the narrative of hypocrisy", and "once publicised widely across the Internet and in the media, the effects of the abuse on public perception were certainly predictable" (Jones and Baines, 2013:76). Interpretation of communication about conflict is contextualised in relation to that conflict in much the same was as pre-Internet discourse was – convergence undermines old linear communication models and structures of information control, it does not however change the context of conflict or the ability of individuals to reason coherently about it.

In fact, a number of developments suggest convergence can be harnessed by powerful communicators in a way that makes communication strategies *more* effective and predictable. Steps in this direction can be seen in the use of advanced analytic tools to measure target audiences (see e.g. Costa and Boiney, 2011) and military-funded research on the propagation of memes (see page 177); and in the use of social media to follow a message once it is 'out there', either through direct official-public communication (for example through spokespeople on Twitter), or through military engagement in online debate. The convergent information environment is recognised by state actors who seek to refine new forms of engagement. One US military analyst, for example, writes that when it come to engagement a press conference, or even a blog entry or Facebook post is insufficient and "represents [only] a single message input", recognising that "if further inputs or contributions are not made as the message evolves within a larger media conversation, then the efficacy of the communication activity has been compromised" (Cunningham, 2010:16-17). This recognition underlines the importance of studying communication activity holistically within Web 2.0 – no longer is military communication about simply refining messages, but convergence requires that communicators follow messages through the information environment, shepherding interpretation and interacting in various ways to try and achieve the desired impact. Convergence has "the potential to disrupt *or reinforce* the control and continuity" (Hoskins and O'Loughlin, 2010:121) of attempts of powerful actors to achieve their goals – the outcome of which is dependent on the degree of mastery of new tools and new environments by powerful communicators.

There are further challenges than convergence however. The changing media environment is impacted by the increased *speed* of information flows. Concerning the ability of government or military actors to respond to crises, Gowing estimates the effective response time at "no more than a few minutes", a development which naturally

causes wholesale change in he way institutions must respond to developing situations (Gowing, 2009:28). This situation is described by Gowing as "not just a Tyranny of Real Time but a Tyranny of the Time Line" (Gowing, 2009:2) – a strange form of "tyranny", which menaces those who rely on effective propaganda techniques to operate. This leads to "a dramatic and timely promotion of both knowledge and insight" which means that the time between an event happening and the "truth emerging is fast being eliminated" (Gowing, 2009:10 see also Armistead, 2004:9). From an elite perspective, these pressures must be "built into the decision-making process and is part of the very definition of crisis" (Hanson, 2008:99), and has led to the development of new ways to gain influence in the information environment. A key element of this approach has been the recognition that speed cannot always be accounted for, and thus the cultivation of "credibility" as a means of enhancing authority has developed as a key element in military and diplomatic communication strategies (see Keohane and Nye, 1998:90; Slaughter, 2011; Kinniburgh and Denning, 2006). We can also see – at the cutting edge of military communication – forms of psychological operations practice which seek to build up and maintain audiences with a sort of latent propaganda value which can be instrumentalised at times when particular messages must be spread (see page 117).

As well as time, Web 2.0 is seen to affect a compression of *space* during conflict – with the distinction between battlefield communication and the domestic or global media breaking down. While some warzone communication efforts *do* remain largely local – the use of leaflets, military-run radio and TV stations, and other information campaigns remain a key part of Information Operations practice (see e.g. Munoz, 2012) - these elements are situated within a global information environment in which communication from one area travels and has effects in others. This fact is reflected in DOD communication guidance which notes that in practice "information intended for foreign audiences, including public diplomacy and PSYOP increasingly is consumed by our domestic audience, and vice-versa" (*Information Operations Roadmap* (2003), quoted in Bakir, 2010:77), with Web 2.0 meaning "it will be practically impossible to control the distribution of signals to only one audience" (DOD - *Strategic Communication JIC,* 2009:7, see also DOD - *JP 3-13,* 2012:1-1). In this respect the traditional distinctions between battlefield-focussed military communication (PSYOPS), domestic media management (public affairs), and diplomatic public communication (public diplomacy) also break down as these media environments and practices converge in a global information environment.

Thus the mediation of conflict depends on "complex, near-instant feedback loops between national, translocal/diasporic and global public opinion" – all of which influence one another and converge in the information environment (Hoskins and O'Loughlin, 2010:18; see also Grusin, 2010:6; Mackinay, 2009:85). This is not necessarily a development which diminishes state power, however, as it works both ways, allowing state actors "access to a great range of globally distributed targets amenable to coercion of various forms" (Betz and Stevens, 2011:39). In the process, the concept of 'mediation' on which many studies of mass media are based comes to be replaced by one of 'medatisation' – moving from an understanding of media as *representation* of conflict, to one in which media and conflict interact in a much more dynamic way (Hoskins and O'Loughlin, 2010:122; 4).

The cumulative effect of the new actors and information flows in the Web 2.0 environment, and the concept which is perhaps the most immediately recognisable and

impactful phenomenon in times of conflict, is *emergence.* Described as "the massively increased potential for media data literally to 'emerge'; to be 'discovered' and/or disseminated – instantaneously – at an unprescribed and unpredictable time after the moment of recording, and so to transcend and transform that which is known, or thought to be known, about an event" (Hoskins and O'Loughlin, 2010:9). Emergent data is that recorded in photographs, videos or any other form which finds its way into the public domain and challenges general understanding and undermines official narratives about an event. The photos of US torture at Abu Ghraib and the video of Saddam Hussein's execution are two prime examples from the war in Iraq which demonstrate how the phenomenon terrorises state communicators (see e.g. Bakir, 2010:140-143).

Emergent data is often linked to the way new ICTs can break down barriers of space and time in creating rapid impact through real-time user-generated content, but there is also a more distinct long-term effect of the phenomenon. The ubiquity of recording (including self-recording) through CCTV, mobile phone cameras, blogs, social media postings, and storage of information digitally contribute to a growing "archive of unpredictability" (Hoskins and O'Loughlin, 2010:9). This means that previously-unknown data may emerge (through dedicated online searching, malicious leakage, or through hacking) at any time after an event and have an impact on debate, narrative, and understanding of that event. The large leaks of State Department cables and War Logs by WikiLeaks are key emergent events which enhanced public understanding of US policy and conflict in the 2000s. The manner in which some of these disclosures discredited aspects of policy, or undermined particular figures, despite emerging some time after the events they documented illustrates how this "archive" may have a long-term impact on state communication power – making unethical behaviour more risky and requiring subversion to be a long-term process, no longer a matter of 'getting away with it' at the time. DOD doctrine describes the new situation as "characterized by increased visibility and transparency" in which almost every military action is considered potentially public (DOD - *Strategic Communication JIC,* 2009:7).

It is not difficult to see how emergence challenges state communication power – it negates information control and censorship, bypasses gatekeepers, and makes the strategic planning of communication fraught with difficulty and unpredictability. Indeed, it means that "centralized and hierarchical modes of information dissemination … can no longer be taken for granted" (Christensen, 2008:157). As the example of Abu Ghraib - which became a driver in the emerging insurgency in Iraq (Burke, 2011:171) - shows, this unpredictability can have effects far beyond the information sphere. As such, the phenomenon can be seen to create a sort of generalised chaos in which those reliant on control of information must fight a "permanent war against contingency itself" (Hoskins and O'Loughlin, 2010:12, see also Dillon, 2007). This chaos of emergence can be seen, in a sense, to mark the demise of a form of state communication power which can be premised on the ability to influence public communication through the filters of mediation – rather, forms of communication power shift to dealing with this contingency and exerting influence in other ways[19].

[19] This shift in military practice was foreseen by Taylor (1995:11) in relation to the 'instantaneous communication' of satellite news, suggesting Web 2.0 is the culmination of a process of the break down of the 'mediation' paradigm rather than a bolt from the blue.

What is challenged is the traditional relationships between military, government, and publics as they play out in the new information environment in which 20th century forms of control and influence are replaced by emergence, convergence, "unruliness" (Bakir, 2010:1), "unknowable risk", "unexpected feedback" and ambiguity (Hoskins and O'Loughlin, 2010:6). For McNair, this underlines that control of information and communication is impossible (McNair, 2006), necessitating a shift in focus away from the attempts to control or influence by powerful actors towards a 'chaos paradigm' (McNair, 2006:vii) in which analysis should focus on "the possibilities allowed by an emerging *cultural chaos* for dissent, openness and diversity rather than closure, exclusivity and ideological homogeneity" (McNair, 2006:vii). That there is change is undeniable. Critical communication studies, focussed on the mass media, where a number of reasonably well-understood structures, as well as a forgiving media logic (slow-response times, very selective mediation of events, limited access to mass audience) showed that the information environment was somewhat predictable such that a level of control could be exercised over media and information flows by powerful actors. McNair's 'chaos' paradigm, while convincingly suggesting this situation as coming to an end due to new ICTs, makes the mistake of conflating the new unpredictability of the information environment with the impossibility of developing new forms of control, or relations of power.

For McNair, the information environment "far from being an instrument or apparatus of social control by a dominant elite, has become more like the weather and the oceans in age of global warming – turbulent, unpredictable, and extreme" (McNair, 2006:xviii). This analogy underlies the three fallacies in a strong-interpretation of the 'chaos paradigm'. Weather is a natural phenomenon (largely) separate from human activity, whereas information and communication are fundamentally social practices. Secondly, global warming is caused by structural factors, suggesting (at least the possibility of) high-level control and influence by powerful agents. Finally, powerful actors do not simply surrender themselves to the unpredictability of the weather – they plan for resilience, against contingency (Duffield, 2011, Dillon, 2007) and position themselves to benefit at times of crisis (Klein, 2007). We can see this later observation evidenced in the work of state agencies to harness new ITCs for surveillance (see e.g. Morozov, 2010; Greenwald, 2014), refine communication programs (Latar et al, 2010), and research to aid military campaigns (the subject of chapter 6). It is folly to assume that challenges to powerful groups in some areas automatically lead to the loss of their communication power *per se,* instead the reaction of these groups to the challenges must be thoroughly examined.

2.4. Examining the Information Environment of Digital Age Conflict

2.4.1. From Mass Media to the Information Environment

Analysis of the rise of Web 2.0 demonstrates the imperative to develop an understanding of state communication power which moves beyond a focus on *mass* media as the referent of military communication practices. This work shows that many traditional elements of mass media upon which successful studies of propaganda have been based are being eroded by Web 2.0. These include the limits of mediation in a relatively small media

environment; the powerful role of militaries on controlling battlefield information; and the structures of media tradition, influence, and other propaganda model filters. An understanding of the proliferation of information and convergence of communication practices in Web 2.0 also shows that media and social experience must be examined in an increasingly integrated and dynamic way – that the "social" part of "social media" is as important as the "media" element.

As such, the distinction between the two bodies of literature outlined in section 2.2 - the general focus of domestic studies on the mass media, and of military-based studies on more distinct techniques and practices of military communication - cannot be sustained in the current context. While the traditional media platforms (TV and newspapers) are not irrelevant, the role they have traditionally played in setting the news agenda and as arbiters between the state the public is significantly challenged (see e.g. Wallsten, 2007; Papacharissi, 2008:239, Kaempf, 2013). Similarly – the analysis of the impact of military or state propaganda practices in terms of their effects on mass media content (e.g. Herman and Chomsky, 1988; Philo and Berry 2004) must be superseded in a situation where emergent media and convergent information flows can drive content to prominence regardless of mediation-based filters. Thus, instead of mass media, this research examines the US military propaganda apparatus in the context of a global *information environment* – a conceptual area which includes mass media, social and new media, and emerging forms of communication; and is the scene of interaction for everyone from government spokespeople to citizen journalists, corporate PR flaks, whistle-blowers, and PSYOPS practitioners.

The information environment is also the key referent of US military Information Operations (IO) doctrine, where it is defined broadly as "the aggregate of individuals, organizations, and systems that collect, disseminate or act on information" (US DOD – *JP 3-13,* 2012:iii, see also King, 2010). In doctrine, this environment is formally described as having three domains - the physical, informational and cognitive (DOD, *JP 3-13,* 2012:viii) – which sometimes leads to a more technical understanding than is useful here (i.e. attacking enemy fibre optic command and control systems would be considered an element of the 'physical' domain of the information environment[20]). However, doctrine also notes that the 'cognitive' dimension, which incorporates the thoughts and decisions of individuals, is the "most important", where "target audiences are most prone to influence and perception management" (US Army – *FM 3-13,* 2013:2-3). There are also descriptions of the information environment as characterised by speed of information, proliferation of competing sources, global connectivity, transparency and newly empowered actors which almost perfectly cohere with the disruptive impact of Web 2.0 discussed above (see DOD - *Strategic Communication JIC,* 2009:vi, also demonstrated in the many quotes from US doctrine in the above section). Top-level doctrine describes how these changes have "transformed the information domain into a battlefield, which poses both a threat to the Department of Defense [...] and serves as a force multiplier when leveraged effectively" (DOD - *JP 3-13,* 2013:1-1) by either the DOD or their adversaries. Thus, the Web 2.0-enabled information environment is identified as the referent of US military

[20] This is particularly true of the "cyber" element of the information environment which is consistently understood in fundamentally technical terms – a matter of protecting and attacking digital infrastructure (see DOD – *Strategy for Operating in Cyberspace,* 2011; US Army – *FM 3-0,* 2008:1-3; DOD – *JP 3-60,* 2013:C-7; GAO, 2011).

communication development, producing a useful congruence between the site of military development and the focus of the research.

Consequently, the analytic focus of this research is broader than that of traditional communication research. It is focussed not at the level of the content of particular military messages, or the impact upon a particular audience or discourse, but instead examines the effect of the propaganda apparatus on the information environment as a whole. Asking how it instrumentalises certain forms of knowledge; how it imbricates military practice within particular areas; and how it structures relationships between military actors and other populations. One of the most important theorists of propaganda, Terence Qualter, argues that the "propaganda effect arises from the interaction of a communication and an audience, through a specific medium, in a particular cultural ideological environment, at a particular time and place. All of these variables must be considered as a unit" (Qualter, 1985:110). I assume that the specifics of an individual communicative act are reasonably accessible to straightforward analysis - indeed they have formed the basis of most communication research to date. Thus, this research looks to develop an understanding of the latter elements: the cultural ideological environment, the medium, and the "time and place" (that is, the socio-technical context) in order to enable a more holistic understanding of contemporary communication power.

The utility of an approach which focuses on the information environment as referent of military development is demonstrated in the analysis of US Special Operations Command-run news websites (section 5.3), which would be most familiar to critical communication studies. The analysis shows that the fact that these websites have built up large audiences through social media, have content which is reproduced in mainstream media in other countries, and thus act as ways to insinuate military influence into online social networks and news flows, are far more important elements than the content of particular stories posted on the site. Only through the holistic concept of the 'information environment' can this type of development be properly understood, where it is situated in an area of convergent information flows, where credibility within a network might be more important than the content of a particular message, and where propaganda websites' main challenge may be vying for followers in an attention economy. As such, an examination of the content of these websites forms only one part of the analysis. An examination of how these sites interact and compete in the broader information environment, and how they embed themselves in the weft and weave of regional or international news or social flows, form a key part of our understanding.

To study the information environment is, to an extent, to examine the construction, manipulation, and contestation of *space*. The changing nature of the information environment (the key *space* in question) due to Web 2.0 ICTs is a key driver in the changing state communication power. To conceive of this environment as a 'space' is to say that it is a place where social activity happens, information travels and becomes objectified (Fuchs, 2008), and power relations are structured and inscribed. Space, that is, is social and an important element in understanding how power is mediated in society (see e.g. Froehling, 1997:293; Rahimi, 2011:161; Pamment, 2012:2). The research takes into account of the importance of examining military practices which aim to "make space knowable" in order to act upon it in certain ways and "arrange both space and information to enact governance" (Barnard-Wills, 2012:95). Following Saco, I contend that space is

never neutral and is "central to the reproduction of particular political-economic relations" even while it is partially affected by those relations (Saco, 2002:6).

To see space as a key element of power is to recognise that the dominant actors in a society play a key role in producing social space: we can see this from control of the infrastructure of the Internet, and in the links between the US Government and the Web 2.0 giants (Benkler, 2011). It can also be seen in the increasingly direct attempts by state actors to influence the information sphere through the legal one – as seen in the prosecution of hackers and pirates, and the pressuring of Internet companies regarding the hosting of specific content (MacAskil, 2010). Power can also be seen as inscribed in social space in even more nuanced ways. This can be through the enforcement of norms (for example through 'real name policies' (Guoming, 2012) or 'web passport' (Washington Times, 2011)), but also through the *exploitation* of exiting norms to draw on space as a 'force multiplier'; the imposition of and creation of ad hoc structures of authority (for example the largely autonomous rise to prominence of a group of terrorism 'experts' through social media (Muqawama, 2012)), or the instrumentalization of the authority of others. This appreciation of the way power becomes inscribed in the information environment coheres with the understanding of the impact of communication beyond a matter of content, as "mechanisms for linking things together, as articulations in networks, as the glue and the infrastructure" (Packer, 2010:90) [21]. In the analysis, it allows the study of elements such as propaganda websites from the perspective of the social spaces they create, and the way information they produce ends up invading other news websites, thus producing a broader effect on the notional space of online news.

In terms of ICTs, Robins and Webster draw our attention to examining how they "provide the filaments through which power and control [...] invade the social body as a whole" (Robins and Webster, 1988:55). A concern with cyberspace *as a space* is a key thread running through state attempts to produce influence in this area, as well as in those who analyse these attempts. For example Herrera (2007) examines ways in which states attempt to 'territorialize' cyberspace, through attempts to render it quantifiable, mappable, and open to intervention by the institutions of state power (primarily the police and intelligence services, see also Naughton, 2001, Diebert, 2008). Thus the analysis must incorporate an understanding of how space is understood, measured, ordered, controlled, regulated, and manipulated as a key element in studying apparatuses of power (see Graham, 2006; Weizman, 2006; Graham, 2010).

The research finds in a number of intelligence and communication programmes a break down in the distinction between military and social space. Pamment argues that this spatial approach can help us understand military communications strategies "in terms of 'transposing' military and economic dominance into other spaces; bridging the realms of 'hard' and 'soft' power" (Pamment, 2012:9, see also Herrera, 2007). This notion of the Internet as contested social space is important as so many studies of state power on the Internet focus not on the social space as whole but on skirmishes at the margins – on hackers battling hackers (Rid, 2011), or on relatively insignificant overt propaganda wars between the twitter accounts of rival forces (Alonso, 2012). Meanwhile, this research

[21] The utility of this type of approach in research on ICTs and conflict has been demonstrated by a number of theorists in technology studies and geography (see e.g. Saco, 2002; Galloway and Thacker, 2007; Dillon and Reid, 2009; Graham, 2012; Mehta and Darier, 1998)

shows, military thinkers reconceptualise Web 2.0 as a key element of the contemporary "battlespace" (see e.g. Graham, 2012; Croser, 2011:1-2), and develop significant processes to mine it for intelligence and PSYOPS purposes. Rather then looking at the novelty 'twitter-war' at the margins, an understanding of this virtual terrain as contested allows us to examine the effect of military activity on social and technical space.

In situating the research around the role of a specific actor (the US military) in this information environment, the research also avoids any prolonged engagement with debates about the nature or capabilities of the various technological platforms which make up Web 2.0. The primacy of technology in driving social change is a much disputed area in relation to the rise of the Internet, and particularly Web 2.0 (see discussion in Hanson, 2008:6), with debate raging over whether new ICTs enable or inhibit political emancipation, social development, or other abstract goods (see e.g. Morozov, 2010; Gladwell, 2010). These debates have generated far more heat than light, and the analysis here goes beyond technological determinism in the recognition that technology is socially, politically and ideologically situated. The Internet is a "dynamic socio-technical system", one in which the technological structure (the codes, the wires, the databases) "can't be separated from its human use and the permanent creation and communication of meaningful information" (Fuchs, 2008:121, see also Rappert, 1999:747). But it is a system in which all outcomes of interest to this research are *social*, concerning the relations between groups of humans. The concept of the information environment recognises that both technological and social factors can have an impact – but allows us to asses that impact in terms of the effects on and in and environment where social outcomes and relations and produced and negotiated.

2.4.2. Mediatisation, War and the Information Environment

The concept of the information environment does not just apply to a more complex understanding of communication however, it also has implications concerning the relationship between information and conflict itself. This reflects an ongoing breakdown of the distinction between war and *its representation*. This is not to take the extreme postmodern perspective that the reality of conflict is indistinguishable from its mediation (e.g. Baudrillard, 1995). Rather, it is to recognise that a number of divisions which made the distinction of studies of war and its representation possible are no longer tenable. The contemporary environment is one in which information from the battlefield is almost impossible to control consistently, where combatants engage in public arguments via official and unofficial accounts on Twitter (Alsonso, 2012), where the filming of attacks and uploading the footage to YouTube is a key element in funding insurgencies (Abdul-Ahad, 2013), and where the social media activity of individuals can even lead to them being targeted by drone strikes (see the case of Anwar Al-Awlaki, Scahill, 2013:398). This is an environment where the relationship between war and media is not just one of an activity and its representation – but one in which communication and violence are deeply intertwined.

Hoskins and O'Loughlin (2009:4) propose that we should understand war as *mediatized,* that is, it has become affected by the "logic of the media" (see Hjarvard, 2008) to such an extent that "the conduct of war cannot be understood unless one carefully accounts for the role of the media in it" (Hoskins and O'Loughlin, 2009:4). This integration happens not

only at the representational level, but also through recognising that "media are integral to those practices where actually coercive or kinetic force is exercised" (Hoskins and O'Loughlin, 2009:5). The examples of Al-Awlaki and the role of YouTube in insurgent activity demonstrate this relationship at the operational level, and it is also clear at the strategic level in the statement of the then-Chairman of the US Joint Chiefs in 2009 that "videos and images plastered on the Web – or even the idea of their being so posted – can and often do drive national security decisionmaking" (Mullen, 2009). This way of thinking about media and conflict in a much more inter-related and mutually-influencing way underlines the necessity of the concept of the information environment to grasp what is at stake.

Whitehead and Finnström (2013) argue that the "emerging virtual space" of the conflict information environment is not just one of news and new media, but one which refers to technologies outside of the public domain: military mapping technologies, surveillance, and other forms of measurement which "mediate both combat and decision making" (Whitehead and Finnström, 2013:2). Through examining military engagement across the Web 2.0 information environment this thesis demonstrates that two key elements of contemporary military activity are those of intelligence gathering and the funding of research into online communication. As such – and in line with the understanding of propaganda as a matter of the politics of information - the understanding of the information environment also extends an interest in military communication activity beyond the realm of communication practices, taking in some key elements of military intelligence and research & development (R&D). Intelligence and R&D are related both in theory and practice to more traditional propaganda activities like PSYOPS – and assessing them within a propaganda apparatus which acts through the information environment allows us to develop a coherent understanding of these practices.

Although it is a newly emerging area, there have been a number of research projects which have approached, broadly speaking, the information environment of Digital Age conflict. One common approach has been to address the environment itself at a theoretical level to assess the "ambiguous" role of the ICTs (such as social media platforms) which make it up by producing an "empirical contextualization of new technologies and the dynamics they afford" (Pötzsch, 2013:5, see also e.g. Fenton, 2012), thus attempting to assess whether they are emancipatory technologies or those which cement the power of the rich and already powerful (e.g. see Bratich, 2011; Morozov, 2011). This approach has been ineffective in understanding the contemporary impact of military actors. Pötzsch, for example, examines Web 2.0 technologies in conflict from a number of perspectives in order to speculate about the *possibilities* they present to state or military actors and how the *could* be used by warmongers or intelligence officers to produce propaganda or limit personal freedom. This approach, more technological-speculationism than technological-determinism (see also Kaempf, 2013), has predominated in popular discourse about military engagement with Web 2.0 – a phenomenon driven by the dearth empirical data in the area[22], and the fraught context of military-public engagement online in the age of WikiLeaks, Anonymous, and Edward Snowden. However, approaches based on such speculation can produce only hypothetical insight.

[22] And the fantastic nature of what information does make it into the public domain (see e.g. Fielding and Cobain, 2011; Greenwald, 2014)

Another approach to the analysis of Digital Age conflict which is common, more often in media than in academia, is one based on drawing together a variety of incidents broadly related to Web 2.0 and conflict and attempting to present a general account of the contemporary situation. For example there are studies based on studying Jihadi social media accounts (Prucha and Fisher, 2013; Alonso, 2012); online arguments between Western government or state actors and their adversaries (McCants, 2013); links between social media trends and unrest or conflict (Lynch et al, 2014; Aday et al, 2012); and the activities of political nuisance-hackers (Limnéll, 2013; Heffelfinger, 2013). Such stories are bread and butter for media organisations, providing low-cost access to fashionable technology and conflict stories, but they represent a very superficial engagement with a complex process of change. A couple of Twitter users arguing about war is, without context, just that. Consequently, attempts to draw this type of example together to produce a single analysis have been largely unconvincing (see e.g. Niekerk and Mahraj, 2013; Pötzsch, 2013), lacking any focus on a particular actor or area of conflict. This is not to say that such research offers nothing of value - indeed, it is drawn on throughout this work and does a good job of demonstrating the range of new phenomena in the information environment - but it does not offer a coherent analysis which can guide the research in understanding of the impact of powerful actors.

The approach taken to the problem in this thesis is this: I acknowledge the changes in the Web 2.0 information environment and military practice, but recognise the relations of power which have historically been decisive in conflict communication (those of military might, key position as information producer and authoritative actor, etc.) hold in Digital Age conflict. This is not to say that the power of military communicators simply carries across into the new information environment – but that most of the military actors and structures which were important in the pre-Web media environment continue to exist, and are adapting their conduct to the new situation. Thus instead of speculating about what military actors *might* or *could* do, this research focuses on those actors who have previously had a decisive impact and are *demonstrably* doing something in this area, and assesses the impact based on a study of their activities. The US military, as the worlds largest military power, at the heart of Digital Age conflict and "at the forefront of the development of and adaption to digital new media technology" (O'Hagan, 2013:558), is the logical place to start.

There are a few studies which focus on US military development in this context, usually focussing on the most visible or superficial elements. There have been a number of studies published on the development "milblogging" (military blogging) as the blogs of soldiers play an important part in the relationship between militaries and publics (see e.g. Carr, 2013; Bennett, 2013). Other studies which discuss the relationship between the US military and Web 2.0 have focussed on the changing policy – based on considerations of public affairs and operational security (OPSEC) – on allowing soldiers to openly use social media platforms (see, e.g. Knopf and Ziegelmayer, 2013; Lawson, 2013). These are service-wide approaches to social media intended to make sure soldiers don't post anything online which may undermine the credibility of the military or accidently get them killed. One of these studies notes that "so far, much military use of Web 2.0 appears best suited for domestic communication and public relations" (Knopf and Ziegelmayer, 2012:12). This conclusion is a self-fulfilling prophecy for studies which have examined only the publicised areas of US military engagement with Web 2.0 – OPSEC and public affairs.

These are areas which, being focussed on force protection and domestic communication, are very much at the self-explanatory and transparent end of the Web 2.0 engagement spectrum.

In examining the struggle between state interests and citizens around the possibility of anonymity online, Zajácz notes that in examining Web 2.0 as an information environment most analysts have approached it with "the average user in mind" (Zajácz, 2013;491, e.g. Goldsmith and Wu, 2008; Lessig, 2006). Much in the same way, studies of the US military focussing on milblogging and official social media policy have given most attention to those areas which have the broadest effects on the use of social media by military users (that is, allowing them to use social media or not). However, Zajácz notes that in order to understand the changing nature of power relations in the information environment we should use "a framework that better accommodates skilled and/or powerful opponents" (Zajácz, 2013:491), where cutting edge practices and the development of more precise or nuanced approaches have significant influence. In recognition of this, the research here pays particular attention to the 'sharp end' of military communication power – not the transparent elements of public affairs or operational security but the more hidden and effective element of *psychological operations*. As chapter 5 shows, it is in this area that "the tip of the spear" (to borrow a metaphor from special operations) of Web 2.0 propaganda is being honed.

The research approaches the subject of contemporary American military engagement in Web 2.0 from a theoretical perspective grounded in a Foucault-inspired understanding of *state communication power.* It seeks to examine how a broad range of military practices – particularly those which had thus far escaped scrutiny due to their clandestine or obscure nature – form a *propaganda apparatus* addressing the challenges and opportunities of *Digital Age conflict*. The referent of these activities, and the site of their impact, is understood as the *information environment* of Web 2.0 – a much wider analytical space than the mass media of traditional communications studies, and one in which the practices of communication and conflict are deeply intertwined. This approach allows the development of insight into the role and impact of a diverse range of military activity relating to Web 2.0, and an analysis grounded in a complex understanding of the relationship between contemporary communication and conflict.

3. Studying Military Activity in the Web 2.0 Information Environment: From Theory to Method

3.1. Governmentality and a Digital Age Propaganda Apparatus

The discussion in the previous chapter presented the theoretical and disciplinary context for the work. It pointed the way to an approach which recognises that understanding of contemporary state communication power can best be achieved through the examination of the range of practices, technologies, structures and relationships which apply to a particular context. This research focuses on a particular aspect of social life - conflict - and on an actor which has a preeminent role in the conflicts in question: the US military. The research also focuses on a particular context for this activity – the development of practices addressing Web 2.0 in the GWOT era, what I have called *Digital Age conflict*. This allows research to proceed in a manner which recognises the complexity of power as operating in a *broad* way but studies it in a *narrow* focussed context as it applies to this particular situation. To do this, we proceed by a method drawing on a further Foucauldian concept, that of *governmentality.*

Like many Foucauldian concepts, governmentality is one which has been interpreted and developed in different ways. Academic engagement with the subject generally falls into two camps – that which engages with governmentality as a theory of the structure of power in liberal societies, and that which draws on it as a method for studying forms of power in particular situations (see Dean, 2010 for an overview of both approaches). This research is not interested in an academic exegesis of Foucault (see e.g. Collier, 2009), instead it draws on what is useful in both bodies of work. Primarily, I draw on this literature as a *methodology* which allows the development of an approach to studying particular sites or areas of power in a way broadly coherent with the understanding developed in the previous chapter. Secondly, analytical work based in the concept of governmentality and related Foucauldian concepts is drawn on to provide context and coherence to the analysis of the data.

The methodological insight this research takes from Foucault is that we must study power by "investigating where and how, between whom, between what points, according to what processes, and with what effects, power is applied" (Foucault, 2007:2). This analysis of power, made observable through studying the complex set of procedures, relations and institutions of its production, is the basis for the development of governmentality as a methodology outlined by Foucault and other theorists since (e.g. Miller and Rose, 2008; Dean, 2010) for studying state power. The methodology has two main steps: firstly, the analysis of the construction of a *problem field* (Miller and Rose, 2008:14-15) or "series of knowledges" (Foucault, 2007:108) which studies how a particular problem is conceived by powerful actors; and secondly, the examination of how "specific apparatuses" (Foucault, 2007:108) or "assemblages of persons, techniques, institutions [and] instruments" come to act and have influence on that problem field (Miller and Rose, 2008:16).

3.1.1. The Problem Field of Digital Age Conflict

The focus on a particular problem field – in this case the field of Digital Age conflict – allows the research to coherently study diffuse processes of power within a framework which gains its methodological and empirical coherence from the research area itself, rather than relying on mirroring the bureaucratic structures or concepts of the organisations studied or areas outlined by previous research which may not be applicable to the contemporary situation. Digital Age conflict is not always addressed in a linear or very coherent manner within the US military – with actors across the organisation working in different and sometimes contradictory ways. Thus, the 'problem field' method allows us to produce a methodological and analytic coherence without positing an empirical one. The analysis of state institutions in this way as they respond dynamically to changing situations - is particularly useful in critical social science which takes the construction of new problems and ways of operating by powerful actors as the subject of analysis, rather than taking state activity "as the unquestioned premise of a research agenda" (Wedel et al, 2005:34, see also Wright and Reinhold, 2011:93). It helps avoid technocratic analysis or reliance on terms of reference integral to state power itself.

In studying how military actors exert power in a particular field (in Foucauldian terms: how the field is *governed*), we begin by asking how a problem is conceived, who thinks it is a problem, where is the problem situated, what language and concepts are used to discuss the problem (Miller and Rose, 2008:14-15), and – crucially as relates to the study of contemporary communication and conflict – what spaces and populations are seen as problematic? In so doing we begin to study the process of how state power acts over the field, by examining how it is "made amenable to intervention" (Miller and Rose, 2008:14-15). This is a crucial first step to examining state activity as "the activity of problematizing is intrinsically linked to devising ways to seek to remedy [the problem]" (Miller and Rose, 2008:15). Or, to put it more bluntly, "the way that a problem becomes understood as *being a problem* is politically important" and has implications for the type of 'solution' proposed (Barnard-Wills and Ashenden, 2012:15).

In looking at state and military practice we must examine which actors in that area produce research and reports relevant to Digital Age conflict; ask how it is understood in doctrine and policy papers, and what form of military activity it is discussed in terms of (e.g. as an intelligence problem or one of military-civilian relations, relating to specific forms of warfare, etc.). The analysis of the problem field thus began in the previous chapters by examining broad elite discourse (and its academic analysis) relating to the challenges of Web 2.0, and of the communication-related aspects of the GWOT (insurgency and the changing information environment). It continues by studying the institutions and doctrine which are influential in producing discourse and in a particular area (see Miller and Sabir, 2012) in the recognition that this is a key element in guiding how the military as whole will act upon the 'problem'.

The analysis of the problem field of Digital Age conflict allows the identification of areas of potential deeper engagement and development. Military activity in this area is largely covered by interlocking areas of military discourse which address the issues of public communication (e.g. PSYOPS, strategic communication, Information Operations, etc.), forms of irregular warfare (counterinsurgency, counter-terrorism, unconventional warfare, etc.), and intelligence. Discursive development in these areas is explored in depth

in the thesis, including in relation to practical developments addressed in the later research chapters, showing that the distinction between *problem field* and *apparatus* is neater in theory than it is in reality, where discourse and practice often cannot be usefully distinguished.

As a discourse-based form of analysis, the exploration of the problem field draws on a wealth of documentary material, including: proceedings of conferences, think tank publications, military and diplomatic journals, books, academic papers, government reports, testimony to lawmakers, military doctrine and semi-official literature (referenced throughout). The analysis takes in texts at the theoretical level – such as those on warfare in an interconnected age (e.g. Arquilla and Ronfeldt, 1997; Hammes, 2009), understanding the role of the 'information environment' (SecDev Group, 2009), or contemporary intelligence (see Flynn, 2010); as well as documents closer to military activity such as developing COIN doctrine (e.g., US Army/Marine Corps – *FM 3-24,* 2006), and the comments of serving military commanders (e.g. Bostick, 2011; Cunningham, 2010). From this literature, key challenges and opportunities are identified, important paradigms in intelligence and operations outlined, and influential ideas in driving new practices placed in context.

This, of course, raises the question of *influence* and how to judge it in documentary data relating to emerging areas. Documentary data has the key advantage of providing material in which influence is evident – other writers are referenced, concepts borrowed, and influence is discernable and frequently acknowledged. Documentary material in the area of interest was examined through careful reading throughout the research period, and the key contents, arguments, and references of hundreds of documents were noted and compared. This allows an informal reference analysis to be performed from which the identification of canonical texts, important paradigms, and concepts can be established. The result of this process is the outline of the problem field addressed most fully in sections 1.3, 2.3 and chapter 4. The method of documentary analysis is discussed more fully in sections which draw on specific bodies of discourse (see also Appendix A).

3.1.2. Examining a Propaganda Apparatus

Having outlined a particular problem field, the research proceeds to examine how the actors in question (the US military) move to exert influence over this field. This is done in a holistic way, examining as an *apparatus* "all those devices, tools, techniques, personnel, materials, and [processes] that enable authorities to imagine and act upon the conduct of persons individually and collectively" (Miller and Rose, 2008:16). The recognition of the sophisticated and multiple ways power relations are reproduced allows researchers to study the "microphysics of power" (Foucault, in Robins and Webster, 1988:52) as they apply to a particular situation. This approach is particularly effective in the study of a developing military bureaucracy where material advantage is does not linearly and coherently transfer into battlefield advantage. The data presented here examines US military activity in a number of different areas: the direct production of semi-transparent fake news websites (often providing "real" news!); the funding of a range of academic projects in fields of online influence; and the development of Web 2.0-based intelligence practices. The apparatus approach allows us to study power as the outcome of broad social processes which apply to the field of Digital Age conflict.

Foucault explicitly outlines the concept of an apparatus of government as: "a thoroughly heterogeneous set consisting of discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic positions [... it] is a network that can be established between these elements [...and] has as its major function the response to an urgency" (Foucault, quoted in Agamben, 2009:2). Thus an apparatus is a *network of elements* which come together in a particular way to respond to the a specific problem field ("an urgency"). It is constructed of material, discursive and structural elements. For example, we see that the area of Web 2.0 PSYOPS bring together military-sponsored contractors (material), concepts such as 'information engagement' which seek to shape the way relationships between military and civilian actors are construed, and structural elements such as the promotion of norms or influencing the use of social networks. Seeing power as operating in particular areas through apparatuses thus allows us, by *limiting* the area of activity (through delineating a problem space), to *expand* our account of the relevant actors, techniques, and structures through which the area is governed - leading to a deeper understanding of how the parts of an apparatus influence outcomes in the area of Digital Age conflict[24].

The study of military power as acting through an apparatus allows us to examine a form of power which "operates across state institutions and others that have nothing (directly) to do with the state" (Lyon, 2003:646). While it makes state power a more dispersed object of analysis, it allows us a framework in which to study the emerging influence of various actors in what is a new and quickly developing field of activity where power and influence are contested. The study of a wide range of actors allows us to take the role played by non-military actors such as contractors and academics into consideration. Furthermore, new technologies (such as smartphones), protocols of communication (such as access provided by Twitter to social media analytics), and contingent events such as WikiLeaks or the Abu Ghraib can potentially have as much influence in driving military practice as years of doctrinal development. In these circumstances, the study of an apparatus – including institutional, ideational, structural, and contingent elements – which forms around the problem field provides a methodological basis for the study which intuitively meets the requirements for examining the research area.

A key element drawn from discussion of apparatus theory is thus the recognition of the ways in which elements not related to structures of power *per se* can shape outcomes and practices. Thus clarification is required regarding the role of actors and intentionality in a propaganda apparatus. While the outline of the problem space by state institutions through such elements as military doctrine, the statements of policymakers, or practitioner-based discourse emphasise the agency of the military in addressing Digital Age conflict, this must not be understood as entailing that the construction of an apparatus as a fully conscious process. While many of the actors involved in particular organisations (e.g. SOCOM, military contractors), in undertaking particular practices (e.g. constructing high-level policy, producing technology for PSYOPS) think about the problem field and their own role in engaging with it in a comprehensive way – this thinking does not

[24] The concept of *apparatus* has been used in various studies (sometimes linked to the term *assemblage*) which have addressed contemporary forms of power (see e.g. Agamben, 2009; Lyon, 2003, 2011; Haggerty and Ericson, 2000). The term *apparatus* is used here as 'assemblages' carries significant ontological baggage through association with the post-structuralist work of Deleuze (1992, see Legg, 2001:128)

completely define the field. I find that one of the most effective parts of SOCOM's PSYOPS website empire is the way it benefits from norms of sharing and linking in the online news ecology. In looking at the totality of institutions, practices, discourses, etc. that cohere to act upon a problem field the intentionality *of the overall apparatus* is non-existent. There is no "propaganda apparatus" overseer in the US military shaping diffuse intelligence practices, R&D programmes, PSYOPS doctrine, and CYOPS practice into a coherent whole – despite the high-profile attempts to create such an overseer in the infamous Office of Global Communications in the early GWOT years (see Snow and Taylor, 2006), the apparatus is larger and more complex than any particular programme.

Neither does being situated within this apparatus imply an intention to aid its power on the part of every element. It is entirely conceivable that many of the researchers working on papers funded indirectly by the DOD discussed in chapter 6 have no idea of this funding, or its role in a broader apparatus of military power. The research they are conducting may well have important effects in other problem fields – in driving academic knowledge. It can even produce contradictions, such as the case of the US Navy-sponsored TOR online anonymity platform, which has been said to directly undermine broader US intelligence power online (see Levine, 2014). Elements are understood in *within* apparatuses, seen as acting on *particular* problem fields, and such incorporation does not exhaustively define the broader social role of each element. This approach thus avoids the analytic *cul de sac* of investigating particular technologies or practices as if their potential for authoritarianism or emancipation is an *inherent* attribute (a popular form of analysis regarding social media and social change, particularly as relates to protest in the Arab and Muslim world, see Morozov (2011) for critique). In analysing power in this area analysts are "encouraged to attend to *how power is exercised, over whom, and towards what ends"* focussing particularly on "local contingencies of how [regimes of power] are coordinated and the ends they serve" (Haggerty and Ericson, 2006:22).

In this way, the apparatus approach allows us to examine military activity across a wide area. The US military is a huge bureaucracy with a variety of different branches, areas of activity, and institutional norms. Developments are driven by a mixture government policy, battlefield lessons-learned, and *ad hoc* factors ranging from personal charisma to ingrained tradition. In addressing military activity as it coheres around the problem field of Digital Age conflict, the concept of an apparatus allows an approach which begins from a wide view of how the military addresses the problem, focuses down onto the areas where key activity is identified, and examines how these various elements act over the problem field. This allows an analysis of the mixture of concepts, technologies, practices, paradigms, knowledge, and other enablers, to be examined as part of a contemporary propaganda apparatus. We thus understand the military engagement with the politics of information not on *its* terms, but as this engagement relates to our own area of interest.

3.1.3. From Theory to Method

This method is based in the previous theoretical work which draws on the understanding of power as complex and working through a range of practices and relationships; and the outline of contemporary state communication power as requiring a new approach to address a Digital Age information environment much more complex than studies of mainstream media allow. In order to research this area, this thesis examines how the

problem field of Digital Age conflict as understood in US military discourse – giving a conceptual and theoretical unity to a diverse military discourse on adapting to new circumstances. It then examines how a *propaganda apparatus* of practices, technologies, concepts, policies and other elements work on this field to structure new forms of state communication power. This approach allows the thesis to present in-depth research into *military discourse* guiding new approach to digital age conflict. In this context, it then presents the *practical* developments in intelligence, psychological operations, and research & development where the problem field of Digital Age conflict is most thoroughly addressed – describing and examining psychological operations websites, clandestine online engagement practices, and deep links to academic research. This approach allows a coherent and detailed explication of evolving US military thought and practice demonstrating the importance of the these developments, and an analysis which allows us to situate and understand them in their broader social context.

3.2. Overview of the Research

3.2.1. Research Aims

This thesis presents an analysis of how the information and communication practices of the US Military are adapting to the contemporaneous developments of the new context of the more generalised, asymmetric, and population-centric forms of conflict associated with the "Global War on Terror", and the changing information environment of Web 2.0 – what I call, as a shorthand, *Digital Age conflict*. The research draws its methodological and theoretical coherence from an analysis that examines diffuse military practices as they apply to this *problem space*. That is, rather than limit the analysis to one which mirrors formal military processes of development – such as the implementation of policy and doctrine in a linear top-down way, or the development of new training programs to eventually impact practice - this research seeks to establish where and how Web 2.0 is identified as presenting challenges or opportunities to US Military, and then examine developments in these areas.

While the social importance of understanding the development of the most powerful military in the world is self-evident, the fact that the area of interest is the public information and communication platforms of Web 2.0 adds another level to the analysis. The information environment of Web 2.0 is understood as a social space of increasing significance to social, political and cultural life, as well as an important space in which state-citizen power relations are reproduced. As such, beyond examining particular conflict communication practices, the research aims to facilitate broader insight into the impact of changing role of military information and communication practices on contemporary state-citizen power relations, and of Web 2.0 as an important communicative space.

As a study of cutting-edge practice, the research necessarily attempts to hit a moving target. The research presented is not a case study, as there is simply no comparison to be made with developments elsewhere, meaning that analysis must relate to broader social practices in order to situate the findings. As I have introduced an understanding of propaganda free of normative or value judgements, and identified the military practices

the research addresses as a propaganda apparatus, the analytic questions lie beyond any unmasking of propaganda or criticism of instrumental communication. Rather, the analysis draws on the concepts or *power/knowledge, space,* and *population* introduced in the previous chapter, asking: if this propaganda apparatus addresses the information environment in a new way, what are the implications of this for our understanding of this environment, and of contemporary state communication power?

3.2.2. Research Questions

The research addresses the following questions:

- How have the contemporaneous emergence of Web 2.0 and a new paradigm of asymmetric and irregular warfare under the "Global War on Terror" – which I have termed "Digital Age conflict" - been understood in American military thought?

- How has American military practice developed as a result of its engagement with the challenges and opportunities of Digital Age conflict? What are the key areas of activity, and what are the most significant outcomes to date?

- As a secondary question, how do these military developments impact upon our understanding of contemporary state communication power, and of the Web 2.0 information environment as an important space of political and social interaction?

3.2.3. Chapter Outline

These questions are addressed through an in-depth qualitative analysis of developing American military thought and practice throughout the Global War on Terror years, from 2001 until early 2014 (when the research was completed). As Web 2.0 is the area of interest, the majority of the material comes from later in this period, after the technology and terminology gained prominence and influence in the latter half of the 2000s – though writing concerning conflict throughout the GWOT period provides valuable context. Similarly, some of the material used in discussing intellectual trends within the military pre-dates 2001 – this is justified by its demonstrable influence in the contemporary situation.

Chapter 4: US Special Operations and Digital Age Conflict: Doctrine, Discourse, and Changing Paradigms in Strategy and Practice

The first element of the research for this thesis is an analysis of contemporary military thought on the impact of Web 2.0 on GWOT practice. Much of this work has already been presented in chapters 1 and 2, which addressed the strategic context and the changing Web 2.0 information environment respectively. In these sections, I have presented the case – drawing on writing by military and academic theorists on information warfare, GWOT strategy, military doctrine, and other areas concerned with the information and communication-based elements of conflict – for Digital Age conflict as a distinct problem field presenting challenges to existing military communication practices, and to their analysis.

Chapter 4 moves from broader conceptions of the 'problem', to an analysis of discourse which refers directly to ways in which the field of Digital Age conflict is addressed by military actors. This chapter outlines how the area of special operations has become the a key site of activity relating to both the martial challenges of the GWOT, and the communication challenges of the Web 2.0 information environment – drawing on discourse from military strategy, formal doctrine, and statements by influential figures. Developing from an understanding of the important role played by special operators at both the 'sharp end' and the strategic developments of the GWOT, this chapter examines the centrality of special operations thought in the military response to Digital Age conflict. Through examining important intellectual and conceptual developments in the fields of intelligence, information and psychological operations and the area of unconventional warfare, the context, importance, and impact of special operations activity is established. This analysis produces the insight that the "problem field" is not necessarily entirely negative for military actors – presenting significant opportunities for new practices and approaches to emerge, which are studied in the chapters that follow.

Chapter 5: SOCOM, CENTCOM, and the Emergence of a Digital Age Propaganda Apparatus

Having identified the area of special operations as the key site of military response to Digital Age conflict, the research moves on to an in-depth analysis of the practical developments within the US Special Operations Command (SOCOM), focussing particularly on the application of psychological operations to the online information environment, what I call *Cyber PSYOPS* or *CY-OPS*. This is an element of military practice which depends on secrecy or obscurity in order to be most effective. However, research based on analysing open source material allows for the development of a comprehensive outline and analysis of significant developments in SOCOM and the US Central Commands.

Shifting the focus from official doctrinal or structural development to cutting edge military practice allows an understanding of actually existing military activity in this area, and the impact 'on the ground' - or rather, online. An examination of the content and structure of SOCOM-administered regional news websites and their social media presence allows for the development of an understanding of CY-OPS practices in which influence must be studied holistically, rather than as a matter of individual messages or of content specifically. Further, a close analysis of diffuse documentary material produces coherent descriptions of CY-OPS practices previously reported only as mysterious outliers, and the revelation of hitherto un-reported programs, as part of a concerted development within American special operations for cutting edge engagement in the Web 2.0 environment.

Chapter 6: US Military Research & Development and Digital Age Conflict

The final part of the research examines an area of formal military development outside of direct military engagement in the information environment – that of research and development (R&D). The US Military has substantial R&D capacity which funds in-house, industry, and academic research projects in a number of areas. This analysis examines military research focussed on Web 2.0 and identifies key research programmes which have disbursed over a hundred million dollars to industry and academic contractors. Drawing on the significant paper-trail such a contracting and research programme creates

the chapter examines the institutional impetus for the research, key areas of interest, important outcomes, and developing research paradigms.

Studying the area of R&D, which applies military funding to cutting-edge research in areas of identified military necessity, offers important insight into the trajectory of theory and practice within the DOD as a whole. There are important links to developments in both intelligence and communication practices elsewhere in the military. This chapter identifies areas of military research in Web 2.0 influence, the spread of memes in social media, and the study of sentiment, trust, and perception as they relate to online communication. It also demonstrates the influence of military funding and sponsorship in the emerging academic fields of social computing and social media analytics. This analysis of military research allows us to link advanced Web 2.0 study to contemporary developments in military intelligence and PSYOPS practice – completing the circle in offering key insight into the future 'problem space' of cyber-PSYOPS in US military thought.

An approach which builds on an examination of how military theorists construct Digital Age conflict as a problem field and then examines how various elements of military activity and development attempt to act on this space provides the structure for this analysis. The practicalities of this approach are explored fully in the sections which follow.

3.3. Practical Methodology: Hostile Contrast, Dirty Data, and Elite Engagement

Practical considerations shape the research approach almost as much as theoretical ones. The focus of the research on cutting edge US Military practice means that the research approach was necessarily exploratory. The particular situation of the US military – indeed any military actor – as distinct from mainstream society and governed by different laws and norms means that any approach to research in this area is necessarily iterative, exploring what works and what does not in tandem with gathering data and forming an analysis of the area under investigation. State actors in the areas of military and intelligence are not common subjects of sociological research and present distinct difficulties to the researcher which means that studying in this area "challenges taken for granted understandings of the research relationship, and forces researchers to address the interrelated issues of access, methodology, attitudes, and ethics" (Bowman, 2009:2). This section outlines the challenges in this area, and describes the forms of engagement which yielded the data on which this thesis is based.

3.3.1. Hostile Contrast in the Post-Wikileaks Research Environment

In focussing on military communication practices this research is situated within a trend in social research in which the researcher choses to 'study up'. It focuses on groups or individuals who hold great power in society, rather than the more common social science focus on those less structurally powerful than the researcher. The imperative to 'study up' is laid out by Nader who argues that the "democratic relevance of scientific work" is dependent on facilitating the "understanding of the processes whereby power and responsibility are exercised" (Nader, 1972:1). For Nader, "attempts to get behind the

facelessness of a bureaucratic society, to get at the mechanisms" of its operation are vital to understanding social life, and key to investigating important questions of power, responsibility and accountability (Nader, 1972:2). Put simply, the function of 'studying up' is to help us understand what is going on, to empower people to act politically and socially in an informed and constructive way.

Nader's description of the 'faceless' mechanisms of society are particularly relevant in this research context. Flows of communication and information on the internet are much greater in complexity, volume, and opacity than anything hitherto, and much population-centric military activity is hidden from general view. Yet the research shows that mechanisms of power are still very important in determining everyday experience. In attempting to render the practices of military actors transparent and trace developing power relations in Digital Age conflict the research can be seen as in direct conflict with some of the practices and institutions which it examines. This is most clear in cases where the phenomenon studied requires clandestine activity or subterfuge – activities which make up much of the intelligence, psychological and special operations practices examined in this thesis. This approach, as well as the examination of these activities within a concept of state communication power that sees it as structuring power relations between states and broader society, places the research firmly within the area of 'conflict methodology', recognising "the ubiquity of social conflict and change" (Lee, 1993:151).

There is a further sense in which conflict marks the research approach, in that it involves "techniques by which information is obtained from and introduced to systems under conditions of hostile contrast" (Christie, 1971:279 quoted in Lee, 1993:150) – through examining "situations in which powerful groups and organizations deliberately withhold or distort information which would serve the wider public interest" (Lee, 1993:15). In this structural sense, the research is certainly conflictual – much of the data gathered, information examined, and outcomes arrived at are antagonistic to the aims of elite communicators – challenging methods, ethics, objectives, and structures; and shining light where some institutions would rather shadow remains. The smooth operation of an intelligence or propaganda campaign is often dependent on the practices or agents involved remaining hidden, in this sense any form of transparency or research *necessarily* puts the researcher in a structural position of conflict with the institution in question. Thus the conflict approach "rest[s] on [...] adversarial premises, highlighting the inherent conflict between dominant institutions' control of information and researchers' needs to obtain data" (Emerson, 1981 in Lee, 1993:150).

In the political, media, and organisational environment within which this research took place this element of conflict is heightened. The years between 2010 and 2014 have been marked by the rise of the Internet as a social, political and military battleground – with the leak of Iraq and Afghan "war logs" and diplomatic cables by Chelsea Manning, the rise and fall of WikiLeaks, Stuxnet (see Zetter, 2011), Occupy Wall Street, disputes over hacking and internet security, the Arab Spring, the NSA and GCHQ links of Edward Snowdon, and Syrian civil war all providing important examples of the role of the Internet in conflict. Many of these developments have been, at least on the surface, detrimental to state or military power, with the US in particular being damaged by a number of these incidents. In such circumstances, the element of 'conflict' in the research can be seen to be aggravated. It places the researcher on the side of transparency and openness, *de facto* associating me

with the leakers, journalists, and activists who have menaced the US security state over the last four years.

The research approach included numerous requests for interviews, documents and information – both formally through Freedom Of Information procedures and informally via letter or e-mail – with people working in various areas of the US military. The majority of my requests were ignored outright (e-mails never replied to), passed up the bureaucratic chain (usually to Public Affairs spokespeople who gave boilerplate responses), or else rejected on grounds of national security, security clearance, or other bureaucratic technicalities. While I have no experience of "pre-WikiLeaks" engagement with these individuals, it is fair to assume that the reticence I experienced in these responses was due to the contemporary vexed environment concerning all things Internet-related in intelligence and military circles.

There was also a further aggravating factor of my own profile in this field. In the age of Google – and even more so in a field where issues of vetting and security clearance may be a concern - even junior researchers cannot remain anonymous to their subjects, and the reputation or online footprint of the researcher may be key. This was a particular issue in the current research. In the first months I published a comment piece for a political blog on Wikileaks and the US State Department's response which was highly critical of US policy (Revie, 2010, see also Revie, 2012a), the article 'went viral' and was linked to by hundreds of bloggers. It is one of the first things that comes up when you search for my name online (as any potential interviewee with expertise in communication and the internet would surely do). Thus, early on in the research I was 'outed' as a critic of US Internet/foreign policy, an element of the 'adversary' relationship between researcher and subject which must be taken into consideration[26].

However, the 'WikiLeaks effect' also had an upside for the research. Difficulties for my own engagement were catalysed by circumstances (the massive leaks of US military, diplomatic, and intelligence secrets) in which an unprecedented amount of information about US military activity was appearing in the pubic domain, itself providing a rich source of data. None of the leaked datasets provided significant data of *direct* relevance to understanding the research problem[27], however the data and the leaks themselves invigorated a deeply inquisitive journalistic and activist culture regarding US military activity during the research period which provided the 'leads' for a number of the projects discussed in this research (particularly "Operation Earnest Voice" and the Social Media in Strategic Communication programme). This also led to interest in my own research (which was the source for two Guardian articles in 2014, see Quinn, 2014; Quinn and Ball, 2014) which allowed me to make contacts with other researchers in the area and share documents to enrich my own data.

[26] Furthermore, the research project initially intended to study developments in the UK as well as the US, one of the reasons for dropping the UK focus was that trouble I had obtaining access and data due to a reputation within relevant groups of the UK MOD for critical research, and disputes over my use of the Freedom of Information Act.

[27] With the WikiLeaks cables and 'war logs' being too general in relation to military activity, and the NSA/GCHQ leaks of Edward Snowden focusing outside of military activity in the field of intelligence, and offering limited access outside of a select group of journalists.

Furthermore, the difficulties in accessing elites necessitated a research approach which is potentially more appropriate and valid in the contemporary research environment where military activity online is the subject of numerous leaks, hacks, conjecture, and partial information. Lack of individual engagement from the US Military compelled me to take an approach based almost entirely on open source documentary material. Given that many interviews I initially hoped to conduct would have been (and, indeed, those I did manage to conduct were) "off the record" the difficulties in producing verifiable data in such a research environment would have been substantial – dealing with the statements of propagandists with an agenda, speaking in an unattributable capacity in an environment in which their work is severely publicly contested. While not a panacea for transparency, the use of open source material has allowed for the authoritative outline and analysis of organizations, programmes and practices based on verifiable public data, examined at a level of detail even the most candid of interviewees would have had difficulty providing due to the dispersed nature of the activities under study and the practical limits of individuals' experience.

3.3.2. Documentary Material – Dealing with Dirty Data

The vast majority of the data used in the research came from documentary sources, including: policy documents, military doctrine, think tank reports, official memos, blog posts, social media comments, mainstream and specialist media articles, military and broader academia, Freedom of Information requests, congressional and parliamentary testimony, budgetary documents, institutional websites, and academic research papers. Having previously researched a project on the UK Ministry of Defence, I was prepared for a situation in which access to information of relevance would be extremely difficult and the scope of what was in the public domain would be extremely limited. However, I found the US Department of Defense to be, relatively speaking, an open organisation – producing an extensive public paper trail of its activities. For example: the various military academic institutions publish every thesis produced there; almost all doctrinal material is published openly; there are a range of internal military publications on various specialisms; and, many units have public websites or even Facebook pages. I also found it to be a surprisingly helpful organisation: I was sent documents quickly without question after casual requests; public affairs people (even in the area of special operations) were generally as helpful as they could be; I was added to email discussion lists for military research programmes after expressing an interest; and Freedom of Information Requests were (despite being heavily redacted or denied) responded to quickly and efficiently[28].

All data was catalogued and examined, used to produce the analyses, inform interviews, and guide further investigation. The approach taken to this analysis is one of "Investigative Research", described by Miller and Mills as "a means to sift large quantities of data in order to pursue hidden or obscure materials as well as allowing the combination

[28] This latter point represents a major difference from the UK, where the Freedom of Information Act is a very poor means of getting information from the MOD. In my own experience I have had requests delayed for months on end or completely ignored. I have seen evidence of FOI officers discussing my "agenda" in internal discussion of my requests (the identity of the requestor is not, legally, supposed to be an issue in dealing with requests). MOD staff have warned me on multiple occasions that my use of the FOI Act will lead them or their colleagues to deny me any form of access or engagement, and even that it will prohibit me getting a job there in the future.

of disparate evidence to glean new insights into organizations and individuals" (2010:206). The approach draws on Power Structure Research, pioneered by Mills (1959) and Domhoff (1975), and consists of the analysis of networks and structures of key actors, and an analysis of "what is said and done within [those] power network[s]" (Domhoff 2005, in Miller and Mills, 2010:205). The approach is key to the assessment of a large trove of documents from a vast military organisation – allowing the analysis of large amounts of documentary data in search of links, influence, and trends. Within these networks the process of establishing influence is a qualitative one, based on close reading, reference analysis, and the examination of bibliographies and biographies in the search for pertinent links. Texts can be authoritative in terms of how often they are referenced; the influence of the publication the appear in; the institutional context (i.e. doctrine, policy paper, etc.); the status of their author (particularly important within military and state bureaucracies); as well as more contingent features such as being the first work on an emerging subject, or capturing a particular zeitgeist[29].

This necessarily qualitative process is aided by technical tools for the storage and management of documentary data. All data was catalogued digitally using a program called *DevonThink* which renders all documents fully searchable and allows for their organisation in folders with tags. While this is a powerful tool to organise a large amount of documentary data, it is not an *analytic* tool, and the majority of the analysis was done through an iterative process of reading, note-taking and tagging – allowing links to emerge between groups and practices, intellectual and organisational histories to be developed, and trends to be found. This process allowed the generation of broad knowledge in the area and facilitated the drawing of links between documents, individuals, and structures. The collection of all documentary material within a single program also allowed for the identification of substantial and coherent bodies of data which form the basis of the major examples used in the analysis.

The use of documentary material in the area of propaganda does not mean that the study is limited to engagement with only secondary or historical material. The example of the PSYOPS websites run by SOCOM in chapter 5 shows an engagement with text-as-practice: the examination of a web page, blog post, YouTube video, or Twitter feed as an example of *the activities* of those whose medium is communication. Documentary material in this case is not a trace or a representation of the practice under consideration, it *is* the practice. As with all web-material used in the data, every page referenced (as well as relevant pages which support the analysis but are not included as individual references) were captured as PDF documents with time-stamps in case pages were changed or removed from the Internet, and as PSYOPS media content its relevance and validity is clear. It is actually the other documentary material, which is a trace or representation of practices under analysis, and allows us to understand and examine developing military structures and practices, that requires deeper discussion here.

The utility of documentary data most interesting in a conflict research situation has been best outlined by Gary Marx (1984), who provides a conceptual framework for talking about documentary data which he categorises as 'hidden or dirty data'. Hidden and dirty data are defined as "information which is kept secret and whose revelation would be

[29] Throughout this thesis the rationale for claims of influence is explained in cases where it is not clear from the context.

discrediting or costly in terms of various types of sanctioning" (Marx, 1984) – and their analysis has been found to be useful in studying contemporary military and intelligence practices (see e.g. Miller and Sabir, 2012; Monaghan and Walby, 2012). This definition needs to be refined in the case of the research context where the discredit or cost does not lie in the exposure of an *individual* piece of data, but in producing insight from examining and cross-referencing large quantities of such data. What we are interested here is not the 'smoking gun' or the big leak, but the collection and analysis of many official and unofficial sources, innocuous press releases or budgetary items, in a manner which makes "revelation" possible. In most cases, the revelation of the data is not *directly* discrediting or sanction-inducing, instead seen in the conflict paradigm it is damaging to the practice of propaganda, adding an extra element of resistance to the process.

For Marx, the ability to uncover hidden information in such situations depends on a variety of complex organisational, technological, and legislative processes. Social scientists need to adapt such processes to their own purposes. Dirty data makes it into the public domain in four broad ways, which Lee, in his overview of Marx' work, summarises as: (1) unwitting disclosure or deception; (2) enforced disclosure, or legal processes; (3) volunteered disclosure, or whistleblowers; (4) uncontrolled contingencies, or by accident (Lee, 1993:154-155). I found that all these forms of disclosure produced useful data: the unwitting disclosure of information by participants at military conferences which I attended 'talking shop' in presumed closed environment; the enforced disclosure of legal requirements to publish contract material and FOI data; the volunteered information of thousands of military employees and contractors via social media; and the "uncontrolled" spill of information through vast networks of military websites and organisations which means important documents leak out.

The category of data gained through uncontrollable contingencies is interesting, referring to opportunities for data collection as a result of accidents or failures in control where events conspire to make the unknown known. Lehmann and Young (1974) call these "technological accidents": "unplanned events which reveal the inner workings of large scale organizations which by mistake or miscalculation caused a breakdown in the conception of public order" (Lehman and Young, 1974:24). An almost paradigmatic example of this is the exposure by hackers of a US military PSYOPS project to create fake online commentators ("sockpuppets") through a project initially reported as being called Operations EARNEST VOICE (see Fielding, 2011), which was uncovered only when the CEO of a potential contractor spoke unwisely about the Anonymous hacking collective, incurring their wrath in the form of the theft of his company's data – which happened to contain details of the clandestine project (Bright, 2011). This type of disclosure can offer a wealth of interesting data, however a reliance on this data in isolation risks a situation where "research agendas [...] become shaped by events rather than by a systematic logic, and research studies do not cumulate (Lundman and McFarlane, 1976 in Lee, 1993:156). This is true if such contingencies are taken alone, however the research strategy presented here is a situation in which such knowledge accumulates within the project itself and is cross referenced with other material. When the data leaked by Anonymous was combined with the 'legal' disclosure of Senate testimony by key military figures and budgetary material; the further 'enforced disclosure' through my use of the FOIA Act to obtain documents from US Central Command; and 'volunteered' information found in the online CV's of military contractors - a much fuller understanding of the programme in

question could be developed (see section 5.5.1). Importantly, this use of other information to put this disclosure into the proper context meant it became an element which enlightened and enriched the broader analysis, rather than 'shaping' it around a particular example.

In the age of Web 2.0 'emergence' and 'mass-self communication' a key form of data disclosure is that of volition – that where "whistle-blowers, informants, and overt participant and non-participant observers share in the willing provision" of information of use to the research (Marx, 1984). Marx writes for example of the use of memoirs, biographies, and letters. What was most notable in this research, however, was a new form of self-disclosure: social media. Individuals volunteer a huge amount of data about themselves online: in blogs, through social media profiles, and sites linked to their jobs. In some cases this data can be examined to gain information which could not otherwise be obtained. For example, the DOD will not list details of those serving in certain military units, yet a search of the career networking site LinkedIn provides a long list of those who claim membership of them, with some even listing locations and dates of service. On a smaller scale, seemingly innocuous data which individuals post online – personal or career information, opinions on comment sites, links to colleagues, CVs – can be analysed in a way which allows insight into particular networks to be gleaned through cross-reference with other data. Marx calls this category of data "give-aways", where information has latent interest and only with analysis, cross-referencing, or future-disclosure does it become pertinent – a situation with interesting parallels to the "archive of unpredictability" seen as menacing official communicators in the Web 2.0 environment discussed on page 34.

The information source which underlines the communication challenge to government in the Information Age – that of hacked and leaked data – falls somewhere between volition and uncontrollable contingency. The mega-leaks for which Wikileaks have become known of military and diplomatic cables, as well as the e-mail logs released by Anonymous of private-security companies (see Ball, 2012) represent leaking on an industrial scale. All data in the public domain was considered legitimate research material – and that from both WikiLeaks whistle-blower documents and Anonymous hacks was used in the analysis. The example of hacking is, of course, based in deception - though this is not a category of Marx's dirty data which is pursued in the study due to ethical reasons, as well as the pragmatic considerations that deception (for example misrepresenting oneself or one's aims) could backfire and seriously hinder any form of engagement and inhibit future research. Deceptive research is, in circumstances which require elite engagement, scorched earth research. All approaches to military actors or other potential sources of information were fully transparent, I gave my name and background, and told officials I was carrying out PhD research into "the adaptation of military communication practice in the age of Web 2.0". This approach led to a surprising amount of disclosure (being added to military discussions lists, sent unpublished documents which helped understand the Strategic Multilayer Assessment program, etc.), underlining the importance of building trust and credibility with subjects.

Another category of Marx's, coercion, however, is a research strategy which was very useful in the research. One of the benefits of studying the powerful is the opportunity to make use of the formal levers of accountability – it is ethical to coerce militaries into

carrying out their legal obligation of accountability where it would not be to coerce civilians into engaging in academic research. We can see examples in the ruling on the publication of the Tobacco Archives as a key example here (Hammond and Rowell, 2001), and in legislation on freedom of information and transparency (Brooke, 2006). In this case, the Freedom of Information Act (FOIA) (see EFF, 2014 for a discussion of the Act's powers) was used to request information from United States Central Command, United States Special Operations Command, and the CIA – only in the first case was information released, and it was heavily redacted, but it provided verification for the existence of a programme spoken of only fleetingly elsewhere.

All the categories of data described above are highly reliant on contingencies such as bureaucratic arbitrariness, whistle-blowers, hackers, and individual carelessness. As such, the reliability of *an individual piece* of documentary data in itself, is relatively low. There is potential that it is fraudulent, wrong, simply nonsense, or was made available in order to deceive. Indeed in the area of US military propaganda there are a huge number of conspiracy websites, which makes cross-referencing and studying the provenance of documents or claims particularly important. This being the case, the process of investigative research described in this chapter produces a research structure in which the validity of an individual piece of data is a function of how it coheres with the larger picture developed using a large set of diverse data. This process relies on constant cross-referencing, exploring how documents, individuals, institutions, organisations, and activities are related through their documentary traces. This is a familiar process in its relation to how many works of history are produced, the difference is that in the context of the research these process are examined in flux, as living practices which are understood not just through their documentary traces, but can also be reflexively examined. As such all efforts were made to contact public affairs spokespeople, authors of papers, bloggers who made specific claims, journalists who wrote articles of interest, in order to follow up on open source information and assess its credibility and validity.

3.3.3. Interviews, Conferences, and the Importance of Triangulation

To supplement the documentary analysis, the research also engaged with military practitioners on a number of occasions[31]. Although I have commented upon the closed nature of the elites studied, it must be noted that those who engaged with the research did so openly, sometimes even enthusiastically, and their engagement was highly valued. Significant non-documentary research in this project comprised: attendance at two annual "Information Operations Global" conferences in 2012 and 2013; one conference of academics, diplomats, activists, and public diplomacy specialists in 2012 (see Revie, 2012b); an e-mail interview with the head of the US State Department's Center for Strategic Counterterrorism Communication; off the record interviews with two UK-based PSYOPS practitioners; attendance at two UK MOD conferences on "cyber influence"; and a visit to the headquarters of the UK MOD's 15 Psychological Operations Group. While the UK-based engagements could not, for obvious reasons, directly address the specifics of US developments, they allowed the development of a deeper understanding of the context of

[31] This is the only time human subjects were involved in the research, for which ethical clearance was obtained from the Universities of Strathclyde (where this research began) and Bath (where I transferred in the middle of the research).

contemporary Western information operations practice. Indeed, the overall benefit to the research of all engagements does not lie in any particular revelations, but in their utility in building a general familiarity with the area and ease in discussing various organisations and practices. In allowing engagement with the human actors behind terms like "psychological operations" and "information warfare", it demystified their activities and allows the analysis of documentary material to be grounded in a real-life engagement with those who work with and produce such discourse.

Given the limits on and difficulties of engagement with military elites it is imperative that techniques are adopted to get the most out of each interview. In order to do this it was necessary to 'foster mutuality' (Kezar, 2003:407): a process that included thorough pre-engagement preparation and consideration of the dynamics of and approach to the interviews themselves. Preparation is a key part of any interview, but there are particular elements of elite engagement which make the preparation process distinct. In order to optimise the data gathered from interviews and conference attendance, these occasions were always preceded by preparatory research into the subjects "background, life history, published views", affiliations, career paths, and the like (described by McHugh as "remote preparation" in (Philips, 1998:9)). As well as reading everything by and about subjects, preparation also often included research into their social media presence (e.g. Twitter, LinkedIn, blogs, media articles) as a means of gauging their range of experience, activities, and interests. This is a form of interview preparation which will no-doubt become the norm in elite interviewing (and much non-elite interviewing), but which is not addressed in the existing literature.

Familiarity with the milieu of subjects was developed through preliminary research, in recognition of the fact that elite subjects "are likely to respond to an interviewer who appears to know about their world" (Williams, 1989:267). This applies to institutional as well as personal knowledge – for example familiarity with military and diplomatic protocol and customs, endless acronyms and bureaucratic distinctions - as well as in depth knowledge of the subject under discussion. In this way the interviewer should try and cultivate the position of "quasi-expert" because "the thematic competence of the interviewers is a necessary condition for a successful expert interview" (Pfadenhauer, 2009:86). Thankfully, the researcher is not thrown into this situation blind, and in this case all elite engagement took place in a context in which (*at least*) a quasi-expert familiarity had been developed during the production of the research.

The process of elite engagement itself also requires consideration of a number of aspects related to an elite focus. All engagements conducted for this research can be categorised as unstructured interviews – or "conversations with a purpose" (Burgess 1984, in Philips, 1998:8). This flexibility was necessary due to the diverse backgrounds of the interviewees as well as the need to "use the interview for what it is" (Berry, 2002:681) - to tailor approaches to particular individuals, for example interviewing an ideologue can give great insight into the arguments driving an issue, while a technocrat can allow the development of knowledge into the structures and process involved which might otherwise be overlooked.

A key consideration in dealing with elite data is that in some situations, such as engagements with military institutions reticent to engage, "information is not usually given freely" (Williams, 1989:266). This applies equally to documentary and interview

data. It is thus important to scrutinise the "motives behind informants' actions" (Williams, 1989:266) – which can range from rivalry, to a belief in the importance of the inclusion of a particular piece of information, to subterfuge. This requires that the research develop a deep circumspection in dealing with data and "an insider's knowledge" of the institutions and individuals under study – the better to understand potential motives and interests (Williams, 1989:266). Researchers must recognise that "it is not the obligation of a subject to be objective and to tell us the truth" (Berry, 2002:680) – on the contrary, it is the job of the researcher to account for such biases and reflectively deal with them in the research. While interview data usually has higher validity – in that it is collected to fit the needs of the research, it is often less reliable, being more prone to distortion of memory, personality or deception (Davies, 2011:77). Furthermore, in terms of published documentary material in the research area, which is highly contested and scrutinised, the publication of falsehood is more likely to be exposed, whereas interviews (especially those 'off the record') face no such sanction.

The problem of being misled by either elite subjects or documents, or on a more personal level of relying on one author or interviewee's perspective over others because of non-epistemological reasons such as charisma (Berry, 2002:680), can be guarded against through a transparent and clear explication of why certain conclusions or inferences have been drawn in the analysis. This includes not shying away from ambiguity or uncertainty, by being clear and open where such issues exist. For example in relation to CENTCOM's classified Regional Web Interaction Program – I have been clear about the limits of data and the basis of inferences. Indeed throughout the thesis, all claims of influence; references to particular programmes, concepts, or events which are not well known; and any contentious claim is referenced in a way which allows the reader to check these data and inferences themselves.

The importance of the process of triangulation is especially important when studying an organisation like the US military which is vast, diffuse, and produces a huge amount of documentary data. This means that one can find documents to fit almost any narrative. One illustrative example is the vast trove of MSc theses published by the various military academic institutions – these are produced by military students and are often of a poor standard, and it requires thorough investigative research to separate the quirky but irrelevant (such as those which advocate "cyber herding" to trick terrorists into fake chat rooms (Moon, 2007); sending soldiers disguised as Arabs into the online world of Second Life (Benson, 2010); or remotely changing terrorists leaders' mobile phone ringtones to "God Bless America" to cause shame (Keller, 2010b:5)[32]) from the genuinely important (such as one by the future-head of SOCOM's main PSYOPS unit (Bostick, 2011)). This is particularly important in the case of subjects such as PSYOPS and military intelligence, where spooky language and weird ideas are commonplace, but the understanding of actual practical developments require more nuanced engagement with the material. Without a process of triangulation emphasis may be given to particular publications or events which are largely irrelevant in reality.

In respect to the question of reliability, the research was aided a great deal by the breadth of the research field and the investigative research approach which takes in data from a

[32] None of these individuals went on to significant positions in PSYOPS, and none of these ideas are repeated in any other documents.

very wide range of (often unrelated) sources – meaning that off the record interviews were used to clarify and build upon information about networks, processes, and content found elsewhere in documentary data. In this sense elite engagement and documentary sources provided verification for each other: the true influence of documents could be established (e.g. did anyone concerned with policy actually read it) and elite engagement could point in the direction of new documentary data. For example: one of the key examples in chapter 5, the Facebook page of the *Southeast European Times,* was the subject of a popular presentation at Information Operations Global 2012, which in turn supported statements about new approaches to online engagement made by interviewees. The process of triangulation of data through this cross-referencing is thus cumulative as well as corroborative (Davies, 2001:75) – allowing the development of a data set which was enriched and validated through the identification of new relevant information throughout the research process, guiding searches or requests for further information and building an understanding of all relevant areas of activity and their context. Combined, these methods allowed the collection of a considerable amount of data upon which to base the analysis, which is referenced throughout this thesis as a verifiable paper trail supporting the research presented and claims made in the thesis.

3.3.4. Investigative Research, the Military, and the Digital Age

This approach is deeply embedded in the particular time in which the research was conducted: reflecting the WikiLeaks-era of investigative journalism and engagement with leaked official data; harnessing the potential of the prolific (and arguably ill-advised) use of Web 2.0 platforms by many military employees and contactors; benefiting from the relative openness of military discourse which characterised the COIN era in US defence thought (see e.g. Ricks, 2009); and taking advantage of a situation in which the military organisations themselves has been necessarily open in inviting academics, the private sector, and (to a much lesser extent) publics to help them come to terms with the challenges of the Digital Age. This latter point is evident in my own attendance two years in a row at the largest global Information Operations conference, and in the data in chapter 6 which documents an extensive R&D programme to prepare the US military to Digital Age conflict.

Being situated in such a time also means that an investigative research approach has been necessary in allowing the incorporation of new material which emerged during the research period. Much – perhaps the majority – of the material studied was published after the research began, and the data includes references which were incorporated right up until the writing-up of the thesis. This complicates the traditional linear research approach of studying the literature, assessing the best methods, and then getting out and collecting data. However, the difficulties of trying to hit a moving target are balanced by the degree of access such contemporaneous research allows to the data. I attended a conference at which the major Facebook campaign of SOCOM's *Southeast European Times* was first presented to the information operations community, and witnessed a workshop in which a number of conference attendees (including some American generals) went on a *Foursquare* treasure hunt around Central London – providing first hand experience of an institution in flux. This contemporaneity also allowed the examination of PSYOPS websites through a *real time* immersive analysis, allowing key insight as many social media sites are

not built with posterity in mind, and become harder to analyse as time passes. As this research argues, such a nuanced and active engagement with state communication practices is now a necessity in examining how state and militaries act in, through, and on the Web 2.0 information environment.

In presenting a new approach to both theorising and examining propaganda practices this research attempts to push analysis of state communication power into the Digital Age. The success of the research shows that an investigative research approach, harnessing the myriad data sources of the online and offline world, can shed significant light on an area of institutional change often presumed to be inaccessible to outsiders. The approach to validity through triangulation, the consistent referencing (and cataloguing) of all data, and explication of claims of influence and inference is one which recognises that the temporality of the research requires rigorous introspection as well as documentation. In this sense it is the responsibility of the researcher here not only to analyse but *to document,* an approach which is shown to bear fruit in the following chapters.

4. US Special Operations and Digital Age Conflict: Doctrine, Discourse, and Changing Paradigms in Strategy and Practice

4.1. Special Operations, Doctrine, and Military Discourse

This chapter examines how US military strategy, doctrine, and discourse address the problem field of Digital Age conflict, with a particular focus on discourse within the area of US military special operations and associated developments in information operations (IO). Sections 1.3 and 2.3 have already drawn on US military doctrine, statements by policymakers, writing by military-linked authors, and other texts to thoroughly describe how the military and Web 2.0 aspects of the problem field are understood and discussed. This chapter narrows the focus, concentrating on special operations and IO discourse in order to explore work which bridges the gap between the broader understanding of Digital Age conflict and the practices, technologies and structures at the cutting edge examined in this thesis. The chapters which follow present special operations activity as the main area of development of Web 2.0-based communication practice, as well as a number of important ideological and practical links between special operations, intelligence, and R&D in the research area. As such, a particular focus on how the problem field is addressed within special operations thought offers key context for what follows and allows the analysis to progress from the problem field understood *as a problem,* to how it is formulated in discourse in a way which directly *addresses* that problem. This is a process with tangible outcomes on military practice and development.

This chapter begins by describing the role of US special operations in the GWOT – demonstrating its influential role through central involvement in covert commando missions which influence contemporary military practice, and a broader strategic position as the key means of coordinating global DOD activities against irregular adversaries (terrorists, insurgent groups, etc.). Both of these roles have key implications for the way the problem field of Digital Age conflict is understood and addressed – influencing intelligence and IO practice across the military, and guiding the strategic paradigms which shape the emerging approach to the GWOT. Emerging thought and practice in intelligence and IO (with particular focus on the area of psychological operations) are examined in detail – with particular attention paid to the work of military thinking under the emerging paradigm of "information engagement". The chapter concludes with an examination of the special operations area of 'unconventional warfare', where cutting-edge military discourse has most directly addressed the potential of Web 2.0 in operations – identifying a key area of interest and underlining the potential *opportunities* for emerging forms of military practice in the new strategic and information environment.

In exploring these more pro-active approaches to Digital Age conflict this chapter draws particularly on military-produced material: doctrinal publications, quasi-doctrinal material (such as service handbooks, training materials, and *ad hoc* policy statements), texts by think tanks and key special operations figures on developing policy, academic and journalistic studies, and a variety of other sources. In some respects, the construction of a problem field within military discourse is very formal: with a broad conception of threats and strategic priorities laid out in policy statements and strategic guidance (e.g. DOD –

QDR, 2010; DOD – *Defense Strategic Guidance,* 2012; DOD – *Information Operations Roadmap,* 2003) which guide doctrinal texts which form the discursive backbone of military development and activity. Doctrine lays out the military view of conflicts which the US may engage in; it describes the "operational environment" for military activities in order to identify essential tasks (e.g. DOD – *JP 3-0,* 2011), areas of responsibility, and domains of conflict; it defines concepts and entire lexicons for the coherent discussion of specific topics (e.g. USAF – *Functional Concept for Cyberspace Operations,* 2010:41-52); sets out the organisational responsibilities of staff in each element of warfare (e.g. DOD – *JP 3-13,* 2012); and it describes specific approaches for all elements of combat. All doctrine which touches on the contemporary information environment has been examined here[33], with almost all material of interest lying in the area of information operations and intelligence[34].

However, the body of doctrine is not a cohesive and decisive tool – there are gaps, contradictions, and it develops in only a semi-coherent way. While formal authority in doctrine is fairly linear, working hierarchically from directives from the Secretary of Defence, through top-level "Joint" doctrine, to individual service (i.e. Army, Marine Corps, Air Force, and Navy) publications, this formal authority does not directly correspond with broader influence over military practice and though. An example of this is that the most significant doctrinal document of the Afghan and Iraq wars was the Counterinsurgency Field Manual (US Army/Marine Corps - *FM 3-24*, 2006), which was developed by the Army and Marine Corps and was aimed at providing operational and tactical guidance. The publication was more widely influential because it was supported by influential commanders and ideologues, and because it captured a zeitgeist in changing military thought and catalysed significant debate, discussion, and development throughout the military (see Ricks, 2009; Miller and Mills, 2010; Network of Concerned Anthropologists, 2009).

This less formal type of influence is also found outside of the area of formal doctrine. In the area of special operations, the cases of General Stanley McChrystal and Lieutenant General Michael Flynn who gained prominence running the 'shadow war' in Iraq and Afghanistan through the Joint Special Operations Command and used this influence to promote changing paradigms and practices in operations and intelligence shows the importance of key figures and experience forged in war in driving change. There are also a number of lower-profile commanders and instructors (e.g. Mayfield III, 2011; Murphy, 2010; Caldwell IV, 2009; Arquilla, 1997; Kinniburgh and Denning, 2006) in the area of

[33] All non-classified (the only classified document of potential interested was *JP 3-12, Cyberspace Operations*) doctrine in the areas of Information Operations, Intelligence, and Cyber – as well as Joint doctrine which more generally describes the operating environment (DOD – *JP 3-0,* 2011; DOD – *JP 2-01.3,* 2009) was searched for the terms "media", "Internet", "online", "Web", "social", "psychological", "cognitive" in order to identify sections of interest. As noted in Appendix A, "Cyber" refers purely to technical aspects of US military online engagement so is not discussed in detail.

[34] There is significant Web 2.0-related discussion in documents relating to Operational Security (OPSEC), which offer soldiers guidance on using social media in a manner which will not allow potential enemies to locate them or their families or otherwise threaten military security (through disclosing troop movements, base infrastructure, etc.). This type of material (e.g. see US Army Office of the Chief of Public Affairs, 2011; The Social Corps, 2011; Moe, 2011) does not directly address impact on audiences and is also very basic and self explanatory, so is not given significant attention here. The challenges to OPSEC of military engagement with Web 2.0 have been addressed in a number of academic studies (see, e.g. Lawson, 2013; Brunner and Dunn Cavelty, 2009; Knopf and Ziegelmayer, 2013).

training and education who have been influential in driving developing Web 2.0 practice and thought due to the prescience of their analysis, and by addressing these issues at times where their salience was greatly increased due the rising concerns about the challenges of Web 2.0 to military activity. As such, this section draws on doctrine as well as broader military writing – tracing links between the two and describing a discourse which draws on the challenges of the problem field, but moves toward a more direct address of the area, forming the foundation for understanding the practical developments examined in the chapters which follow.

4.2. JSOC's Shadow War and the 'Death Star'

The role of special operations (the area beyond conventional military activity which includes covert operations, missions behind enemy lines and in undeclared warzones, liaising with proxy forces, special reconnaissance, and assassination) at the intellectual level of military development cannot be separated from its key role at the operational level, at the 'sharp end' of the GWOT. Through the commando activities of the Joint Special Operations Command (JSOC) and the broader strategic role of the US Special Operations Command (SOCOM), special operations activity has played a mostly covert but always crucial role in the conflicts since 9/11. This period saw not only the elevation of SOCOM into the most lethal and capable arm of US military power, but laid the ground for its increased influence in developing military strategy and practice, and key institutional influence in developing concepts and paradigms in Digital Age conflict (Scahill, 2013; Ambinder and Grady, 2012). A short examination of the practical role of special operations in this period provides important context for understanding its intellectual and strategic influence.

Perhaps the most remarkable thing about the influence of special operations is the divergence between the relative secrecy of its activities and the significance of its impact – nowhere is this clearer than in the rise of JSOC in the 2000s. While the rise of counterinsurgency as the military theory *du jure* in the latter half of the 2000s has had demonstrable impact on developing military thought and practice with the "population-centric" approach becoming the key narrative of the Iraq and Afghan wars; behind the niceties of "hearts and minds" and the cups of tea with local elders in Iraq and Afghanistan another war was being waged. Simultaneous to the 'soft' COIN approach was a very 'hard' shadow war, focussed on the killing or capturing of insurgents by coalition special forces in an accelerated form of counter-terrorist targeting. In Iraq and Afghanistan (and in other peripheries of the GWOT including Yemen, Pakistan, and Somalia) JSOC – a sub-command of SOCOM focussing on counter-terrorism operations – run in relative obscurity, an "almost industrial-scale counterterrorism killing machine" (Nagl, in Niva, 2013:186) with its own integrated intelligence and operations capacity, conducting thousands of night-time raids on alleged insurgent targets (see Urban, 2010; Ambinder and Grady, 2012; Scahill, 2013; Schmitt and Shanker, 2011).

This approach evolved within the post-9/11 culture in US security and military circles that exceptional measures were required to fight terrorism. JSOC was built up from 1,800 personnel in 2001 to 25,000 by 2011 (Lindsay, 2013:441). It became *the* key organisation

running commando operations against insurgents in Iraq (from mid-2004) and later Afghanistan[35] – conducting hundreds of raids a month and killing or capturing an estimated 11-12,000 people (of whom around 3,000 were killed between 2003 and 2009 (Urban, 2010:71)). JSOC also conducted drone strikes and raids in undeclared warzones with no accountability other than to the executive branch, operating effectively as a secret paramilitary force (Wolf, 2013; Scahill, 2013). Yet during the peak of the Command's activity in Iraq the 2004-2009 period it managed to remain largely anonymous in media and political discussion – allowing the 'hearts and minds' COIN narrative to become pervasive - despite having a "less than 50%" success rate, providing "little information about civilian casualties" (Priest and Arkin, 2011:22), and running its "own detention and interrogation centres, where accusations of torture and abuse were raised" (Niva, 2013:193).

This divergence of obscurity and impact is interesting in light of the links between technology, communication and conflict in the context of Digital Age conflict and the RMA discussed previously. JSOC's success in remaining anonymous is attributable to GWOT-era classification, and operations such as night-raids which are *by their nature* inaccessible to scrutiny[36]. The speed and precision of JSCO's operations is also a function of the Command's technological mastery, such that Lindsay argues its operations represent a contemporary application of the RMA-vision of military autonomy through anonymity, seeing its success[37] as achieved through the use of advanced technologies and an adapted version of RMA 'network-centric' thinking (Lindsay, 2013:422-423). For Lindsay, JSOC's activity represents the zenith of the "conflation of RMA and COIN", using the "bestiary of technology" from drones to eavesdropping equipment and stealth weapons to achieve great success in kinetic operations in the "midst of a paradigmatic 'population centric' fight" (Lindsay, 2013:423). For a time at least, JSOC, with the help of the popularisation of the 'hearts and minds' narrative perpetuated by the conventional military and most media and analysts, circumvented the "counter-Revolution in Military affairs" and used advanced technology and concepts to successfully run 'hard' military operations largely free of scrutiny.

In time, in overcoming the perceived limits of both population-centric warfare (the need to win 'hearts and minds' in the warzone and at home) and kinetic enemy-centric approaches (a casualty-aversion and potential 'blowback' from the application of extreme violence) the JSOC approach was lauded within the military and in much reporting (see e.g. Schmitt and Shanker, 2011), particularly after special operators killed Osama Bin Laden (Schmidle, 2011). It also thrust its key architects to prominence, with JSOC commander Stanley McChrystal and his intelligence chief Michael Flynn becoming particularly influential in developing GWOT discourse. In widely-read and referenced articles they outline how JSOC looked at the networked nature of the insurgency and

[35] When former-JSOC commander, Gen McChrystal was put in charge of the Afghan war, night raids rose from 20 to 600 a month (Niva, 2013:196).

[36] They take place at night, are geographically diffuse so victims families or journalists do not know where to go for information, they are fast and often leave little trace - in one infamous case JSOC forces even removed their bullets from an innocent family they killed before leaving the scene (Scahill, 2013:334-347). For this reason JSOC operators are often referred to as 'ninjas' (Kelly, 2013)

[37] Success, that is, in its own terms: killing and capturing suspected insurgents and building its capacity, institutional power, political support and prestige.

understood it would "take a network to beat a network" (McChrystal, 2011), bringing together intelligence analysts, special operations commandos, surveillance specialists, mapping experts, linguists and others under one roof to work collaboratively without bureaucratic constraints to rapidly speed up the process of targeting and running kill-or-capture missions (see Flynn et al, 2008; Urban, 2010). The command centre they created – bringing together advanced intelligence and elite commando units empowered to strike rapidly without traditional oversight - became known as the "Death Star" due to the "sense that 'you could just reach out with a finger as it were, and eliminate somebody'" (Scahill, 2013:162). Thus RMA technology was put to work not to manage an entire battlespace as originally envisioned (where the "just in time" logistics metaphor was used), but to facilitate lethal small teams of intelligence analysts and commandos (McChrystal was fond of referring to non-hierarchical McKinsey management science techniques (Urban, 2010:34)) who wielded the technology like a scalpel, removing 'bad' actors from the broader COIN operating theatre.

Kill-or-capture missions also included on-site intelligence collection and exploitation (from electronic devices, personal possessions, pocket litter, etc.) as a vital element, meaning that intelligence and operations apparatuses became highly integrated within JSOC, often with "intelligence recovered on the spot … instantly pushed digitally … to analysts who could translate it into actionable data while the operators would still be clearing rooms and returning fire" (McChrystal, 2011). Intelligence was further enhanced with extensive use of drone surveillance, interrogation, and developing "nodal analysis" which exploited intelligence about the "infrastructure" of enemy networks (locations of funders, meetings, media, headquarters, or weapons caches) and other data which was collected to allow networks to become "more visible and vulnerable" (Flynn et al, 2008:58). This intelligence would in turn lead to more raids – sometimes even in the same night, in a sort of snowball-targeting process. This integrated intelligence capability became so important to JSOC that Flynn argued it could no longer be distinguished from operations, rather "intelligence *is* operations" (Flynn et al, 2008:56).

The story of JSOC provides a couple of important insights for proceeding in the analysis of Digital Age conflict. Firstly, it highlights the continued importance of understanding the relationship between communication, technology and military practice in drawing our attention to the role of advanced technology in limiting scrutiny of a decisive element of the GWOT (Lindsay, 2013). This compels us to look beyond the public perception of conflict, as well as that which is articulated in conventional military statements and doctrine, to what highly empowered special operations actors are doing. It also demonstrates the importance of a holistic understanding of military activity – the COIN approach cannot be understood properly without an appreciation of the role JSOC's "industrial-strength targeted killing machine" played in cutting through insurgent networks behind the scenes (Lindsay, 2013:447). Neither can the JSOC approach be understood without an appreciation of the role the COIN narrative played in obscuring the more violent elements of coalition military activity. Secondly, we must aim to produce a holistic understanding of particular military approaches – with the role of intelligence in supporting JSOC's 'death star' being key. As we will see, though this role was developed by Flynn for JSOC, when the strategic context of his job moved – first to the 'conventional' Afghan COIN theatre, and then to the more general level of military intelligence as head of the Defense Intelligence Agency – the approach to intelligence changed such that

'intelligence *is* operations' can be seen not just as a JSOC mantra, but one which guides intelligence support to many different types of operations. Later I demonstrates how Flynn's JSOC-derived influence has translated to influential advocacy for new forms of intelligence being applied to special and psychological operations in the contemporary information environment.

4.3. SOCOM and the Indirect Approach

JSOC is just the most prominent and spectacular element in the broader development of the US Special Operations Command as key in the GWOT. As the command which oversees irregular warfare and other specialist military missions, SOCOM is known as the "tip of the spear" of DOD operations. While all other military combatant commands [38] have geographically-bounded areas of operation, SOCOM's area is global. As such, SOCOM has assumed a key role in the GWOT of coordinating and pursuing the fight against 'global terrorism'. This role is understood through a paradigm known as the "indirect approach" (Comer, 2010) and is set out in the DOD's Campaign Plan 7500 (CONPLAN 7500) which guides GWOT strategy, and puts SOCOM at the heart of a military-political approach which incorporates the use of US power in an indirect way to "shape" and "stabilize" the "Global Environment" to make it less hospitable to terrorist recruitment, funding and activity. This plan is outlined in the slide in Figure 1 and is known as the in the US military strategic community as simply "the GWOT slide", which "appears in almost every briefing" given by SOCOM "to explain the necessary actions in the GWOT (Comer, 2010; Olson, 2008:8).

Figure 1: The "GWOT Slide", outlining the "indirect approach" to GWOT strategy

[38] Apart from Strategic Command which focuses on cyber and space warfare, and Transport command which focuses on logistics

In this plan, SOCOM is designated both as key strategic coordinator and special operations practitioner, it is to act in a direct way upon the enemy in the form of more or less traditional military action (and, as we have seen, through JSOC's commando raids, drone strikes, etc.); as well as through 'indirect means' – including working and training other nations' forces (see e.g. Turse, 2012; Khalili, 2013), and pursuing the ideological goals of "deter[ring] active and tacit support of [violent extremist organisations]" and "erod[ing] support for extremist ideologies". This identifies SOCOM as the key actor in psychological operations in the US military, within a broader approach which conceives of conventional and unconventional military action as part of a coordinated approach to attack both 'violent extremist organisations' and their presumed ideological and logistic support bases.

In a hearing on the role of SOCOM in 2010, then-commander Admiral Olson described SOCOM as the "lead synchronizer for countering violent extremism" encompassing both "kinetic and nonkinetic efforts" (that is, violent and non-violent) (Committee on Armed Forces - *DOD Appropriations Hearing for FY2011*, 2010:818), and that SOCOM strategy "reflects the primacy of indirect approaches" and of "ideologically-based activities", the lynchpin of which is the "Expanded Trans-Regional Psychological Operations Program"[39] which guides regional PSYOPS in support of the indirect approach. The main elements of this program are the provision of regional "Military Information Support Teams" deployed around the globe in US embassies (discussed in section 5.4.3), and a number of "regional influence web sites [which] counter Internet-based misinformation supporting extremism, while synchronizing DOD's web-based messages on CVE topics" (Committee on Armed Forces - *DOD Appropriations Hearing for FY2011*, 2010: 819). These websites – a program which has more than doubled in size since Olson's testimony - form the largest element of DOD online public engagement, and are examined in section 5.3.

The importance of the "indirect approach" lies in understanding the way CONPLAN 7500 conceives of the application of the precise, extreme violence of JSOC as part of a holistic strategic approach which addresses what as seen as a global ideological and political conflict. It incorporates 'softer' elements including cooperation with other militaries, political and social programmes, and PSYOPS. This sees the parallel JSOC and COIN campaigns in Iraq gone global – demonstrating a holistic ideological *and* kinetic campaign which, in the case of the 'indirect approach', is organised through a command which has control of the most advanced kinetic tools and the most advanced psychological operations apparatus to match. Being global in nature means the indirect approach sees military power being applied outside of declared conflicts – in such cases the use of online forms of communication become key tools in allowing access to global populations. Thus we see a key element of the special operations approach to the problem field of Digital Age conflict – one based not in the challenges of Web 2.0, but in the possibilities it offers in relation to its global ideological mandate.

The strategic mandate of the indirect approach sees a conception of military power expanded in space (to include the entire world), but also one which expands temporally, being applied outside of times of conflict. Doctrine refers to activity outside of conflict as "Phase 0" operations, referring to a "phase" of conflict before hostilities begin (e.g. DOD –

[39] Now known as the Trans-Regional MISO Program (TRMP) (Committee on Armed Services - *Hearing on National Defence Authorization Act for FY2014*, 2013)

JP 2-01.3, 2009:III-12; 2011:I-2, see Figure 2) - more popularly understood as *peacetime.* Operations which take place in this situation are also described as "shaping" operations – "those that are designed to dissuade or deter adversaries and assure friends [...they are] executed continuously with the intent to enhance international legitimacy and gain multinational cooperation by shaping perceptions and influencing adversaries' and allies' behaviour ... mitigating conditions that could lead to a crisis" (DOD *JP 3-0,* 2011:V-8), and ideological engagement through psychological operations.

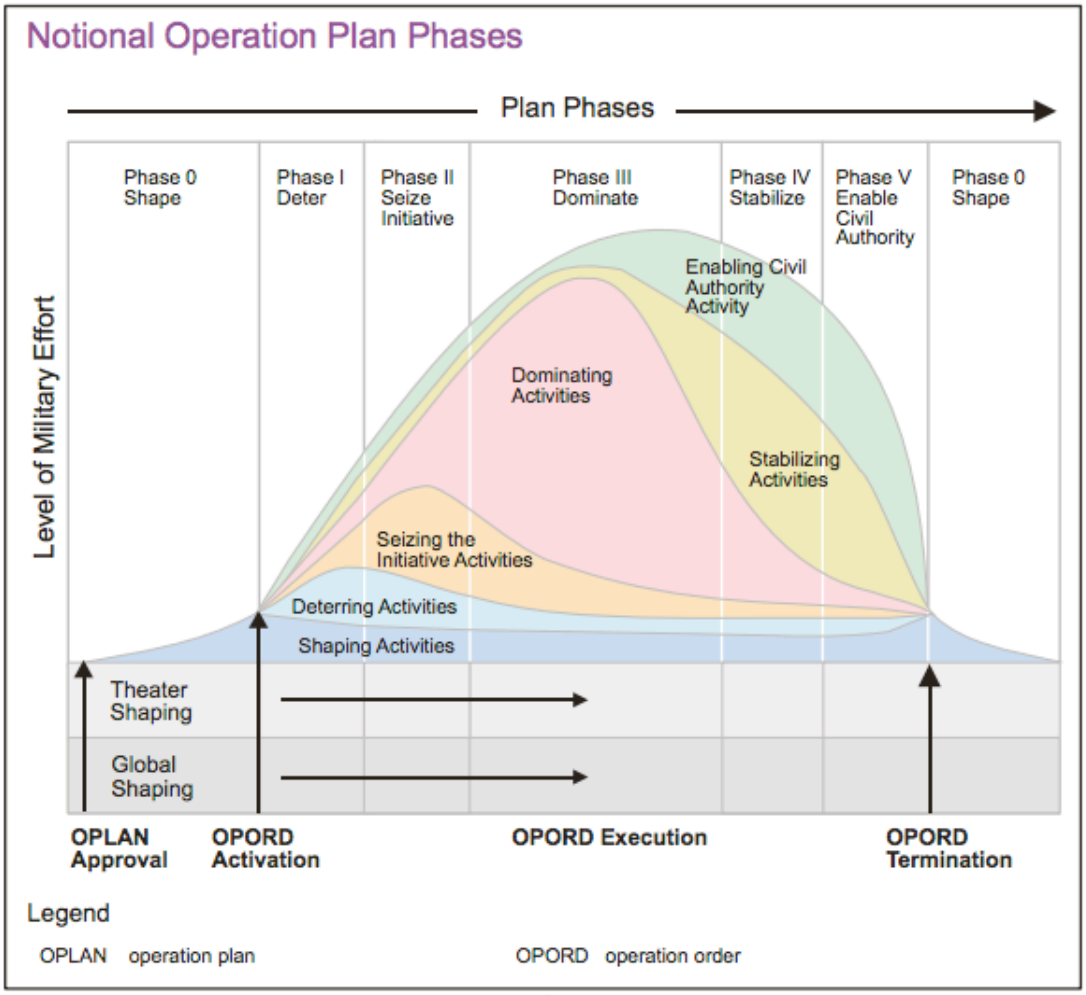


Figure III-16. Notional Operation Plan Phases

Figure 2: Diagram from Joint Operation Planning doctrine showing the phases of conflict (DOD – JP 5-0, *2011:III-32)*

Concern with this area of military strategy has risen sharply since the events of the Arab Spring, which presented a series of strategic shocks to analysts that are seen to be paradigmatic of the policy, diplomatic, and defence challenges of the Digital Age (see e.g. Seib, 2012:2; Jones and Baines, 2013:72). In this situation the indirect approach requires tools and practices for persistent and pre-emptive engagement. This includes intelligence "left of bang" (Flynn, 2013:2), that is, on the left of the timeline before a conflict starts, for the identification of "levers of change" in which the military can win a "competition for influence over relevant populations" in a context outside of conflict "where the cognitions and emotions of a target audience become the primary contested space" (Canna, 2013:13). Here again, we can identify an area where the rise of Web 2.0 offers a key means of

meeting military strategic priorities – offering a means to access information about those outside of conflict zones during "phase 0", and a channel to communicate with them and so "shape" the global operating environment.

Indeed, as GWOT strategy has developed under the Obama administration, this JSOC-inspired and SOCOM-led approach has gained further influence, with 2012's DOD strategic guidance document declaring that "US forces will no longer be sized to conduct large-scale, prolonged stability operations", and will instead work through cooperation with other military and non-military actors, and "limited" operations and "innovative … small-footprint approaches" (DOD – *Sustaining U.S. Global Leadership,* 2012:4;2). Here the SOCOM approach becomes central to the conception of the US military's role in the world – with "small-footprint approaches" such as the surgical attacks pioneered by JSOC and cooperation with other militaries as trainees and proxies, underlain by an approach which sees non-kinetic approaches as key to achieving military objectives. The strategic guidance was followed by the announcement of an expansion of SOCOM funding and personnel and mounting evidence that it was operating in some capacity - training foreign military or other fighters; running PSYOPS campaigns from embassies; and engaging directly in kill-or-capture missions - in around 100 countries across the globe (McRaven, 2012; Khalili, 2013, see also Lujan, 2013).

In these military developments we can see that the problem field of Digital Age conflict is approached within special operations from a strategic perspective in which global influence to combat both extremist organisations and their support base is the key aim. In doing so, an approach which uses a mixture of the application of extreme and precise violence largely hidden from public view and indirect engagement through global military and diplomatic cooperation and psychological operations guides strategic thinking. SOCOM is tasked with the job of coordinating and operating a global communication campaign against "violent extremism" and its ideological enablers – which, as we will see in chapter 5, uses Web 2.0 as a key tool. The problem field of Digital Age conflict as conceived in the special operations approach addresses many of the concerns of post-RMA military thought: the proliferation of non-state actors threatening the US military; the challenge of ubiquitous recording and publishing to military strategy; and the vastly increased complexity of both strategy and the communicative process in Web 2.0. Thus we can see the emergence of an approach to military strategy in which Digital Age conflict is not just a *challenge* to the DOD, but a key enabler in pursuing the GWOT. This is also demonstrated in the practical discourse focussing on intelligence and emerging forms of military communication – and lays the groundwork for emerging military practice in which actors at the 'tip of spear' engage with Web 2.0 not just as a *problem,* but as an *opportunity* to meet new strategic and operational imperatives.

4.4. Intelligence in the New Information Environment

In examining the effects of these strategic changes at the more practical level, formal and conceptual development in the area of intelligence demonstrates the influence of the

special operations approach. Though intelligence is not solely a military activity[40], the gathering of information about adversaries and (increasingly) non-combatants in areas of conflict (known in doctrine as *Intelligence Preparation of the Battlespace/Operational Environment,* see DOD – *JP 2-01.3,* 2009; US Army/Marine Corps – *FM 2-01.3,* 2009) is an in important area addressed in a number of documents which address the changing information environment. Intelligence is also an area in which the role of SOCOM has been very influential – with Michael Flynn co-authoring papers on the "Death Star" intelligence process (Flynn et al, 2008), the role of intelligence in COIN in Afghanistan (Flynn et al, 2010), and on the broader use of socio-cultural intelligence in both COIN and global strategic analysis (Flynn et al, 2012; Canna, 2013) which have been seminal in military intelligence practice in the latter GWOT years. This position of influence was formally recognised in 2012 when Flynn became head of the Defense Intelligence Agency (Ackerman, 2012). Overall, the changing conception of the operational environment as global, social, and permeating civilian life, leads to an expanded role for military intelligence both during conflict and outside of it.

I noted that JSOCs integrated intelligence and operations machine was influential in the shadow wars in Iraq and Afghanistan – using advanced surveillance technologies such as drones and electronic surveillance, and analytical techniques based on building up knowledge of networks. These techniques are making their way into official doctrine, with the Army *Information Collection* field manual discussing "Network Surveillance" as "the observation of organizational, social, communications, cyberspace or infrastructure connections and relationships [...] and the role and importance of aspects of physical or virtual infrastructure" (US Army - *FM 3-55,* 2013:1-12), as well as new forms of (unspecified) "cyber-enabled intelligence" (US Army - *FM 3-55,* 2013:1-14). The most important area in operational intelligence however has been the rise of Social Network Analysis (SNA), which has developed as a key aspect of the JSOC and COIN approach, and laid the ground for significant adaptation to the Digital Age operating environment based on the use of Web 2.0 data (explored in section 6.4).

SNA is an analytic tool which has been widely discussed within military intelligence circles in relation to COIN and counter-terrorism (see e.g. Wheaton and Richey, 2014; Ressler, 2006; MacGinty, 2010; MacCalman et al, 2013). The 'social networks' of interest to military SNA are not primarily the Web 2.0 ones of Facebook or Twitter, but of more traditional social networks such as families, community groups, militias, and insurgent cells. However, in providing a pre-existing military and intelligence knowledge and practice base in social networks, military activity in this area provides one context for the development of tools which *do* directly address the online information environment.

SNA was developed by social anthropologists as a tool for "mapping social dynamics and rendering complex social patterns intelligible to the outsider [...] by representing networks diagrammatically" – visualising links of kinship, friendship, business, or other affiliation between members of a society in order to "see their extent and significance" (MacGinty, 2010:210) producing web-like network diagrams of social ties. The attraction of this tool to military intelligence practitioners is plain, offering a quantitative and visual

[40] Indeed, the activities of the non-military intelligence agencies in surveilling and acting in the online information environment exposed by Edward Snowdon's leaked information show military activity in this area is far surpassed by other intelligence agencies (Greenwald, 2014a).

analysis of complex social groups, making them amenable to rapid outside understanding and potential intervention. In the contemporary military context SNA has been developed in two main ways. Firstly, at the larger societal level to "analyze systematically large data sets […] to anticipate individual and network responses to changing circumstances" (Carpenter and Stajkovic, 2006 in MacGinty, 2010:210) – providing a useful ontology to military planners concerned with population-centric approaches and with the effects of military actions on larger social groups. Secondly, at the micro level SNA has been applied to the analysis of "dark networks" such as criminal or terrorist groups – allowing them to be conceptualised as networks and examined (and combatted) in terms of key nodes (individuals, locations, groups) and links (relationships, conduits, communication channels) (see Sageman, 2004; Everton, 2012b; MacGinty, 2010:211). The latter approach has been particularly significant in combatting decentralised and networked forms of insurgency and terrorism prevalent in the GWOT – with SNA providing a tool which it advocates say renders these groups visible, intelligible, and thus targetable.

The utility of SNA in the post-9/11 security situation has been claimed in a number of high-profile assessments of counter-terrorism operations. It has been used (after the fact) to assess the 9/11 hijackers (Krebs, 2002, see also Bohannon, 2009:410) and the Noordin Top network in South East Asia (e.g. see Everton, 2012b), is said to have aided the hunt for Saddam Hussein (Wilson, 2010; Reed, 2007, US Army/Marine Corps – *FM 3-24*, 2006:B-14), the targeting of foreign Jihadis in Iraq (Felter and Fishman, 2007), countering insurgent IED teams in Iraq and Afghanistan (Peter, 2008; Bohannon, 2009:411; Shakarian et al, 2009), and even credited with a role in the assassination of Osama Bin Laden (Knoke, 2012:2). These examples highlight the claimed use of SNA at the lethal end of the military spectrum. One key theorist notes that "it appears to be almost an article of faith that once a dark network's structure has been mapped and its key members identified, one is supposed to capture or eliminate designated high-value targets" (Everton, 2012b:32).

The SNA approach is often related to the activities of JSOC (see, e.g. Ford, 2012; Knoke, 2012), however an assessment of their reported activities suggests SNA was used as a rough guide to activity rather than a key method. Ford calls JSOC's intelligence and operations an "industrialization" of an "SNA-based" approach to targeting which mapped insurgent networks in order to identify targets (Ford, 2012:126). However – this misunderstands the purpose of SNA: the JSOC approach was not based on a deep understanding of social networks in order to *understand their dynamics* or *target them more efficiently*, but based on the quick exploitation of intelligence from raids to increase the *tempo* of operations. This form of what we might call *snowball-targeting* is far from the promise of SNA to allow greater understanding of the dynamics, social context, and wider networks of adversaries. Its focus on a rapid operational tempo owes much more to Boydian principles of getting inside the enemy's "OODA Loop"[41] than it does to social anthropology. Identifying a target based on following someone in his or her social circle does not make the approach SNA-driven.[42] This suggests that while SNA may offer a

[41] John Boyd's concept of the "Observe, Orient, Decide, Act" loop is a key cornerstone of operational theory in the US military (see Boyd, 1995; USMC – *Operating Concept for IO,* 2013:8; Ambinder and Grady, 2012:Chapter 3)

[42] Similarly, just because an approach mentions the word "network" does not make it SNA-driven. McChrystal's oft-repeated mantra of "it takes a network to beat a network" is understood by Knoke to

helpful system of visualisation or set of heuristics ("nodes", "links", "branches", etc.) for thinking about insurgent groups and perhaps guiding the targeting process, as far as the *analysis* element goes it requires no more technology than a whiteboard (see e.g. the example of *Battle of Algiers* SNA methodology in Morganthaler and Giles-Summers, 2011).

Outside of targeting operations, the SNA section of the Counterinsurgency manual (US Army/Marine Corps – *FM 3-24*, 2006) presents it as a tool for "understanding the organizational dynamics of an insurgency and how best to attack or exploit it", moving beyond the example of the hunt for Saddam Hussein (US Army/Marine Corps – *FM 3-24*, 2006:B-14) to an approach based on mapping or uncovering networks in a larger social group. The manual describes a process to uncover insurgent networks based on using an "activities matrix" which maps international ties, night time activity, student associations, as well as an "association matrix" which maps possible or suspected associations between individuals and tries to connect the dots to uncover insurgent networks. It states that "for an insurgency, a social network is not just a description of who is in the insurgent organization; it is a picture of the population, how it is put together and how members interact with one another" (USMC, 2007:B-15). This suggests a form of SNA that is scalable and potentially useful for exploiting existing information – as opposed to targeting approaches which are basically aimed at guiding further intelligence or kinetic operations.

COIN offers an example in which, rather than providing the blueprint for a targeting campaign, SNA forms a key part of 'Intelligence Preparation of the Operational Environment' – essentially becoming a tool for understanding the "human terrain" element of the space within which counterinsurgents plan to do battle (see US Army/Marine Corps – *FM 3-24,* 2007:Appendix B; DOD- *JP 2-01.3,* 2009:B-17, II-37, IV-2 – IV-6). MacGinty outlines the rise of "cultural intelligence" as bound up with the fact that "SNA allowed analysts to situate militants and militant groups in their social hinterland", and thus "the realization, among intelligence analysts, that 'most networks grow from pre-existing social networks' had profound implications" (MacGinty, 2012:212, referencing Hammes, 2006:23). This application of SNA as a way of understanding the totality of the operating environment rather than superficially guiding the targeting process meant that "the 'battlefield' now became the family, community, workplace or university campus with the result that counterinsurgency activities would be socially invasive" (MacGinty, 2012:212). As such, despite such human "terrain analysis" (Reed, 2007:27) being a less intrinsically *violent* an activity than targeting, in extending the scope of SNA – essentially viewing the population of an operating environment as the "network" in question – it ultimately extends the scope of military intelligence and operations in a way which militarizes (and thus takes into the potential scope of violent activity) a much larger population.

Thus, when the *Counterinsurgency Field Manual* describes SNA as "a tool for understanding the organizational dynamics of an insurgency and how best to attack it or exploit it" (US Army/Marine Corps, 2007:B-10) it suggests a middle ground between targeting and broad social understanding. In this sense we can see a continuum between

---

further underline that JSOC's approach is SNA-based (Knoke, 2012:6). However, McChrystal's meaning is clearly that JSOC was agile and brought together a number of special operations and intelligence actors under the same roof – which says nothing about their approach being SNA-driven. Knoke similarly draws such false inferences from the use of the word "network" in various doctrinal publications (Knocke, 2012:7).

SNA for understanding social dynamics (population-centric) and one end and combatting 'dark networks' (Everton, 2012b) at the other (enemy-centric) – with the former being more distant from military violence but much larger on scope, and the latter referring to the direct application of violence to a very tightly-defined network. In the former case it may be interested in a populations happiness, tribal affiliation, or level of trust in the government; in the latter it may mark individuals out for a drone strike because of who they have made phone calls to. This understanding of the scope of activity facilitated by SNA and the range of ways it can conceive populations provides important background for our understanding of developing Web 2.0-related intelligence activity.

The interest in population-centric intelligence is also manifested in discourse relating to SOCOM's role in global operations and concern with global stability and ideological change – moving beyond SNA but also building from the influence of the COIN manual (US Army/Marine Corps - *FM 3-24,* 2006) in expressing the need for *population-centric* intelligence to develop a "deep cultural understanding" of those in the operational environment (DSB, 2008:419) to meet the requirements of a counterinsurgency strategy focussed on 'the people'. Flynn, writing in 2010 as head of intelligence in Afghanistan, demanded that information gathering and analysis be repurposed to support COIN tactics to "win" the civilian population (Flynn et al, 2010). He directed analysts to focus less on the enemy and to instead use information such as census and polling data, patrol debriefs, shura minutes, and other cultural data to produce intelligence of "strategic importance – a map for leveraging popular support and marginalizing the insurgency itself" (Flynn et al, 2010:7). He argued that the military needed to "think of the Afghanistan war as a political campaign, albeit a violent one" in which intelligence is needed on "which districts [are] undecided", which ones are "most worth of competing for", and "what specific messages [are] necessary to sway them" (Flynn et al, 2010:11). Here we see the requirement for a shift in intelligence to become part of a COIN and psychological operations apparatus – supporting information needs for communicators and guiding priorities, rather than being strictly enemy-focussed.

As thinking on insurgency and instability developed from the Afghan-specific situation to a more global, general military strategy under the indirect approach further developments have emphasised the importance of "understanding identities, attitudes, behaviours, and cultures; media trends and information flows; social and influence networks", which require the knowledge of "communications technologists", "behavioural scientists and cultural anthropologists", historians, linguists, and even "artists, authors and musicians" to guide engagement with civilian populations (DSB, 2008:420-421). Notably, a number of communication technologists and experts in influence, networks, and communication flows have since been employed by the DOD under R&D programmes examined in chapter 6. In these developments it is clear that new intelligence concerns relating to a changing operational environment mean that non-combatants (be they sources of knowledge, subjects of surveillance, or populations to "win") are drawn in to military consideration in new ways with significantly implications for military-civilian relations as *population-centric intelligence* goes global.

The most developed work on Digital Age intelligence comes in papers published by Flynn and his colleagues (Flynn et al, 2012; Flynn, 2013; Canna, 2013) during his time as head of the DIA, using the Strategic Multilayer Assessment programme (a key area of analysis in

chapter 6) as a platform. In this role Flynn has given a number of presentations which takes the interest in "the people" from COIN-era population-centric intelligence writing and generalise it, propounding on the value of "socioculatural analysis is today's environment" (Flynn et al, 2012) and the value of behavioural and social science to military operations (Canna, 2013) in the indirect approach to military influence. This generalisation of the importance of sociocultural knowledge is contextualised by the strategic surprise of the Arab Spring – a shock to US defence and foreign policy which demonstrated the role of the new information environment in driving rapid and revolutionary global events, meaning that understanding (and potentially influencing) quickly-changing regional dynamics becomes the new challenge to the US intelligence, military and policy communities (Flynn et al, 2012:13). In this global situation, intelligence relating to broader socio-political events at the strategic level (Flynn et al, 2012) becomes vital in the pursuit of influence in "phase 0" throughout the strategic environment. Flynn outlines the need for "a sensory capability to better detect the precursors to political change, a "social radar" [a key emerging paradigm examined in section 6.4] with a level of granularity [and] understanding, that enables policy leaders to make informed decisions that maximize the national influence left of bang" (Flynn et al 2012:15).

This type of intelligence should have a sociocultural focus to allow engagement through communication, it "should seek to explain how populations understand their reality, why they choose to either support or resist their governments, how they organize themselves socially and politically, and why and how their beliefs transform over time" (Flynn, 2012:2). This is of course a tough ask, though this interest in 'phase 0' also coincides with a period of conflict (peacetime) where information is more readily available from "academia, private sector companies, and social media, all of which often enjoy unfettered access to the population and generate information about it as a normal activity" (Flynn, 2012:7). Thus the new information environment is not only important in driving change (as in the Arab Spring), but in allowing important changes happening in public domain discourse to be monitored and understood for intelligence purposes, it "can provide a wealth of information enabling analysts to develop base line assessments of populations, cultures, behaviors, and social narratives" (Flynn, 2012:7 – see Figure 3). In this sense, the strategic focus on 'phase 0' can be seen as not simply based on delusions of omniscience, but on the fact that this period offers the greatest *access to data* about populations with which the military can work, and thus the greatest possibility of an informed response. This new conception of intelligence is not only one in which the practices of intelligence change, but also the *subject* – interested in issues of political belief, change, and the internal political and social dynamics of other nations; and the *subjects* – the general population as social and political actors, rather than a strict adversary-focus.

This interest in behaviour and narratives demonstrates that along with the importance of intelligence as a population-centric process, there is also a growing synthesis between intelligence and communication practices. The head of the HSCB Program, a key DOD R&D component discussed in chapter 6, writes that developing intelligence and communication practices cohere in a strategy which seeks to "detect, monitor, *and engage* at "twitter speed"" (Schmorrow, 2013:21, emphasis added), with engagement based on communication rather than violent action: seeking to "shape perceptions and influence adversaries' and allies' behaviour" (Schmorrow, 2013:2) before conflict emerges. Similarly, Canna notes that the broad application of social science knowledge across the

DOD allows military actors to identify "levers of change" (Canna, 2013:7). She describes 'shaping' operations in this context as "a competition for influence over relevant populations", producing a situation in which "securing influence in the global information marketplace will be critical", in facilitating contemporary military practice which "move[s] past more traditional conflicts towards operations where the cognitions and emotions of a target audience become the primary contested space" (Canna, 2013:13).

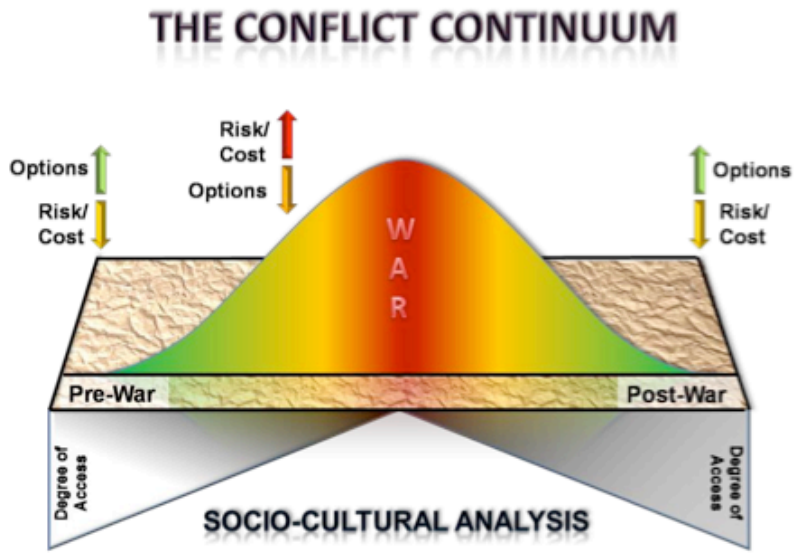


Figure 1. Conflict continuum.

Figure 3: Diagram showing availability of information, options, and risks in the phases of conflict. Phase 0 (the far left) offers optimal access to sociocultural data about populations as well as options for intervention (Flynn, 2012:8).

Thus in advanced special operations-influenced discourse on intelligence, the *availability* of information about populations "left of bang" goes hand-in-hand with the new *strategic importance* of intelligence on sociocultural elements of civilian populations under the indirect approach. Coming at a time where US foreign policy is averse to large scale "boots on the ground" intervention – the growing scope of the information environment as a platform for engaging with populations, for both intelligence and communication becomes clear. Demonstrating that new conceptions of the information environment facilitate a move beyond traditional intelligence collection, in the new conception of intelligence "strategists must learn how to leverage new technologies to influence and shape social behaviors through social media, online entertainment, and other means that are now global in nature" (Canna, 2013:14). To paraphrase Flynn, under the indirect approach to Digital Age conflict, intelligence *is* psychological operations.

This recognition is found in top level strategic thinking relating to military communication, with the 2010 *Commander's Handbook for Strategic Communication* noting that intelligence on "the informational and cognitive dimensions that permeate the

local social, political, economic and information networks" are key to commanders' communication strategies (US Joint Warfighter Command, 2010:xv). A precursor document notes that intelligence "will change significantly to support the needs of strategic communication, emphasizing the collection and analysis of information on the perceptions, attitudes and beliefs of potential foreign audiences – not traditionally considered intelligence targets" (DOD, 2009, *Strategic Communication JIC,* 20). As we see in discussing military R&D (an area in which those quoted in this section are highly influential), the area of "human, sociocultural and behavioural" intelligence is a key growth area in the DOD. It is one in which links to key developments in both special operations and Web 2.0, making intelligence a key element in the Digital Age propaganda apparatus. This recognition presents a challenge to our understanding of the developing role of information in the relationship between military and civilian, between what is understood as part of conflict and what is not, and it is a key element in understanding new information operations practices, which are discussed below.

4.5. Information Operations and Strategic Communication

The area of intelligence is not the only one dramatically impacted by the rise of population-centric strategies and the new operational environment. Also key is the doctrinal area covered by the term *Information Operations* (IO), in which adaptation to the information environment of Digital Age conflict correspond with the strategic shifts discussed above. In 2001, the *Quadrennial Defense Review* (DOD – *QDR,* 2001) identified IO as a "critical operational goal" for development within the DOD and designated it a "core capability" for future forces - a term which formally identified public communication as having central importance within military operations (DOD - *Information Operations Roadmap*, 2003:2). At that time then-Secretary of Defense Donald Rumsfeld described the doctrine as an example of the DOD's "commitment to transform [its] military capabilities to keep pace with emerging threats and to exploit new opportunities afforded by innovation and rapidly developing information technologies" (DOD - *Information Operations Roadmap*, 2003:1). This marked the relationship between communication, technology, and conflict as key in developing IO practice – which covers psychological operations (PSYOPS), public affairs (PA), and other tasks relating to information at a more technical level (such as protecting military radio frequencies, or attacking enemy navigation systems).

In the early 2000s, military public communication efforts (PSYOPS and PA) were very much guided by the linear communication concept of 'messaging', based on information products "produced rapidly at the highest quality standards, and powerfully disseminated directly to target audiences", with a focus on "adversary behaviour modification" (DOD, 2003, *Information Operations Roadmap*, 6-7). This was an approach which fused the traditional military monopoly of the information environment in a warzone (through ability to distribute leaflets, hijack airwaves, etc., see Snow and Taylor, 2006) with the communication practices of advertising or PR (Plaisance, 2005) – based on a belief that the US's technological and media skills would prove decisive in any 'battle of ideas' (see e.g. Holbrooke, 2001, Waller, 2007). Throughout the research period however, with the growth in complexity of Internet communication and challenges of population-centric

approaches to conflict, this direct "messaging" approach to public communication has given way to a more nuanced and holistic vision built on dynamic engagement with target audiences and bespoke intelligence, situated in an strategic environment in which communication and military operations converge, making IO a more thoughtful and subtle tool at the core of US military thinking and planning.

This change was catalysed with the rise of the concept of *Strategic Communication* – a term which has been used frequently by policymakers and practitioners since the mid-2000s and has sometimes been written into policy, encapsulating an enhanced understanding of the relationship between words and deeds in understanding the impact of military or foreign policy (see e.g. Borg, 2008; Murphy, 2010:92; Gates, 2007; Brooks, 2011, Kuehl, 2008; US Joint Warfighter Command - *Commander's Handbook for Strategic Communication,* 2010; DOD - *Strategic Communication Joint Integrating Concept,* 2009). In the military realm, the concept identifies the need for a nuanced understanding of the relationship between kinetic operations and their effects in the information environment, such as how they are perceived or how they reinforce or undermine military narratives (see Tatham, 2008; Mullen, 2009). Commanders' guidance identifies the rise of the Internet and new ICTs as the catalyst for the focus on strategic communication, saying that "the continuous, rapid communications flow in the information environment, facilitated by modern technological advances and media distribution methods, requires responsive, agile processes and capabilities to preserve and enhance the credibility and influence of the United States… greatly amplify the impact and speed of change in foreign and domestic public opinion and the subsequent influence on activities of the US Government" (US Joint Warfighter Command - *Commander's Handbook for Strategic Communication,* 2010:I-1). However, we can see strategic communication as a recognition of the strategic difficulties of hypocrisy (that no amount of 'messaging' can counteract bad policy or unpopular actions, see Mullen, 2009). This will be no surprise to critics of US foreign policy, but in terms of military doctrine has led to a significant paradigm shift for a generation of strategists who grew up in the RMA era of virtual and virtuous war, thinking of communication and public opinion as secondary to the application of violence, or else were blinded by the righteousness of their cause in the post-9/11 political climate (see e.g. Glassman, 2008; Waller, 2007).

Strategic communication takes the battle for perception and 'hearts and minds' in the battlefield to a more global level, addressing "a full-blown battle in the cognitive dimension of the information environment" based on consistency of information and action (US Joint Warfighter Command, 2010, *Commander's Handbook for Strategic Communication,* xiii-xiv). While strategic communication does not have doctrinal authority and remains a rather ephemeral concept (see Brooks, 2011)[43], in demonstrating policy-level engagement with a global information environment which sees words and deeds as part of a coherent strategic program across the military and government it captures a key moment in the development of Digital Age communication policy in which military action and its representation (echoing the linked kinetic and non-kinetic approach of SOCOM) become understood as a coherent whole. It drove perception and communication to the

[43] Indeed, towards the end of the research period it was announced that the DOD was scrapping the term "Strategic Communication" and replacing it with "communication synchronization efforts" due to the old term creating "confusion" (GAO, 2013:1)

heart of military strategy and thought. The outcome of this can be seen in current top-level *Operations* doctrine which describes the operational environment as "saturated with information, with almost universal access to telecommunications and the Internet", in which perception failures are strategic failures, and vice versa, and states that the "action and message can no long remain separate parts of operations because perception is so important to success" (US ARMY - *FM 3-0,* 2008:1-18, see also US Army - *FM 3-13,* 2013:1-1).

As well as taking kinetic and non-kinetic military activity as a whole, new *Inform and Influence Activities* doctrine (IIA, an alternate new term for IO, US Army - *FM 3-13,* 2013:1-1) also moves beyond previous conceptual distinctions within IO thought which sought to address audiences in the warzone, those in the homeland, and the global audience in a compartmentalised way. Instead, contemporary IO doctrine addresses the *global* information environment of contemporary military activity and communication "simultaneously", as "today's global information and communications environment means that messages *and actions* delivered to one audience also reach other audiences" (US Army - *FM 3-13,* 2013:v, emphasis added, see also DOD - *Strategic Communication JIC,* 2009:8). As such, IO practitioners are tasked with engaging "all audiences within the information environment, which include domestic, foreign friendly and neutral, adversary and enemy" (DOD, 2009, *Strategic Communication JIC,* 8). Thus we see a corollary of the expansion of the purview of intelligence and strategic thought on the importance of audiences outwith the conflict zone – who now also enter the purview of IO practitioners in a global information environment.

4.5.1. PSYOPS and Public Affairs in the New Information Environment

Information Operations is broadly defined as "the integrated employment, during military operations, of [information related capacities] in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and protect our own" (DOD - *JP 3-13*, 2012:vii, see also DOD Directive 3600.1 – *Information Operations,* 2013). These capacities include Psychological Operations (PSYOPS), Public Affairs, Military Deception, Key Leader Engagement and Cyberspace Operations (DOD - *JP 3-13*, 2012:ix) – all of which have their own subordinate doctrine. This thesis follows other analysts of IO (Hammes, 2009:29; Hoffman, 2009:104-105; Lawson, 2013:4; Brunner and Dunn Cavelty, 2009:360, Rumbaugh and Leatherman, 2012:12) in viewing the areas which apply directly to the field of public communication – Public Affairs (PA) and PSYOPS – as a distinct branch of IO, and the focus of interest here[45].

[45] The areas of Electronic Warfare and Computer Network Operations focus entirely on the physical element of the information environment, such as jamming or protecting radio frequencies and other command and control-focussed elements (DOD - *JP 3-13.1,* 2012*;* US Army – *FM 3-38,* 2014:v). The term "cyberspace" also refers entirely to technical aspects in a doctrinal context (see e.g. DOD – *Strategy for Operating in Cyberspace,* 2011; DOD – *National Military Strategy for Cyberspace Operations,* 2006). *Operations* doctrine refers to cyberspace operations as the only ones which do not happen "among the people" (US Army – *FM 3-0,* 2008:1-3), and they are described in targeting doctrine as following "the processes and procedures used for traditional [i.e. kinetic] targeting" (DOD – *JP 3-60,* 2013:C-7). Similarly, in the DOD (2010) *Joint Terminology for Cyberspace Operations* there are no concepts relating to psychological or cognitive areas, and IO doctrine refers to cyberspace operations only in relation as their ability to provide an internet connection to practitioners (US Army – *FM 3-13,* 2012:3-5) or denying an internet connection to enemy forces (DOD – *JP 3-13,* 2012:II-9). The area of Military

Although they both address public communication, PA and PSYOPS have always been carefully distinguished in doctrine (e.g. DOD - *JP 3-61,* 2010:viii; see RAND, 2013:59) – with the former's approach to "informing" domestic and foreign audiences about a conflict being distinguished from the latter's efforts to "influence" those in the conflict zone. However, the new IIA approach, while still maintaining the distinction between the respective roles of PA and PSYOPS in saying that "US forces strictly *limit their influence activities* to foreign audiences [which] typically focus on persuading selected foreign audiences to support US objectives" (US Army - *FM 3-13,* 2012:1-2, italics added) – recognises a convergence of the two areas in the global information environment.

The formal disavowal of PSYOPS "influence" activities in favour of those which merely "inform" audiences is a sociologically and epistemologically dubious distinction (which is recognised as facile in other doctrinal discussions, see DOD - *Strategic Communication JIC,* 2009:iii; RAND, 2013:xxv). However, the division of the concepts offers conceptual guidance in that PA tries to maintain a distance from PSYOPS practices which are perceived to be more manipulative, and thus aims at more direct communication with publics based on press releases and conferences, media relations, and more traditional communication roles. PA practice is based on the stated belief that the Military "has an obligation to communicate with the American public, and it is in the national interest to communicate with the international public" (US DOD - *JP 3-61,* 2010:vii), and of the two bodies of doctrine it is the one which has most directly engaged with the Web 2.0 information environment.

Web 2.0 presents a number of forms of disruption for PA, which is historically based on developing a beneficial relationship with the media, which acted as the key conduit for information that made it into the public domain. However as a situation emerged in which "the ability of anyone with Internet access to communicate and provide graphic visuals as an event unfolds" it means there is an "increased transparency of military operations" and "constant scrutiny" of all actions (US DOD - *JP 3-61,* 2010:I-10), and thus traditional PA practice is challenged. This leads to more complex relationships between the military and the public which is no longer fully-mediated by the mainstream media and manageable through these relationships. As such, current doctrine finds PA at something of a crossroads, the area is said to be "still largely a matter of ensuring media have access to information they need" (US DOD - *JP 3-61,* 2010:III-1), while also recognising that "the Internet … provides numerous options and challenges for unfiltered communications with various audiences" (US DOD - *JP 3-61,* 2010:II-1), undermining the role of the media and opening up a new area of direct military-public communication.

This later point suggests a potentially important growth area for PA, and many non-doctrinal but important developments demonstrate the key role unfiltered information provided by military PA now plays (for example through official military Facebook pages and blogs, see Bennett, 2013; USMC Social Media, 2014). Yet the only real discussion of PA developing Internet communication programs in doctrine is a section noting the presence in conflict zone media operations centres of a "new media" section which should maintain

---

Deception (MILDEC) addresses only the deception of opposing military actors though processes such as producing false radio chatter or feinting manoeuvres (DOD – *JP 3-13.4,* 2012), and is in any case in the process of being moved out of the area of IO (US Army, *FM 3-0,* 2008:6-19).

a "public website" associated with the mission and publish content, as well as use "interactive internet activities" such as "email, blogs, chat rooms, and social media" to support operations. We can see this for example in the ISAF website (Figure 4), which offers all such services. This type of publishing and communication activity is always transparent and open to public scrutiny, so the analysis of PA websites does not form a major part of this research.

Figure 4: Screen capture from Isaf.nato.int on 07/07/2014 – the ISAF mission website, showing the new Public Affairs online engagement imperative in action (ISAF, 2014).

The identification of "interactive internet activities" as a new element of PA sounds far reaching, but the doctrine specifies that "only PA personnel [can] engage in interactive Internet activities with journalists employed by media organizations or with individuals and websites that may be considered equivalent to an established news organization" (US DOD - *JP 3-61,* 2010:D-2). This suggests that this engagement is stuck in a pre-Web 2.0 mode, simply accommodating new influential platforms outside of the traditional press rather that embracing the interactivity of social media and the proliferation of 'information doers'. The doctrine also mentions "blogger engagement services" run by the Defense Media Agency, which facilitates PA by linking bloggers with DOD leaders through means including telephone conferencing and transcription services (US DOD - *JP 3-61,* 2010:D-2) – again, adapting traditional PA activities (press-releases, interviews) to modern technology in a fairly direct way. PA can thus be seen to be adapting to some forms of online engagement, and some new "interactive" elements are seen in CENTCOM's Digital Engagement Team examined in section 5.5.2. However they are not the wholesale changes of a fully Web 2.0-savvy approach, instead developing to keep up to date with changes in journalism and what might be considered the Digital Age mainstream.

These limited developments in PA doctrine, however, make the area of psychological operations look positively prehistoric in comparison. Contemporary US PSYOPS doctrine is remarkable much more for its lack of engagement with the Internet than any revelations or cutting edge adaptation (DOD - *JP 3-13.2*, 2011; US Army - *FM 3-05.302,* 2007). It is the element of US military activity most often linked to propaganda, as it is through PSYOPS that the military seeks most comprehensively to engage with and "influence" audiences in areas of military interest, yet it discusses the Internet very little. This is likely due to the need for doctrine to be as widely applicable as possible and thus apply to situations (such as Afghanistan) where the Internet is not such an important part of the operational environment. Joint doctrine (*JP 3-13.2*) focuses primarily on how to build a PSYOPS team and liaise within command structures rather than the specificities of particular information environments, while the tactical doctrine spends pages discussing the ideal layout, size and weight of leaflets (US Army, *FM 3-05.301,* 2007:chapter 4), mentioning the Internet only to suggest practitioners get in touch with the IO section who can help them "obtain" (sic: access) web sites to find information which might help their planning (US Army - *FM 3-05.301,* 2007:6-17). However, when we understand PSYOPS in the context of the contemporary information environment developed elsewhere as increasingly based on ICTs, and a strategic environment where influencing populations is an increasing focus, the area is of obvious interest to the research.

In 2010 the DOD changed the name of PSYOPS to Military Information Support Operations (MISO), although this thesis will continue to use the term PSYOPS[46], which is defined as "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organizations, groups, and individuals in a manner favourable to the originator's objectives" following a "deliberate process" based on understanding the environment, audiences, and delivering tailored messages and actions through "sophisticated media delivery means" to "produce observable, measurable behavioral responses" (DOD - *JP 3-13.2*, 2011:vii-viii). It is, we can see, the measured and systematic use of communication in an instrumental way in the attempt to make people do what the military wants them to do. PSYOPS is the discipline most frank about its focus on influence and behavioural change due to its historical focus in conflict-zone information operations – such as dropping "surrender" leaflets on enemy soldiers, handing out fliers to civilians on everything from checkpoint safety to sanctions for supporting the enemy, and running warzone radio stations (see Munoz, 2012). Thus in the COIN context it has become the

[46] PSYOP was renamed MISO by the DoD in 2010 (by an unreleased but frequently referenced memorandum by Admiral Olson, the head of SOCOM). This was largely reported, based on DOD sources, as "just a terminological change, not a substantive change" (see Ambinder, 2010; Rumbaugh and Leatherman, 2012:16), premised on the notion that "MISO" does not sound as sinister as "PSYOPS". However, there was also intense internal debate within the PSYOPS community around this time as to whether this attempt to make PSYOPS more palatable to mainstream policy makers would restrict potential avenues of persuasion and diminish the autonomy of military communicators (see Boyd, 2011 and Paddock, 2010). In August 2014, the main "MISO" units in the military (those studied in section 5.4) changed their name back to "Psychological Operations Groups", thus the saga continues (see ShadowSpear, 2014). The continued use of the term PSYOPS in this thesis reflects the continuity of organisation, thought and practice, as well as a scholarly resistance to the prettification of the concept by DOD terminologists.

area of military activity on which the responsibility to win "hearts and minds" falls most directly – elevating it to a central part of GWOT military practice[47].

This increased responsibility is reflected in changing organisational imperatives and practices of those tasked with PSYOPS (with the practices of the SOCOM-based PSYOPS units the key subject of analysis in chapter 5.4), however in terms of the practicalities of contemporary PSYOPS the doctrinal material lags significantly. It does not address the contemporary information environment in a meaningful way, referring to communication platforms and practices in only general terms. It discusses pursuing influence goals by communicating within an environment where it is understood that "the informational, cultural, social, moral, political and physical aspects of the operational environment" are all critical (DOD - *JP 3-13.2*, 2011:vii). This broad brush approach allows us to hypothesise that in the context of a Web 2.0 'operational environment' PSYOPS becomes a key element of Digital Age military engagement – where intelligence discourse has already pointed out these as crucial elements. Joint Doctrine also notes a shift in contemporary conflict, with the importance of engaging "international audiences to clarify intent, prevent escalation of tension, ease concerns, and mitigate the potential effects and capabilities of adversary information activities" (DOD - *JP 3-13.2,* 2011:1-2, see also CJCS, 2011) – thus suggesting a role for PSYOPS beyond the immediate conflict zone, into the global information environment.

Although the PSYOPS doctrine is light on details of Internet activities it has both the conceptual potential, through the direct outline of a stated aim to influence target audiences and the outline of the operating environment of conflict, to form the doctrinal basis of an important area of development in Digital Age conflict. Indeed, the lack of engagement with the contemporary information environment belies the fact that the most concerted engagement with Web 2.0 comes from PSYOPS practitioners based in SOCOM and CENTCOM. Far from being stuck in the age of leaflets and radio broadcasts their practices are at the cutting-edge of conflict communication. The next section looks beyond official doctrine, at broader discourse produced by military figures thinking about the potential future of PSYOPS – and provides some useful concepts for thinking about developments in this area.

4.5.2. Towards Information Engagement

While doctrine, as the formal and coherent body of military thought and practice, is a necessarily slow-developing and often very general framework for military activity, in that generality it offers the opportunity for new practices and approaches to develop *on the fly* in wider military thought which can be understood within the broad doctrinal framework (e.g. see Rid, 2007). In this regard, the work of a number of IO and PSYOPS figures who address Web 2.0 offers deeper understanding of military adaptation to Digital Age conflict. These writers explore how the military can learn to "leverage new media", in the recognition that, like old media, Web 2.0 "can also be enlisted to serve specific masters, though perhaps with greater difficulty" (Caldwell IV et al, 2009:4). This body of work

[47] This is not to say that the 'hearts and minds' imperative falls on PYSOPS *exclusively,* indeed COIN doctrine is emphatic in the responsibility of every soldier to account for the potential consequences in terms of public opinion of every action (US Army/Marine Corps – *FM 3-24,* 2006:A-5)

outside of official doctrine, within military journals, think tank reports, and military academia, approaches the changing nature of Web 2.0 intelligence and communication practice much more directly. It offers suggestions for new concepts or practices, reports on changes on the horizon, and provides insight into cutting-edge thinking in the problem field which has not yet transferred into the formal annals of doctrine.

The shift in IO thinking from the view of communication as a matter of "messaging" in a linear sense to a more dynamic and complex understanding of the communication process is fleshed-out in this quasi-doctrinal work. Here, a report by the US Army War College based on a workshop of IO practitioners in 2009 offers an important concept through which to understand contemporary changes. *Bullets and Blogs: New Media and the Warfighter* outlines a paradigm shift in IO, from one based on information control and linear dissemination, to one of "information engagement" (see figure 5) – in which IO practitioners seek to *engage* in the information environment though understanding the media milieu, advanced target audience analysis and intelligence practices, building credibility and trust, and understanding Web 2.0 information flows and platforms (Collings and Rohozinski, 2009:2).

DOD and information engagement:
Cultural and organizational change

Participants concurred that the move to a culture of engagement will require fundamental organizational and cultural change.

Away from	Toward
Information control and media avoidance	Information and media engagement
Information environment as an afterthought in operational planning (information as a support operation)	Information environment as a core determinant of the operational battlefield, and sometimes the focus for the main effort
Information dissemination	Strategic communication
Uni-directional "Messaging"	Interactive strategic listening and establishing credible relations with key audiences and communicators
Reactive	Proactive
Focus on tactical operational success	Packaging tactical operational success for strategic wins with key audiences
Information hierarchies, centralized control and permissions	Full-spectrum agility, empowerment at the lowest levels, with appropriate rules of engagement
Piecemeal efforts and policies	A holistic and integrated approach
Digital immigrants	Digital natives

Figure 5: Comparison of 'information engagement' and previous 'information control' or 'messaging' approaches to Information Operations (Collings and Rohozinski, 2009:19)

Echoing the strategic thinking outlined above, the rapporteurs of the workshop write that participants agreed "new media and the Global Information Environment present sustained challenges and opportunities… [requiring] preparation for a battlespace in which symbolic information wins may precipitate strategic effects equivalent to, or greater than, lethal operations", describing the changes brought by Web 2.0 to IO as requiring "a paradigm shift away from an emphasis on information control and towards

information engagement" (Collings and Rohozinski, 2009:1, see also Kramer and Wentz on "information effectiveness", 2008:3). This paradigm shift requires a move away from the information strategy based on attempting to control damaging information about what goes on in the battlefield and using media channels to transmit carefully crafted messages intended to boost public support (the early-GWOT approach), to one which recognises that such information simply cannot be controlled, that the transmission of messages is no simple matter in the online information environment, and that the division between what happens in the operational environment and information *about* that activity is not a viable division of labour in Digital Age conflict (Collings and Rohozinski, 2009:ix). That is, it takes the broad insight of the 'strategic communication' paradigm (as IO doctrine has), and applies it directly to the understanding of PSYOPS-type communication practice – presenting a new paradigm for military communication in Digital Age conflict.

The workshop outlined six "core competencies" for information engagement: increased speed of military messages (to combat insurgent and citizen journalists' speed at uploading information); a flattening of the approval process for engaging in the information domain (less concern with OPSEC in order to speed up communication); better tailored communication with different audiences (based on "strategic listening", the refinement of messages through dynamic audience analysis); a focus on building up a presence on various platforms (such as followers and credibility on social media platforms); the use of trusted messengers or conduits (in order to bypass disparities in military credibility online); and the importance of "sychronicity" or a coherent strategy in communication and practice (Collings and Rohozinski, 2009:3-4). These elements are found throughout the advanced IO literature – and taken together work towards the development of a new form of IO addressing the particularities of the new information environment through a set of practices dubbed "CY-OPS" (Cyber-PSYOPS) (see Thomas, 2007, Collings and Rohozinski, 2009:8; and Shakarian et al, 2013:35-36), which make up the process of "information engagement".

Information engagement requires a new way of thinking about PSYOPS and other military communications. Where post-9/11 communication strategy brought in marketing gurus and rhetoricians in order to try and craft 'better' messages which would resonate with foreign publics (e.g. see Waller, 2007; Plaisance, 2005) – information engagement stresses the "multiplicity of information producers and channels" of new media and its "viral nature", "eviscerating the capacity of any actor, including the U.S. military, to control the information available" or focus solely on sending well written messages (Collings and Rohozinski, 2009:15). At the most basic level, this is a shift to an approach based in dialogic communication (see US Joint Warfighter Command – *Commander's Handbook for Strategic Communication,* 2010:III-11) which recognises that the traditional forms of military communication (e.g. the press conference, press release or the information leaflet) and their Web 2.0 equivalents of a Facebook post or blog entry are 'incomplete actions' in the interactive new media world, and should be seen as "a first act, a necessary but insufficient undertaking" which must be followed up (Cunningham, 2010:35). This follow up may take the form of engaging in dialogue and following these messages as they "evolve and within a larger media conversation" (Cunningham, 2010:16; cf. Jones and Baines, 2013:77), or understanding and engaging with the importance of "viral" communication and message "stickiness" (Collings and Rohozinski, 2009:2) or "infectivity"

(DSB, 2008:396). Both approaches to engaging with Web 2.0 communication are found in the research on military practice presented later in this thesis.

Information engagement has seen a number of military theorists draw on work which explores the behavioural or psychological effects the use of Web 2.0 media platforms can have on Web users. Drawing on the work of Fogg (2002), who outlines a discipline he calls *captlology* as the "study of computers as persuasive technologies" (see Stanford Persuasive Tech Lab, 2014), a number of military authors have discussed the potential CY-OPS application of these insights. Fogg's work looks at how various human-computer and online social interactions can affect users' perceptions and behaviour – and has been identified as potential CY-OPS growth area by Efaw (a key figure in SOCOM's social media development), who is attracted by the application of behavioural psychology to the production of Facebook apps to encourage people to share PSYOP messages, saying "these applications are a tool to put ["credible [voices] in the War of Ideas"] into credible mouths (Efaw, 2009:6). While under-developed as a practical concept, captology has gained sporadic interest in PSYOPS circles – with Skarda *et al* presenting it as a key concept in "operationalizing social engineering for offensive cyber operations" (2008) and Spitaletta identifying it as a potential basis for the development of "neuropsychological operations" (2013:73). While it is not appropriate to generalise from only a few instances, it does draw our attention to new technological forms of PYSOPS which attempt to shape the moment of communication, facilitated by new ICTs – and section 5.3.5 discusses CENTCOM's PSYOPS activities' inclusion of iPhone and Android apps aimed at Muslim audiences, showing military communication moving beyond a matter of content and taking an interest in platforms and non-semantic elements of communication.

As well as suggesting new element of PSYOPS which address the *process* and *structure* of communication rather than its content, the emphasis on Web 2.0 information flows also leads to an increased emphasis on understanding the position of the communicator. Unlike old media where authority "was largely conferred automatically upon established unitary actors", it is now seen as "something that resides within the context of one's social networks where personal relationships are firmly established and trust continually nurtured" (Cunningham, 2010:20). As such, "becoming an integral presence in the ongoing public conversation" online is understood as an information engagement imperative, including "in all the forums where critical audiences dwell", moving from a reactive and broadcasting paradigm of communication to one of "proactive engagement" (Collings and Rohozinski, 2009:16, see also Gilmor and Osial, 2011; Jones and Baines, 2013; Mayfield III, 2011; Bigge, 2009; Burgstein, 2014, see also Comor and Bean, 2012). This proactive engagement also entails a deeper knowledge of the audience, from the need for "blog-watchers" to understand stories as they evolve (Collings and Rohozinski, 2009:16), to a more advanced form of "target audience analysis" which understands the communication landscape as "denser, more complex, and more participatory" and acts as a "living document … that serves as a dynamic and detailed method for gathering not just intelligence, but also insights into audience vulnerabilities, accessibilities, and susceptibilities in a given culture" (Bostick, 2011:12, see also Kramer and Wenz, 2008:3). The intelligence value of Web 2.0, particularly as relates to PSYOPS is a key element of the contemporary problem field which has given rise to new practices and techniques, and documents obtained during the research show that a long-term assessment of the

sentiment expressed by users of anti-US forums is a key element of covert CY-OPS campaigns to try and influence that sentiment.

The importance of understanding audiences and the cultivation of credibility leads to the consideration of another element of "information engagement" – the importance of using conduits or other credible sources to spread military messages. The *Bullets and Blogs* study identified the use of conduits – what they call "independent friendlies" or "third party validators" – to spread messages online to be a key "force multiplier" (Collings and Rohozinski, 2009:16, 3-4). At the most direct level, this can bee seen in the role played by milbloggers as the 'human face' of the military (see e.g. Mayfield III, 2011). It has been suggested that the loosening of hierarchical control of information dissemination (i.e. requiring less official clearance for bloggers or public statements) will allow the US "to compete with the proliferation of messages exchanged in today's Attention Economy", and so the military should empower all competent communicators to engage online (Cunningham, 2010:ii). One practical move towards this de-specialisation is a policy at the US Army Command and General Staff College where a concerted effort is being made to have trainees familiarise themselves with the Web 2.0 environment: requiring all students to blog as a requirement of graduation and all Information Operations specialists to learn "the basis of Web 2.0 with the understanding that [they] will often advise their superiors on the nuances of social media" (Caldwell IV, 2009:26-27).

At another level, this use of conduits can also be seen in the use of non-military actors to spread PSYOPS information by embedding it in web flows, or the conscious manipulation of others to spread ones messages. The latter case is the most controversial. Kinniburgh and Denning suggest the possibility of "clandestinely recruiting or hiring prominent bloggers … to pass the US message", but note the potential negative consequences if such practices are uncovered (2006:10). A phenomenon which would provide an online echo of the scandal surrounding an IO contractor planting stories in the Iraqi media in the early days of the occupation (see Mazzetti and Daragahi, 2005). Of course, in the Web 2.0 environment, where the link between a "cyber persona" and a real individual is fuzzy, the use of conduits does not necessarily imply the co-optation of an individual, rather the use of unattributed social media personas or websites can in a sense be seen as conduits – this slippery nature of identity is a key point of analysis of developing SOCOM CY-OPS practice.

Strategic communication doctrine says that in the online information environment the military must "set the agenda", and that "seizing the initiative will apply as much in the cognitive domain as to physical one", necessitating forms of "pre-emptive" engagement (DOD - *Strategic Communication JIC,* 2009:14). It is in the understanding of building up credibility on online platforms, relationships with conduits, and intelligence of audiences under the paradigm of "information engagement" that this requirement is addressed. The paradigm addresses the requirements of strategic thinking, and builds on the doctrinal base to present a way of thinking about new practices which addresses the Web 2.0 information environment in a sophisticated and dynamic way. It builds on an intellectual basis which pays much more attention to the production of information from the warzone (rather than just the control and spinning of it); an understanding of the *processes* of communication through online communication flows and new forms of influence; the role of intelligence about both communication flows and audiences; and, the development of new ways of distributing PSYOPS information which address the limits of military of

credibility. This paradigm for engaging with the information environment is described in current *Operations* doctrine as the "science of control", about *understanding* the environment and the *limits* of influence, and *engaging* in a *dynamic* way as part of broader military strategy (US Army – *FM 3-0,* 2008:6-1, emphasis added). The next chapters explore these developments in cutting edge military practice and R&D thoroughly – demonstrating information engagement as a key paradigm driving the construction of a contemporary propaganda apparatus. Before that, however, the concluding section of this chapter examines cutting edge thought in a particular area of special operations which demonstrates the influence of information engagement in developing military practice.

4.6. Special Operations PSYOPS and Unconventional Warfare

This chapter began by discussing the important role of special operations in the GWOT – developing an understanding of the role JSOC and SOCOM have played in conflict underlining the importance of the relationship between technology, communication and war; and a description of the influence of key approaches on broader DOD practice. Through SOCOM, special operations is central to the emerging strategic approach under the 'indirect approach' to Digital Age conflict in which social, political, and communicative elements are key features of war. Furthermore, as the official PSYOPS coordinator and key practitioner, SOCOM is the key site of development of "information engagement" practices within the DOD. This chapter concludes by bringing the strategic and practical developments together again in exploring a particular aspect of special operations, *unconventional warfare* (UW), and describing how developing discourse in this area addresses Digital Age conflict with important practical outcomes.

UW is one of a number of disciplines within special operations which involve subversion, infiltration, and operations in undeclared warzones. It is officially defined by the US Army as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt or overthrow a government or occupying power by operating through or with an underground, auxiliary and guerrilla force in a denied area" (US Army Training 18-01, *Special Forces Unconventional Warfare,* 1-1). UW "seizes on and supports existing political, military and social infrastructure to accelerate, stimulate and support decisive action based on calculated political gain and U.S. national interests" (Petit, 2012:23). In simple terms, it is a doctrinally-outlined and institutionalised form of military interference in political and social developments of foreign countries through the clandestine support of dissident or rebel groups used as proxies for the purposes of regime change or destabilization.

UW doctrine[48] outlines the central role of intelligence and communication in this context: determining "key psychological factors in the operational environment", including "identifying actions with psychological effects" on target audiences; training resistance leaders on "information capabilities"; "shap[ing] popular perceptions to support UW

[48] This publication is not *strictly* doctrine but a "Training Circular" which is "authoritative but not directive", it "serves as a guide" but doesn't stop units developing their own standard operating procedures which aren't included (US Army - *TC 18-01*, 2010,18-01). Doctrinally it is governed by more general Special Operations doctrine which leaves much more room for interpretation (see DOD – *JP 3-05,* 2014; US Army – *ADP 3-05,* 2012).

objectives", and countering "enemy misinformation" (US Army - *TC 18-01*, 2010:1-10). PSYOPS is to be incorporated in all phases of operations and is based in producing "desired behaviours" and "anticipating and controlling psychological effects" of military operations (US Army - *TC 18-01*, 2010:3-6). It is seen as key in 'exploiting' US-supported guerrilla successes to erode enemy morale and support, assisting in building support networks, and increasing "support for the resistance movement" amongst the general population (US Army - *TC 18-01*, 2010:3-6). If you take away the reference to resistance movements, this is basically a description of PSYOPS in all operations 'amongst the people'. This is key in offering broader insight into developing practice, as UW is also the context in which the relationship between Web 2.0, PSYOPS, and intelligence has been most thoroughly addressed in special operations thought.

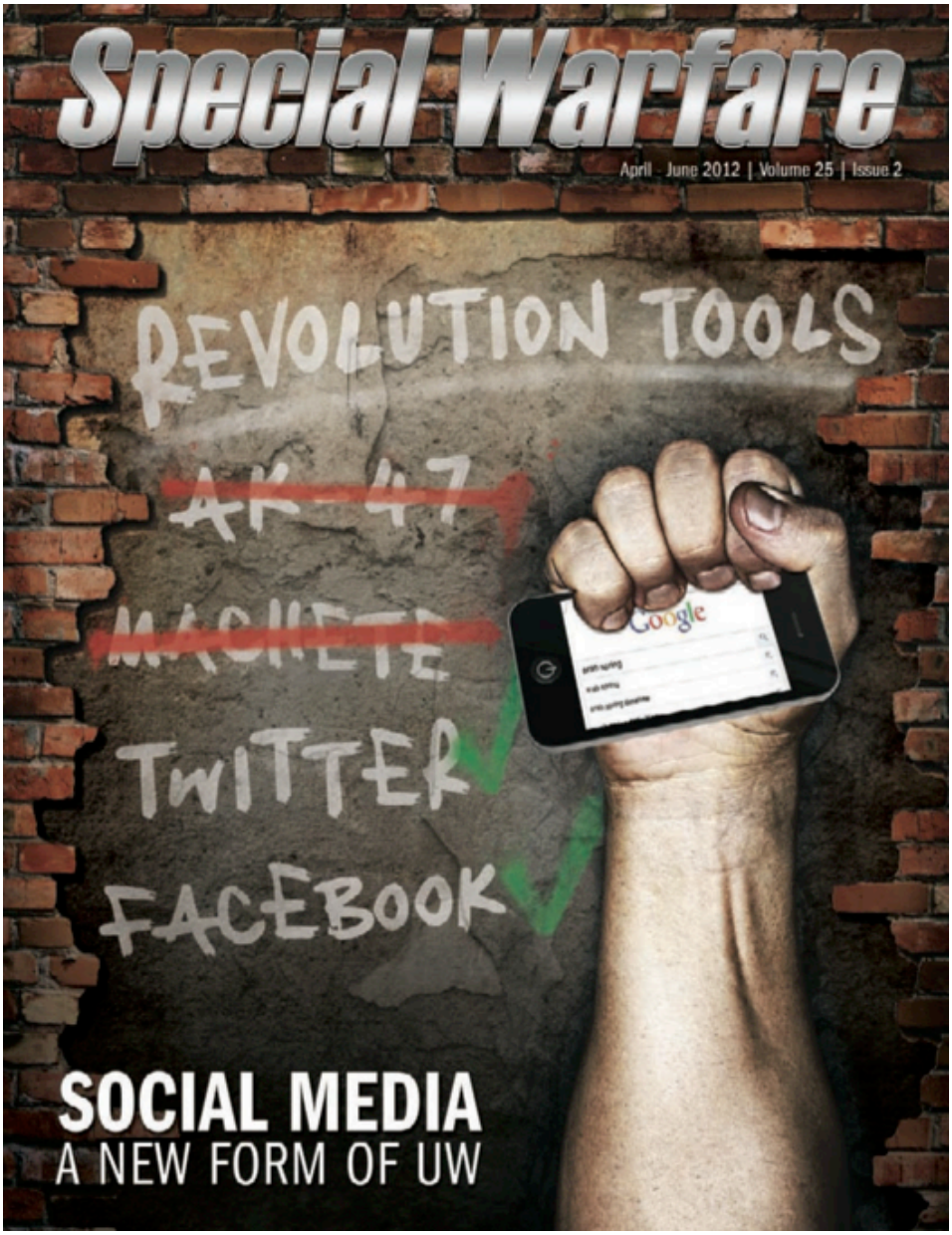


Figure 6: Cover of Special Warfare, 25 (2), June 2012. Published by the JFK Special Warfare Center

In 2012, an issue of *Special Warfare*[49] was published with a cover article (see Figure 6) declaring social media to be "A New Form of UW". This was the first of a number of examples during the research period that demonstrates that UW thought has embraced social media in a significant way (see also Fingerhut, 2013; Reeder, 2013; Lucente and Wilson, 2013; Souter and Heidger, 2013; and Burrell, 2013). The article – by Lieutenant Colonel Brian Petit, the Director of Special Operations Forces Leader Development and Education at the Command and General Staff College[50] – is, like much of the contemporary literature on social media and conflict, premised on the role social media was seen to play in the Arab Spring, which Petit argues has "profound implications for the U.S. special-operations mission of unconventional warfare" which now must "deliberately account for and incorporate social media" (Petit, 2012:22). This position is endorsed by the Commandant of JFK Special Warfare Center, who writes that in the Arab Spring "bloggers, and posts on Facebook and Tweets on Twitter changed the political landscape of one of the most volatile areas of the world. For many of us who practice the ancient art of unconventional warfare, it was a wake up call. We Quiet Professionals must delve into these new realms and learn not only how to understand, but more importantly use this powerful tool in our kit bag" (Reeder, 2013:4).

Traditional UW practice is based on special operators infiltrating hostile environments (in "pilot teams") and liaising with potential allies or conduits in an attempt to empower them to wage an insurgency in line with US objectives (US Army, TC 18-01, 2010:3-3), and then providing training, materiel or operational support to them as proxies in pursuit of US strategic goals. Petit explores the new operating environment of Digital Age conflict and suggests new forms of UW engagement adapted to the new possibilities of Web 2.0 engagement, describing how the combination of "the chaotic power of borderless social mobilization [via Web 2.0] with the lethality and precision of focused military effort" (Petit, 2012:24) can become an important growth area for US special operations.

The most important lesson Petit takes from his analysis of the Arab Spring is the changing role of *leadership* and *accessbility* in resistance movements. In traditional UW doctrine the leadership role is seen as coming from "the underground" which "provides the direction, organization and stewards the strategy for a resistance force", as well as the functions of intelligence, counterintelligence, subversion, propaganda, and tactical direction (Petit, 2012:26). Petit sees the Arab Spring as replacing this revolutionary 'underground', instead being based on a leaderless and decentralised model (following Brafman and Beckstrom, 2008) which, when it was attacked, went overground, finding strength in publicity rather than secrecy, in a "reversal of the UW doctrinal template" (Petit, 2012:25-26). For Petit, this presents an opportunity to supplant the UW interest in liaising with undergrounds with an approach which attempts to steward or subvert existing revolutionary movements, working instead through influencing a decentralised social media-enabled mass. Petit argues that the 'classic' perception of UW as "the underground resistance-cell leaders meeting with U.S. advisors, clustered in a dark basement around a crumpled map, secretly organizing" must be augmented with the addition of "a scattered network of

[49] A journal published by the JFK Special Warfare Center and School, the intellectual hub of the US Army special operations community.

[50] Petit has also previously commanded Special Operations Task Forces in the Philippines (see Strobel, 2008) and Afghanistan (see Petit, 2011).

digerati […] local and global, all texting, tweeting, posting and hacking from thousands of locations" (Petit, 2012:27).

Of course UW is at heart a political activity, and at the strategic level, Petit writes that social media proliferation allows an "information order with an operations annex" (Petit, 2012:25). He outlines a political campaign approach to dynamically engaging in PSYOPS messaging, recognising that in politics the interpretation of a candidate's message is "seldom left to chance" (Petit, 2012:26), and that information must be followed into the information environment and spun along the way, This approach demonstrates a key element of 'information engagement' outlined above, and is evident in the multi-level online information engagement within CENTCOM's Operation EARNEST VOICE explored in section 5.3. Petit concludes that "the challenge is maintaining the psychological initiative where everyone – citizens, states, provocateurs, refugees, media, militaries, hackers – has equal access to information and therefore, influence" and argues that "the [special operations] community must recognize that social media and its rapid and effective proliferation of narrative have expanded the boundaries of the UW battleground" (Petit, 2012:27). Another way of looking at this, of course, is that the proliferation of special operations thought into the field of social media has seen it slip its reigns and move into new areas of social and political life, imperilling democratic and social movements (and certainly placing dissidents, who are often accused of being US proxies, in danger). An analysis of *practical* developments in military practice in the following chapters supports this interpretation.

Petits article in Special Warfare preceded a number of others demonstrating that his ideas capture a zeitgeist within the special operations community which has since been followed up by others, and translated into significant sub-doctrinal and training outcomes (e.g. Lucente and Wilson, 2013; Souter and Heidger, 2013, see sections 5.4 and 6.4). At the level of organisational development, when the plan for advancing Army Special Operations capability laid out its "blueprint for change" in 2013. It describes the near-future operating environment as shaped by the "proliferation of smart phones, mobile devices and social media" which present "opportunities for both adversary and U.S. MISO efforts" (ARSOF 2022 (2013) in Special Warfare, April 2013:27). This environment is seen as allowing the development of "innovative tactics, techniques and procedures for use of social media and other tools to influence foreign target audiences in support of special warfare", and necessitating an increased focus on "use of social media and other cyber-based tools" in the field of social and cultural intelligence with the long term goal of developing the capability for "executing mass and precision influence missions in all environments" (ARSOF 2022, 2013:27).

What this analysis demonstrates is that – as with developments in the indirect approach at the strategic level - far from being stuck in the headlights of Web 2.0 technology; key areas of military activity are addressing and adapting to the changing ICT context, not only to protect the integrity of exiting practices but to develop new one in which Web 2.0 becomes a key enabler. Within the influential area of special operations, tasked with both strategic responsibility (the indirect approach) and practical activity (PSYOPS) in Digital Age conflict, this has led to the development of approaches seeking to put the information environment to work to address both the strategic, intelligence and communication challenges it faces. The area of UW discussed here is that most deeply involved in political

and social conflict, and thus is where the most advanced engagement with new Web 2.0 technology and social features have been most thoroughly articulated. As we will see in the next chapter, the ideas and context of adaptation presented in this section are echoed within the broader special operations community – and the problematic nature of Web 2.0-enabled UW in addressing broad areas of social, political and communicative life compels us to examine the serious implications as these discourses and practices proliferate into wider military development.

The broad problem field of Digital Age conflict was explored in sections 1.3 and 2.3. At the military or strategic level it was characterised by an important relationship between technology, communication and conflict – which in the contemporary environment was seen to present significant challenges to military activity in terms of the proliferation of non-state actors, the empowerment of adversaries in irregular warfare. This problem is amplified by a disadvantageous information environment which produces great instability due to the phenomena of emergence, convergence and information doers which displace traditional information flows. This chapter moved on from this broad conception of Digital Age conflict *as a problem,* and examined military discourse which approaches the field in a more direct and constructive way, examining how it is "made amenable to intervention" (Miller and Rose, 2008:15). We have seen that in addressing the problem field key military actors have identified not only challenges, but *opportunities.* With the new information environment facilitating a number of key developments in the GWOT strategic environment. This understanding of the problem field forms the direct basis for the development of the propaganda apparatus examined in the following chapters.

5. SOCOM, CENTCOM, and the Emergence of a Digital Age Propaganda Apparatus

As well as being the key site of intellectual and conceptual development in Digital Age conflict, the US Special Operations Command (SOCOM) is the location of major practical development in the field of online military communication – pushing new CY-OPS practices and information engagement strategies. This chapter describes the institutional context of these developments, and present the range of practices which make up a Digital Age propaganda apparatus. Drawing on documentary material this chapter pays particular attention played to the role of *Trans-Regional Web Initiative* online news websites, the activities of *Military Information Support Teams* which embed special operations communicators within embassies, and the role of PSYOPS forces working for US Central Command (CENTCOM, which covers the Middle East and Central Asia) in directly engaging with foreign audiences via Web 2.0 platforms. This research represents, to my knowledge, the most comprehensive examination of contemporary US PSYOPS in media, academic or policy writing. It allows the development of an understanding of Digital Age communication power beyond one based merely on content or the control of conflict information flows or influence at the point of mediation, to one based on *information engagement* which addresses the shaping and integration of military information into the communicative space of the online information environment, and embeds special operations activity within the weft and weave of Web 2.0 communication.

5.1. SOCOM as PSYOPS Hub in the Global War on Terror

In identifying areas of interest for the research within the DOD, this chapter builds on the outline of the problem field of Digital Age conflict outlined in the previous chapters, which (in common with most work on military communication practice) identified the area of Information Operations, and PSYOPS in particular as the key military activity, with particular interest in these activities within a special operations context – where the 'tip of the spear' of both GWOT military activity and Web 2.0 adaptation has been identified. The focus on the SOCOM and CENTCOM also stems from an in-depth analysis of all potentially-relevant military units across the DOD in terms of their online communication activities. I investigated a number of groups, from combatant commands through to individual units, in order to assess their relevance to the subject at hand – see Appendix A for a list of groups examined and a discussion of data and methods of analysis. This comprehensive search confirmed that all developments of interest to the research interact with SOCOM at some point, thus it forms the most important location of analysis in this chapter.

The rise of the SOCOM to prominence was shown in chapter 4 to be one of the key elements in understanding US military strategy in the GWOT, and it is the most important location of DOD adaptation to Digital Age conflict. The Command has a large degree of autonomy compared to the other combatant commands: it has its own R&D and investment capacity, a much more flexible budget (indeed it has continued to grow significantly while most other areas of the DOD have shrunk, Khalili, 2014), and operates with a degree of secrecy that inhibits both political and public oversight (Ackerman and Ambinder, 2012). Under the 'indirect approach', unlike the regionally-focussed COCOMS it

has broad responsibilities as the lead organisation in the military element of the Global War on Terror (Olson, 2008:14), tasked with "shaping … the global environment" to make it less hospitable to terrorist groups (see Comer, 2010; Olson, 2010:819), it is also specifically tasked as PSYOPS lead within the DOD and it is primarily in this capacity that the Command's activities are of interest in this chapter.

SOCOM's bureaucratic importance in the area of PSYOPS is – like its strategic role – best understood in the particular context of the post-9/11 military environment. A report by the Washington-based Stimson Center thoroughly examines the development of "public diplomacy-like activities" (that is, activities which attempt to engage with and influence with foreign publics) at the DOD during this period[55] and outlines how a broad-based, mass audience, strategic form of PSYOPS became the domain of SOCOM, meeting the post-9/11 impetus within the DOD to engage in the 'battle for hearts and minds' (Rumbaugh and Leatherman, 2012:7). The authors identify policy changes (DOD – *Information Operations Roadmap,* 2003; DOD – *QDR Strategic Communications Execution Roadmap,* 2006) which placed PSYOPS within the remit of SOCOM and called for a substantial increase in funding for the discipline - "this wealth of resources drove most psychological operations conversations out of strategic communication [which at the time was a concept on the verge of official doctrinal recognition] and … into special operations" (Rumbaugh and Leatherman, 2013:27) making it the key beneficiary of the shifting IO paradigm identified in section 4.5. SOCOM had a longstanding relationship with PSYOPS dating back to a coordinating, training and equipping role as early as 1993 (see SOCOM, 2008:2), but in 2011 it was specifically designated as the "policy proponent" (with decisions on doctrine and budget) for PSYOPS (CJCS, 2011), giving the Command further influence in the area (see also DOD - *Directive 3600/01*, 2013).[56]

Since 2008 SOCOM has been tasked with developing a "strategic PSYOP force", which it has done under the name of Joint PSYOP Support Element which later became the Joint Military Information Support Command (SOCOM, 2008:20)[57], which was set up to "plan, coordinate, integrate, and, on order, execute strategic and trans-regional PSYOP to promote U.S. counterterrorism goals and objectives" (SOCOM, 2008:20). As this is the only area in which *strategic* and *trans-regional* PSYOPS is discussed in the DOD, it is key to understanding the focus on the Web as both concepts infer a large, broad audience accessed through public channels (such as the Internet), and take the idea of PSYOPS beyond (typically leaflet or radio-based) messages which affect only those in areas in which troops are active. The examination of developing *trans-regional* PSYOPS policy and structures in this chapter, particularly through the *Trans-Regional Web Initiative* and the activities of special operations PSYOPS forces, demonstrate the key role that SOCOM has come to play in this area.

---

[55] The Stimson report is based in a level of data access that it seems only Washington-based think tanks producing work for policy-makers can realistically achieve – with the cooperation of key figures across the organisational spectrum and access to official documents not available to the public.

[56] At this time, other elements of IO – such as military deception, computer network operations, and public affairs – were assigned to other commands for policy control, showing a discrete focus within SOCOM on the psychological element of IO.

[57] During the wars in Iraq and Afghanistan, JMISC staff worked on the Information Operations Task Force in Iraq, the Joint Psychological Operations Task Force in support of CENTCOM in Qatar, and in an Special Operations Forces Task Force in Iraq (SOCOM, 2008:21).

Along with SOCOM, the geographic combatant commands also took an increased role in PSYOPS during the post-9/11 period amid political pressure on the DOD to generalise engagement in the "battle of ideas". This was because the military services (Army, Navy, etc.) and policy branches (the Pentagon-based DOD elements) were "loathe to cloud their well-defined missions with a vague task like public diplomacy" or strategic PSYOPS. However, the geographic combatant commands "already have a nebulous mission" (running a variety of operations across large regions of the globe from the quasi-diplomatic to direct military engagement), and thus saw incorporation of public communication tasks as a useful way to increase their bureaucratic influence over policy in their regions of responsibility (Rumbaugh and Leatherman, 2012:7). The role of the largest one of these, the US Central Command (CENTCOM), which has responsibility for the Middle East and Central Asia (and thus the wars in Iraq and Afghanistan) is examined in this chapter – and exemplifies the role of PSYOPS at this regional level. Through examining the developments of PSYOPS in both SOCOM and CENTCOM, this chapter explores all identified CY-OPS practices in the DOD's emerging Digital Age propaganda apparatus.

5.2. The Word From The Top: DOD Policy and the Move Towards CY-OPS

In developing an understanding of developments of SOCOM PSYOPS activities, I have noted both the strategic and institutional drivers. Bringing these contexts together, we can see the seeds of the current approach in two rather innocuous policy directives, issued in 2007 as Web 2.0 platforms were growing in importance, assigning roles in dealing with this new environment to SOCOM. These directives empowered SOCOM to develop Internet-based public communication activities which have become *the* key CY-OPS activities.

The first policy-level engagement with the proactive use of Web 2.0 tools for public communication[58] came in June 2007 in a document called "Policy for Department of Defence (DoD) Interactive Internet Activities" (Secretary of Defense – *Policy on DoD IIA*, 2007, which is still standing policy, see DOD- *Current DOD Issuances,* 2014). This policy guidance defines Interactive Internet Activities (IIA[59]) as "the use of a system accessible via the internet which allows for two-way communications, e.g. email, blogs, chat room, and internet bulletin boards, in a timely, if not real time basis; as opposed to a system in which information flows only one way", situating the term directly within the Web 2.0 paradigm. The document describes these activities as "an essential part of DoD's responsibilities to provide information to the public, shape the security environment, and support military operations" and states that the policy particularly applies to public affairs[60] and to "programs, products, and actions that shape emotions, motives, reasoning,

[58] Previous policy *had* covered the use of Web 2.0 tools, but only from the perspective of balancing the danger to operational security with the perceived PR benefit of allowing soldiers using social media to give a 'human face' to the military (see Knopf and Ziegelmayer, 2013).

[59] Confusingly, IIA is also used as the acronym for Inform and Influence Activities in more recent Army doctrine (see page 80), they are not the same thing.

[60] The public affairs guidance in the document is basically a direct application of standard PA principles to online media, which also authorizes PA officials to give official statements to blogs with large enough

and behaviors of selected foreign entities" (Secretary of Defense – *Policy on DoD IIA*, 2007:1). Significantly, this is the first (and relatively early) policy level engagement with Web 2.0, providing guidance explicitly for the use these new ICTs in support of military operations to conduct PSYOPS, note the latter part of the above quote is the doctrinal description of PSYOPS/MISO (see page 83)[61].

Authority is delegated to the geographic COCOMs and SOCOM. They are not given a completely free hand however – there are a number of qualifications which give insight into the types of activities IIA involve. The first qualification applies to content of communication, and specifies that all communications must be "accurate and true in fact and intent" (Secretary of Defense – *Policy on DoD IIA*, 2007:2), guidance which seems fairly straightforward. However, it is then directly contradicted by guidance on attribution which states that communication must be attributable according to one of three methods. Firstly, "U.S. attribution", which is open acknowledgement of the source "in the content of the email or product, or in the initial phase of engaging in online exchanges" – this form can be seen in, for example, posts by CENTCOM's Digital Engagement Team on various forums (see page 132). The second is "concurring partner nation attribution", which is using local partner nations as a conduit for communication – potentially exploiting their credibility or authority and thus masking the true source of the communication, which was identified as a key element of "information engagement".

The third "method of attribution" is described as "non-attribution", allowing the dissemination of information "without clear attribution", with the caveat that "when asked if the U.S. Government or DOD is the source of the specific activity, DOD will acknowledge its involvement as soon as operationally feasible as determined by the Combatant Commander unless "a Combatant Commander believes that [this acknowledgement] will not be possible due to operational considerations" (Secretary of Defense – *Policy on DoD IIA*, 2007:2). So, the third form of 'attribution' is actually disguised communication which commanders can argue from a privileged position may never be disclosed. The policy states that "this method is only authorized for named operations in the Global War on Terrorism, or when specified in other Secretary of Defense Execute orders" (Secretary of Defense – *Policy on DoD IIA*, 2007:2). This reference to "named operations" in the GWOT leaves the scope very large, as SOCOM is involved in a number of named operations designated by the prefix "Operation Enduring Freedom" covering large parts of the world for an unlimited time period (see for example OEF-Horn Of Africa, OEF-Trans Sahara, and OEF-Caribbean Central America – see e.g. SOCOM – *Budget Justification Book, RDT&E,* 2012:viii). How communication which uses conduits or completely masks its authorship can be true "in intent" is not clear, and the issue of being limited to "truthful" content is a classic *canard* in propaganda studies in which the selective use of truthful information can be far more effective – and less risky – than the use of false information in instrumental communication.

---

audiences (Secretary of Defense – *Policy on DoD IIA*, 2007:2), echoing PA doctrine discussed in section 4.5. This guidance is basic online adaptation for PA spokespeople and does not affect military communication strategy our outcomes in the way changing PSYOPS policy does.

[61] The document also tasked USSOCOM with producing a publication on "Best Practices for Interactive Internet Activities" to be updated on an annual basis. During the research I requested a copy of this document from SOCOM, though a spokesperson told me that such a document was never produced due to organisational restructuring meaning the authority for producing the document was discontinued.

In August 2007, the IIA policy document was followed by another memo, this time outlining policy on "Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences" (Secretary of Defence – *Regional Websites,* 2007). This directive described "the production and maintenance of [COCOM] regionally oriented websites" as "an essential part of the responsibility" of commanders to "shape" the information and operational environment (Secretary of Defence – *Regional Websites,* 2007:1). This document directly addressed the growth of COCOM-run news websites – which there were two of at the time – which consequently developed into the SOCOM-administered Trans-Regional Web Initiative, discussed in the following section.

The policy guidance gives COCOMs the authority to "produce and maintain regionally oriented websites tailored to foreign audiences", on which all information must "be accurate and true in fact and intent", and states that "all websites within the scope of this policy will display a disclaimer link that clearly identifies the sponsoring Combatant Command on the homepage of the website" (Secretary of Defence – *Regional Websites,* 2007:2). COCOMs are instructed to work with the State Department and other agencies to "coordinate themes and messages, orient to and emphasize specific issues, and recruit regional contributors and key communicators" in running these websites, and it is emphasised that all material should be designed to support the GWOT and counter ideological support for terrorism, which should be synchronized by SOCOM (Secretary of Defence – *Regional Websites,* 2007:2), representing a key capability in its "indirect approach".

This policy statement led, within a year, to an expansion of the use of regional news websites by COCOMs, overseen by SOCOM (through the Joint Military Information Support Command, Rumbaugh and Leatherman, 2012:29-30). The new SOCOM-administered Trans-Regional Web Initiative took control of the existing PSYOPS news websites which had begun under the European Command, and worked to create more – developing a "centrally-managed web site architecture" to run websites in different regions and serving as "the trans-regional synchronizer for all content" (SOCOM, 2008:2). In the following 7 years SOCOM built the TRWI into a significant news provider, with 10 regional news websites and magazines in areas of US military interest across the world. It became the biggest online PYSOPS project in the DOD, thus the process of SOCOM's running of these websites, their content and audience is examined below.

5.3. The Trans-Regional Web Initiative: SOCOM's Global Online News Empire

The Trans-Regional Web Initiative (TRWI) evolved as an institutionalisation and expansion within SOCOM of the operation of regionally-oriented news websites run as PSYOPS programmes at a regional level during the 2000s. The idea of regional news sites originated with a news-aggregating website set up during the Balkan war in 1999 called Balkan-info.com, run by the infamous IO contractor the Rendon Group (USA Today, 06/12/2013; Bamford, 2005). This site later became the *Southeast European Times*, and the programme continued with the creation of *Magharebia* to cover North African news in 2004, with both sites run by EUCOM under a program known as ASSURED VOICE

(Rumbaugh and Leatherman, 2012:28)[62]. After the 2007 directive these websites passed over to the control of SOCOM, which used the model to create 8 more regional news sites across the world, ending up providing content in 20 different languages[63]. These websites are identified in table 1, and example front pages are shown in figure 7. All sites have the strong appearance of independence, covering multiple regions around the world in a number of languages, and have all the features of regular news websites: multiple short news pieces and longer features posted daily, comment functions, social media integration, and polls. The initiative has grown to be the most significant producer of DOD-sponsored PSYOPS content.

The 10 websites I have identified[64] share a number of key features: they are all run through contracts SOCOM has with General Dynamics IT; all are available in English (this is specifically "English (UK)" as SOCOM seeks to avoid any suggestion its sites are aimed at US audiences (Altman, 2013)) as well as local languages; all are attributed to the relevant Geographic Combatant Command in an "About Us" section accessible through a link at the bottom of the page and feature a DOD disclaimer about liability on another separate page; all are frequently updated, and have a number of interactive features (comments function, like/dislike voting per article, and Facebook and Twitter integration of some sort). These websites are a key element of the DOD's Digital Age propaganda apparatus, and an examination of these various elements allows us to develop an understanding of how the nature of military communication is changing in response to Web 2.0.

[62] All Geographic Combatant Commands have PSYOPS operations with the "VOICE" designator of which public news websites are core operations – the others are: OBJECTIVE VOICE (Africa Command); EARNEST VOICE (Central Command); CLEAR VOICE (Northern Command); RELIANT VOICE (Pacific Command) and SOVEREIGN VOICE (Southern Command) (Rumbaugh and Leatherman, 2012:18).

[63] As well as regional news sites SOCOM runs 3 military to military sites (www.agorarevista.com; www.apdforum.com; and www.dialogo-americas.com) focusing on defence industry news and regional military cooperation, I have not included these sites in the analysis as they are not based on appeal to a large public audience.

[64] Extensive searching found no further TRWI websites: this involved examining DOD documents, Senate and House testimony; government-funded and independent analyses of the TRWI program; advanced searches for domains bearing the boilerplate DOD disclaimer text used on all identified TRWI websites; and looking at URL-registration records which found no other relevant websites registered by the employee of General Dynamics IT whose details are associated with all identified TRWI websites.

Figure 7: The English version of the front pages of SETimes and Magharebia on 10/08/2014

Website	Languages	Region
SES Türkiye (www.turkey.setimes.com)	**English, Turkish**	**EUCOM (Turkey)**
Southeast European Times (www.setimes.com)	**Albanian, Bosnian, Croatian, English, Greek, Macedonian, Serbian**	**EUCOM (Balkans, Greece, Romania, Bulgaria, Moldova)**
Al-Shorfa (www.al-shorfa.com)	**Arabic, English, Farsi**	**CENTCOM (The Middle East, Iran)**
Mawtani (www.mawtani.al-shorfa.com)	**Arabic, English, Farsi**	**CENTCOM (Iraq)**
Central Asia Online (www.centralasiaonline.com)	**English, Farsi, Russian, Urdu**	**CENTCOM ('the 'Stans', Iran, Pakistan, Afghanistan)**
Magharebia (www.magharebia.com)	**Arabic, English, French**	**AFRICOM (North Africa - from Mauritania to Tunisia)**
Sabahi (www.sababhionline.com)	**Arabic, English, Kiswahili, Somali**	**AFRICOM (Djibouti, Kenya, Somalia, Tanzania)**
*** Agora Revista (www.agorarevista.com)**	**Spanish**	**NORTHCOM (Mexico and other South and Central American countries – though they are outside of NORTHCOM AOR)**
Info Sur Hoy	**English, Portuguese,**	**SOUTHCOM (Central**

(www.infosurhoy.com)	**Spanish**	**and South America)**
*** Dialogo-Americas (www.dialogo-americas.com)**	**English, Portuguese, Spanish**	**SOUTHCOM (Central and South America)**
Khabar South Asia (www.khabarsouthasia.com)	**Bengali, English, Urdu**	**PACOM (India, Sri Lanka, Bangladesh, Pakistan, Maldives, Nepal, Bhutan)**
Khabar South East Asia (www.khabarsoutheastasia.com)	**Bahasa Indonesia, English**	**PACOM (Southeast Asia)**
*** Asia-Pacific Defence Forum (www.apdforum.com)**	**Bahasa Indonesia, English, Thai, Standard Chinese**	**PACOM (Pacific region of military cooperation)**

*Table 1: List of Trans-Regional Web Initiative websites. Those marked with a * are military-to-military cooperation websites, not general news ones.*

5.3.1. The TRWI Contract

The contracting documents with General Dynamics IT offer a key starting point in understanding the websites, as they offer insight into the aims, requirements and rationale for the program. The contract to run the TRWI in 2008 (FBO – SOCOM, 2008) states that SOCOM requires "the capability to posture for rapid, on-order global dissemination of web-based influence products and tools in support of strategic long-term U.S. Government goals and objectives", it describes TRWI as "an internet architecture [...] which [COCOMS] can use as necessary in support of the Global War on Terror" (FBO-SOCOM, 2008:5). This coheres with policy documents relating to the program – identifying it explicitly as a network of influence platforms in the GWOT context, making it an important and extensive CY-OPS project.

The contract outlines further specifications beyond simply providing websites: the contractor must provide information to help the U.S. government "shape the global media landscape … exploit new and emerging Internet technologies and techniques" including video and podcasts, polls, blog integration, and other multimedia (FBO-SOCOM, 2008:6). Contractors should also seek links to appropriate national and regional news sites (FBO-SOCOM, 2008:8) to embed the DOD sites within regional media environments. Here, already, we can see a development in the nature of military communication – one which recognises shaping and becoming embedded in the *space* of the global information environment as a key element. Contractors must also plan to include moderated chat rooms, incorporate blogs and "strive to involve and incorporate target audience generated content to the greatest degree possible" (FBO-SOCOM, 2008:11) – recognising engaging with the public as involved in co-creating the space of online communication (and thus, online influence) as key. This request for interactivity and embeddedness within the media environment show that from the outset, this CY-OPS programme operates at a level beyond the grasp of traditional understandings of propaganda based on semantic content alone.

The contract is quite clear on the content of the TRWI websites – contractors are responsible for the collection and production of content and are asked to "develop, a network of indigenous content stringers and staff of editors" (FBO-SOCOM, 2008:6), and to "identify, develop, obtain and maintain a network of native/indigenous content contributors" with expertise in politics, sport, culture, security and "other aspects of the GWOT, which appeal to foreign target audiences" (FBO-SOCOM, 2008:12). Much of the content is expected to come from third parties such as wire services, press releases from US and partner governments, blogs and sports websites – it is to be of general broad appeal and "not replicate the role of DOD public affairs" (FBO-SOCOM, 2008:11). Importantly, all content has to submitted to "the owning COCOM for review and approval prior to posting on the website" (FBO-SOCOM, 2008:10). This introduces an explicit layer of DOD filtering of content, and despite one ex-Magharebia editor's claims that this is a formality and "a single person at EUCOM would look at the text, and generally approve it as is" (Critalli, 2011), the mere existence of such a filter is likely to influence editorial choices and decision-making as contractors internalised the values of the DOD – and carry out the explicitly instrumental form of communication stipulated in the contract.

General Dynamics IT were awarded the contract, to run the TRWI from September 2009 until September 2014 for which they were paid $121m (FBO-SOCOM, 2011). However a number of other companies have had a role in running the TRWI, as can be seen through information posted on the recruitment website LinkedIn and elsewhere. These companies are L3 (a large military contractor specialising in information warfare who worked on the TRWI between 2007 and 2009, likely as an interim measure while contract was out to tender), Jacobs Technology (a large military contractor with IT contracts at SOCOM and CENTCOM (Jacobs Technology, 2014), which worked on the Spanish-language websites) and Concepts and Strategies, Inc (a small communication contractor which specialises in "Cyber engagement and analytics" (ConStrat, 2014), which had a market research-type role). The contract expired in 2014 and in late 2013 SOCOM posted a new solicitation on FBO for the continuing TRWI project (FBO-SOCOM, 2013). However, due to budget cuts across the DOD and some high-profile criticism of the program (discussed below) it was discontinued in 2014 (see Vanden Brook, 2013; Altman, 2013), which at the time of writing was the situation, as confirmed by a SOCOM spokesperson. Although General Dynamics was continuing some websites through contracts directly with regional commands by late 2014 (see Mazmanian, 2014).

5.3.2. An Analysis of the TRWI Websites

The following sections present an examination of the content of TRWI news websites in order to understand both the extent of their influence and the ways the programme compels us to develop our understanding of CY-OPS and the developing propaganda apparatus. This research is based on a qualitative content analysis of the websites as a whole (rather than a story-by-story formal content analysis). This process was based on gaining an overall impression of the content of the websites, how they function, and how they engage users and fit into the broader new media ecology. It involved an examination of the design of the sites themselves and the immersive analysis of coverage over a one month period (1-31 November 2013, where I visited the websites daily, made notes of impressions, and captured articles of interest) which looked at all stories posted, the

subject matter covered, their sourcing, levels of audience feedback and engagement through social media, and web analytics which show integration in broader online news flows.

In order to examine the general content of the websites and the role of audience participation there is simply no formal or quantitative quick-fix for analysis which can substitute for a qualitative engagement with a small sample of content over an extended period of time, and for an unstructured analysis of social media engagement and other forms of interactivity. This does, of course, mean that any analysis is liable to be subjective – in recognition of this, I have fully laid out the rationale for coming to certain conclusions or drawing certain inferences, as well as referenced the comments of others where possible. Furthermore, Appendix B presents a table outlining the details of the various websites and notes on qualitative analysis.

This approach to analysis was taken as the TRWI websites are most usefully understood as operating under a notion of military influence that is based on building up audience relationships and integrating military communicators into communication spaces (as outlined in contracting documents and the information engagement paradigm) rather than the case-by-case presentation of information supporting a military agenda which might be expected under a traditional understanding of PSYOPS. This is not to say that the news content of these sites is not distorted in favour of US interests, this analysis finds examples where this the case, and the contract to run the sites *states quite clearly* that content is to be instrumental in supporting US aims in the GWOT. As such, the analysis takes as a given that the websites are instrumental communication to further US military objectives. The analysis thus focuses on understanding *how* they operate as part of a propaganda apparatus, through studying broader dynamics of winning target audiences, integration into online news environments, and positioning for long-term strategic influence.

5.3.3. Attribution, "Cloaked" Websites, and Embedding in Online Information Flows

The most basic element in assessing the news websites is that of attribution. It is clear from contracting and policy documents that they are part of PSYOPS practice which is explicitly aimed at influencing foreign populations as an instrumental part of GWOT strategy. But, is this clear to the websites' users? All the websites feature an "About Us" page which clearly states that the website is "sponsored by" the relevant COCOM, with further explanation along the lines of "for supporting and enhancing US efforts to promote stability, co-operation and prosperity in the region" (Magharebia - *About Us*, 2014 – see figures 9 and 10). This is a clear statement of attribution, however to find this information users must scroll to the bottom of a fully-featured and content-rich news site and click the "About Us" tab. Otherwise the sites have the appearance (with the exception of their lack of advertising) of any other independent news website. Rumbaugh and Leatherman say they have "the strong appearance of civilian journalism" (2012:17), each with its own branding, identity, and no further mention in the content of links to the US military – even in stories which are effectively COCOM press releases (see e.g. Magharebia (14/07/2011) "AFRCOM Chief Visits Mauritania", and Al-Shorfa (30/11/2010) "US Military Hands Over Imam Ali Airbase").

Figure 9: Example of Magharebia landing page – "About US" section is at the bottom and requires scrolling down to see

Figure 10: Magharebia "About Us" section – typical of all TRWI websites

In writing on the problems of the link between ideology and information in online news, Daniels has presented the concept of "cloaked websites" which "conceal authorship or feign legitimacy in order to deliberately disguise a hidden political agenda" (Daniels, 2009:661). Such websites challenge users to browse the web with the understanding that "values are part of the process of evaluating knowledge claims" in the online world (Daniels, 2009:675) to a degree which may jar with the somewhat seamless nature of

surfing the online information flow. Daniels emphasises that investigating "authorship and deep research on sources is imperative" (2009:676) to understand the links between information online and the ideology of those providing it, but that for the casual web-user these practices can be time consuming, difficult or require of a degree of internet literacy which not all web users have (Daniels, 2009:666).

In this context it is possible that a website need not concertedly hide all aspects of its identity to mask its authorship – many users may never check the 'About Us' section of a site which looks like a normal civilian media platform. Are the TRWI sites, then, 'cloaked"? The individual branding of each site, and the breadth of coverage, does masks the authorship of the site to some extent, and the claim of ownership in the "About Us" section can be assumed to be passed over by many readers. However, it also allows the DOD to credibly claim full transparency and maintain legitimacy, putting the onus onto the user to inform themselves about the source. In this respect, the norms of online publishing ("About Us" disclosures are standard transparency devices) and the practices of Web 2.0 news consumption (engagement with multiple news sites without close scrutiny) facilitate the potential 'cloaking' of the PSYOPS agenda without diminishing the credibility of claims to transparency.

This issue is further complicated by the fact that website content becomes embedded in social media information flows (e.g. articles are Tweeted, shared on Facebook), meaning a potential engagement from users on an article-by-article basis (rather than concerted or habitual use of the sites) which makes investigation of authorship even less likely. This research shows that the DOD has explicitly used social media to build audiences based on peer-recommendation. When an news article is linked to by a friend or someone within a user's online social network it draws credibility from the social position of the person who linked to it – further diminishing the chances of a user 'clicking through' to read the disclaimer. Embedding sites within flows of information in social networks in which credibility is inferred through personal relationships has been identified as a key growth area by theorists of information engagement (see. e.g. DSB, 2008:420; Collings and Rohozinski 2009:2), but it is also a bread-and-butter of Web 2.0 media promotion and marketing, meaning our understanding of a CY-OPS practices must develop (as those practices themselves have), in line with broader contemporary practice in online communication.

Beyond embedding in social media flows, many TRWI websites are integrated to a significant degree within the online news ecology of their regions of interest and beyond. In discussing the success of the TRWI programme in 2013 one of its creators, Roger Smith, said that "400 to 500 articles a month are reposted on other websites, some considered unfriendly to U.S. and allied interests" (Altman, 2013). This type of integration further 'cloaks' TRWI authorship – placing it (at least) another hyperlink away from the "About us" disclosure. Another, lesser form of cloaking, can be seen in other websites hyperlinking to (but not reposting) articles from TRWI sites, thus implicitly endorsing them as legitimate sources of information. Both these forms of integration into the broader information environment (hyperlinking and reposting) effect our understanding of 'attribution' of the websites in question.

The web analytics service *Alexa* allows users to access a list of websites which feature links to a given domain. This service is by no means comprehensive (for example the

Twitter feeds of each site would account for thousands of links to each, but are not included), but does offer some insight into how stories posted on TRWI sites have an audience beyond those who visit the sites through highlighting a number of other sites which link to SOCOM-sponsored domains (notes on the analysis I undertook of Alexa-identified links are in Appendix B). For this research Alexa provided lists of links to TRWI domains, and I examined particular links from English-language news websites or other popular sites familiar to me – a qualitative analysis which was not exhaustive or comprehensive, but is helpful in producing an understanding of the breadth of links and various ways TRWI sites are integrated into the flow of news in the online information environment.

All of the TRWI websites are hyperlinked to in a variety of news sources on the English-language web. For example, relevant stories are sometimes included in the "around the web" selection of links at the bottom of Huffington Post news articles, in lists which include stories from more reputable sources such as the BBC, Reuters and national newspapers (see, e.g. Huffington Post, 10/02/2013; 22/01/2013) – conferring on them legitimacy of both the Huffington Post and by implication the sources they are listed among. These links are not manually selected by Huffington Post, and are automatically generated through an algorithm that chooses similar stories based on web searches, demonstrating an *algorithmic* embedding of CYOP material into online information flows. At the more manual level, a number of stories from all TRWI sites are linked to in the Wall Street Journal's "Risk and Compliance" blog (e.g. Wall Street Journal, 17/06/2014; 26/07/2013) which rounds-up international news stories relating to corporate compliance and investment news. These examples demonstrate that being 'on the radar' of either a link-producing algorithm or a journalist who aggregates a lot of content can have significant impact in potentially driving readers to TRWI sites. This allows the sites to benefit from the reputation of more credible media actors, and become embedded in an online news ecology which has benefits in terms of traffic to the website, credibility, and search engine optimisation.

In a more *ad hoc* way, stories from all the websites are included in hyperlink form in various mainstream news articles as references for quotes originally recorded in TRWI-site articles, or for events which have happened for which the link is provided for verification or further information. In most cases these are non-controversial events or quotes – such as news of a summit taking place (Sabahi, 25/06/2013), research findings being released (SETimes, 05/01/2012), or reporting on crimes announced by officials (InfoSurHoy, 08/08/2013), and links are included as it is standard practice in online news to hyperlink to a source for more information. As is the norm with hyperlinked-references on many online news platforms the source of the link is not mentioned in the text, and where it was mentioned all but one instance examined in the research (BBC, 07/09/2013) failed to identify the TRWI source as in any way linked to the US government or military.

Most of these links are fairly innocuous, but in the research sample there were a number of examples in which SOCOM-funded news websites are used as the sole source for claims which – had their source been known by the audience – would likely be judged worthy of further scrutiny. These included a hyperlink in a CNN story (CNN, 07/01/2014) to "media reports" of the Afghan police stopping a 12-year old girl from becoming a suicide bomber, this link is to a Central Asia Online (21/11/2013) story which is based entirely on the

statements of Afghan officials – a source which journalistic norms suggest should be treated with some scepticism. A number of Central Asia Online stories using only Afghan or Pakistani official sources are quoted in online publications (see, e.g. International Business Times, 14/09/2013; Dawn, 19/12/2012) – indicating that its role as an easily accessible English-language source in the area allows it to be readily integrated into international coverage. This has the effect of spreading CY-OPS-produced 'news' into the wider media ecology, reproducing statements from US or US-linked sources which are worthy of more scrutiny in a sanitised context, and reinforcing the credibility of the TRWI websites themselves.

An examination of such reposting of content during the sample period suggests the role some websites play in producing English-language news from areas of relative scarcity is significant. Al-Shorfa, for example, covers the Middle East and Iraq, and is quoted relatively infrequently compared to the other sources suggesting the existence of quality news coverage from other reputable sources diminishes its chances of being reproduced readily in international publications. Conversely, there is relatively wide reference to Sabahi's Somalia stories, where there are few English-speaking news sources: Yahoo News (15/11/2013) quotes one story extensively as its sole source on an article about al Shabaab (Sabahi Online, 14/11/2013); CNN uses it as a source for confirmation of a reconstruction conference taking part in Somalia, ironically in an article headlined "Why [the US] should keep out of Somalia's affairs" (CNN, 02/08/2013); and it was also used as a reference in the Daily Beast (12/01/2014), Foreign Policy (04/11/2013) and the Canada Star (02/10/2013). Again, the source of these references was never disclosed to be the US Government, never mind a special operations PSYOPS programme.

The above examples are all *ad hoc* incorporations by news providers of links to TRWI sites because they publish information of relevance to the story being presented. This is standard practice in contemporary journalism and produces the environment of hyperlinked information which is a key feature of the online news ecology. However, this multitude of links to TRWI sites – especially with no disclosure of the organisation behind the site – provides them with legitimacy, drives traffic to them, and further complicates the notion of attribution. The reproduction of their information on more established news sites certainly means that information gets to audiences in situations where it is extremely unlikely they will read the "About Us" section and find out the information comes from a PSYOPS programme. However such hyperlinking is not unusual and we must allow some agency on the part of journalists producing these stories. The majority of the links are to uncontroversial facts or to statements attributable to others, and one suspects that in cases where TRWI sites were breaking news unreported elsewhere or were the only organisation reporting it then journalists would scrutinise their sources further. Hyperlinking to the BBC, or Voice of America, or Fars as a source does not necessarily mean a journalist is being co-opted by the UK, the US, or Iran – the more significant issue here seems to be one of boosting the credibility (and search engine rankings) of the sites, further masking their SOCOM sponsorship and heightening the potential for more mendacious forms of CY-OPS.

There are a number of cases in which this 'cloaking' effect is more dramatic – where stories from TRWI sites are posted in full on other news websites. The research found that this is a common occurrence on nationally-focussed blogs, which often act as content-

aggregators for news on particular topics and repost full stories from other sources (see e.g. BangladeshWatchdog, 15/08/2013). Some sites post TRWI content more consistently: the TheMuslimTimes.org blog posted 13 full stories from Khabar South Asia and 4 from Khabar Southeast Asia in 2013, in line with stories from other sources and simply a "Source: Khabar" acknowledgement at the bottom. Similarly, the small news and comment site HondurasWeekly.com has re-published 59 articles from InfoSur Hoy on its website with "This article was originally published by Inforsurhoy" as the source note. Khabar South Asia seems to be the most advanced in this practice of reposting on other sites – with its stories being reproduced not just in blogs but on the websites of national newspapers. The Bangladesh Chronicle has posted 16 stories in full from Khabar, with "Source: Khabar South Asia" at the bottom of the article as the only attribution. Indeed, the only time it has mentioned Khabar and the DOD together is (ironically) in an article (reposted from another, different, source) criticising the existence of the TRWI site, saying "it is inappropriate for a military behemoth to run a news-and-analysis portal aimed at the Southasian public, for it can only be a masquerade" (Bangladesh Chronicle, 03/04/2012).

The biggest influence of Khabar South Asia however is through a Bangladeshi news site called Natunbarta, the 4th most popular news site in Bangladesh. Natunbarta has posted over 400 articles based entirely on stories from Khabar – including complete re-posts and stories in which Khabar articles are the only source. These stories often contain hyperlinks to multiple Khabar articles on similar subjects (e.g. Natunbarta, 11/10/2013). This involvement with Natunbarta is – in terms of article numbers – the largest integration with another news source which the research identified. It demonstrates how effectively TRWI sites can be masked without technically hiding sponsorship, as well as acting as a platform for the integration of PSYOPS content into a national news environment. Bangladesh accounts for the majority (over 70%) of Khabar's readership, and though it is only the 1,414 most popular site in Bangladesh, through its relationship with Natunbarta (the 4th most popular news site in the country) it has an important conduit to a much larger audience – where its content is presented in a much more credible (and more cloaked) manner.

This analysis shows that while technically sticking to the instruction of the DOD and TRWI contract to produce attributable news websites, the TRWI sites are able to integrate into the flow of information in the online news environment in a way which makes it unlikely that the sponsorship of the content will be known by many of those consuming PSYOPS-produced information. In this case the Web 2.0 information environment of hyperlinks, social-promotion of content, and news information flows is an ideal scenario in which CY-OPS practitioners can maintain their legality and credibility (the "about us" attribution is clear for all to see, should they want to), while allowing their role to be masked and their content to be spread and leant credibility by an array of conduits. It is fair to assume that in the case of Natunbarta someone working for the TRWI contractor in the region has stuck a deal with the website to post their content in bulk, but much of the reposting and hyperlinking I have described is simply an organic effect of how content is shared, linked and incorporated into an online news environment. In this case, the TRWI sites (and CY-OPS products more generally) must be understood not just in terms of what goes on in their own pages – but how they provide a platform or base for PSYOPS practitioners to expand their influence and ingrain themselves into the space of the wider information environment.

5.3.4. TRWI Content – Supporting US Interests, But How?

In assessing the content of the websites the approach taken was not a quantitative one of word or topic frequency or other lexical features. Rather, the whole user experience of accessing the websites for news was broadly examined, accessing them on a daily basis and examining the breadth of stories over a one month period, checking social media activity, and reading other media coverage on the same topics (again, see Appendix B for notes on this analysis). Almost all of the websites publish two types of articles: a large quantity (40-200 a month depending on the site) of short articles called 'headlines' or 'latest news', and a smaller amount of longer 'features' articles (18-60 depending on the site)[65]. Headline articles are generally only a few sentences long and do not bear the name of journalists – they report on recent incidents, statements, and reports in the local and international press. 'Features' are longer articles, generally 8-12 paragraphs, and have a byline from journalists working in the region.

Thematically, both 'headline' and 'feature' stories vary from region to region. For example, Magharebia publishes a high volume of sports stories (around 30%), mostly related to North African football, while other articles cover regional political and security developments. Articles from Khabar Southeast Asia, Khabar South Asia, and Central Asia Online focus predominantly on the two issues of regional security (terrorism, regional rebel groups) and of inter-regional and inter-community cooperation (summits, multi-lateral agreements, integration policies, etc.). Southeast European Times and SES Turkiye both focus on inter-community and regional relations and cooperation, as well as regional political and cultural developments. Even within a more unstable area, Al-Shorfa and Mawtani (the Iraqi subsidiary) feature a large number of these stories on national and regional cooperation, in line with the websites stated aim to "[highlight] movement toward greater regional stability both through bilateral and multilateral cooperative arrangements and steps governments take towards stability in Iraq" (Mawtani Al-Shorfa – *About Us*, 2014). On the site which covers South America, InfoSur Hoy, the majority of headlines refer to the drug war in that continent, with others discussing national and international political issues.

Short headline articles generally reference information reported in international media (particularly the AP and AFP wire services) and in regional newspapers, websites and radio. In some cases sources in local government, military, or NGO communities are directly quoted in short stories based on press releases or official statements. While across the sites these 'headlines' generally draw from a wide variety of reputable regional sources, the use of official statements is striking in the case of the Iraq stories which make up the bulk of Al-Shorfa's headlines, in which many have as their sole source on a security incident (bombing, arrest, attack, raid, etc.) a statement by an Iraqi official. This type of sourcing obviously privileges the position of the US-sponsored Iraqi military and police, and interspersing these stories with those by reputable international news sources on a fully-functional multi-lingual news site lends the statements a legitimacy they might not otherwise have. In this cases, Al Shorfa acts as a direct conduit for US client security forces, providing access to the regional and global news media.

[65] Southeast European Times, SES Turkey, and Mawtani publish only 'features', no 'headlines'.

Across the TRWI websites the position which articles take towards US military or government interests varies – the sample period contained stories which both directly whitewashed deficiencies in US allied states, and those which contained information critical of them. For example on Magharebia, the research period covered an election in Mauritania, a key US ally in the region, which was reported in a way that minimised criticism: stories stuck to uncontroversial facts of names, dates, etc. and the completion was marked in a story called "Mauritanian elections end in calm" which stated that African Union observers had "confirmed that no irregularities had been seen" (Magharebia, 25/11/2013a). No articles on the subject mentioned that it was the first election since a military coup five years before, or that it was boycotted by almost all opposition parties who described it as an "electoral masquerade" (BBC, 23/11/2013). However this avoidance of criticising allies is not consistent, for example the Somali-focussed Sabahi does include stories critical of regional US allies, such as "Kenyan anti-terrorism police accused of human rights violations" (21/11/2013), which even mentions US and UK funding of those forces. In such cases, it appears that the credibility of the sites as trusted sources of news can trump the glossing-over of negative coverage of American interests.

These observations on sourcing and editorial stance are superficial, intended only to identify issues of note and points of potential contention. A full analysis of TRWI coverage requires in depth area knowledge of specific regions, and an expert understanding of the news dynamics there. The only such analysis which has been published concerns the coverage of Central Asia Online by a regional expert (Trilling, 2011). Trilling examines the site's coverage of Uzbekistan, and finds that it "has shown a disturbing tendency to downplay the autocracy's rights abuses and uncritically promote its claims of terrorism [as a pretext to crack down on opposition]", which he links to the fact that Uzbekistan was, at that time, a critical supply route in and out of Afghanistan for NATO (Trilling, 2011). Further, Trilling notes that Central Asia Online's position in the regional news environment was made more significant by the fact that many foreign news outlets were denied accreditation by the Uzbek government, and that news sites critical of the government were "routinely blocked" – giving CAO a monopoly on both news-gathering and publication in an area vital to US interests. More worrying still, an Uzbek analyst of stories covering the Uzbek government said that "the authors have access to officials and clerics who customarily refuse to meet independent-minded journalists; they only talk to government-affiliated journalists whose work is approved by [Uzbek intelligence]". One article even quoted a prisoner - "a startling feat of reporting prowess, considering that the U.N. special rapporteur on torture has been denied access to Uzbekistan's prisons for years" (Trilling, 2011). For Trilling, this raises the serious question: "is U.S. taxpayer money being given to a for-profit military contractor to shill for a Central Asian dictator, just because he's a useful ally in the war on terror?"[66].

Wherever the content of TRWI websites has been discussed in relation to U.S. regional interests it has been described - by both critics and supporters - as tailoring content to suit

[66] The links between SOCOM PSYOPS and Central Asian autocracies with poor human rights records do not end here. In April 2013 the 4th Military Information Support Group hosted a joint training event with four officers from the Kazakh military's new Psychological Operations branch (DVIDS, 2013); and in April 2014 a co-director of the CORE Lab (a research and training center linked to special operations, see section 6.4.1) provided instruction in the use of social network analysis in intelligence at the Uzbekistan National Military Academy in Tashkent (CORE Lab – *Facebook Post, 18/04/2014,* 2014).

these interests. On the other side of the fence is Roger Smith, the program manager for the TRWI who "wrote the initial TRWI concept in 2005 while he was still in the Army", who has spoken about the content in similar terms to Trilling (Altman, 2013). In response to Trilling's criticism, Smith says that "it is not Centcom's mission to be the human rights watch [...] this is a counter-terror website" (Altman, 2013). Smith also discusses Al-Shorfa's coverage of the revolution on Syria, saying that its coverage "points out the dangers of sectarian rhetoric, outside sources exploiting the revolution, and extremists scaring off international community. The site also encourages humanitarian efforts and takes a position that political transition in Syria should be led by the Syrian people and supported by the international community" (Altman, 2013)[67]. A statement which acknowledges that coverage is guided to support U.S. policy goals – as is ingrained in the policy and contract.

The content of TRWI sites is explicitly politicised – as a PSYOPS product which focus on counter-terrorism goals and on promoting regional stability, this prerogative is clearly built into the program. However, this politicisation does not lead in a direct way to coverage which predictably supports US interests and cheerleads for US activity across the board. The vast majority of stories are not directly related to US interests, which can be understood less directly as a way of becoming a trusted source and credible voice, as building up a reserve of good faith which is necessary to be effective in PSYOPS. Yet there are also cases in which coverage does demonstrably support US interests in a more direct way.

These two elements of coverage need not necessarily be seen as contradictory. Rather, in the context of 'information engagement' it can be argued that the general coverage and limited criticism of the US builds a base of credibility from which this more selective coverage can benefit – a strategy which taps into the key Web 2.0 imperatives of engagement, credibility, and consistent and structured engagement in the online space as a pre-requisite for influence in the new information environment. This understanding underlines the necessity for an analysis of contemporary state communication power which moves beyond a focus on content as the site of analysis. Of course content is important (as the Uzbekistan example shows), but the instrumentality of the communication is admitted and inscribed in the programme, and analysis needs to be at least as subtle as the PSYOPS platforms under investigation. Much of the content – the innocuous reports on football, regional cultural events, etc. – is not directly instrumental, and instead must be understood in terms of its role in constructing an audience, integrating PSYOPS platforms into the online news space, and other less-direct forms of influence. The next section underlines this in describing how the websites act as platforms for audience engagement.

5.3.5. Audience, Interactivity, and Information Engagement

Although there are no comprehensive statistics on the use of TRWI sites in the public domain, there are a number of means to gain insight into the extent of their usage. SOCOM released a statement with the stats for one website, telling Trilling that a monthly analysis

[67] This statement was made in mid-2013, before the Syrian conflict spilled over in a serious way into Iraq with the rise of ISIS/Islamic State

of Central Asia Online found it received 168,000 visits from 85,000 unique visitors, and 380 reader comments per month (Trilling, 2011). Central Asia Online is available in Urdu, Russian, Farsi and covers all the 'stans' (including Afghanistan and Pakistan) and Iran – a cumulative population of around 66m internet users[68], which means (assuming every user was within this region) 0.13% users visits the site in a month. This is not a huge amount – though there are other metrics of success, including Alexa rankings, social media followers, and engagement using interactive features.

Judging popularity through the interactive elements of the websites themselves is not easy – the use of the comment feature and vote to like/dislike news stories which are available on all TRWI sites varies greatly. Generally most stories get none or only a handful of votes and comments, although some articles which are particularly timely or controversial can get up to around 300 votes and 20 or 30 comments (see, e.g. Magharebia, 25/11/2013b; Al-Shorfa, 19/11/2013), this suggests at least a small potential readership – though whether they are drawn (through social media links or otherwise) by specific stories, or read a lot of other content but only interact sporadically, is unclear. Some of the websites have attempted to add new interactive elements to the site: Magharebia has an interactive section called Zawaya that features video clips intended to instigate discussion, but of the 35 clips posted between January 2013 and February 2014 the majority had 0-5 comments and only 6 had more than 10 – not exactly ground-breaking considering the vibrancy of the North African online public sphere during this post-Arab Spring period.

Another measurable element are the apps for Android phones that are produced by Al-Shorfa. These apps are advertised on the Google Play and iTunes stores as provided by USCENTCOM via "the Open Dialogue Forum, a U.S. Central Command sponsored discussion community"[69]. The apps include one on Arabic calligraphy, one with a collection of "key books that embody the fruits of Arab Enlightenment" (both with 50,000-100,000 downloads), a music app with classic Arabic music (10,000-50,000 downloads); and an app called "Towards Mecca" which uses smartphone location settings to point users towards Mecca, set prayer time reminders, and has "clickable prayer beads" (5,000-10,000 downloads). This shows an attempt at engagement with the hi-tech mobile market as well as an indirect approach to influence – through the provision of useful tools unrelated to war to try and win 'hearts and minds'. The use of these apps show relatively large numbers engaging with TRWI-linked cultural products through mobile technology, and demonstrates another facet of "information engagement" which uses new technology and non-discursive tools to engage with foreign publics[70].

[68] Figures from the World Bank: sum number of internet users in each country (World Bank, 2013a, 2013b)

[69] There is no further information available about the "Open Dialogue Forum" and requests for clarification from CENTCOM were ignored. At the time of writing – with no other evidence of the Forum's existence - it seems to be simply a notional 'Forum' to add some credibility to CENTCOM's app production.

[70] Of course, the fact that CENTCOM curates key texts of the "Arab Enlightenment" and classic music will be of interest to students of orientalism, and until an app developer examines the code of "Towards Mecca" we will need to assume that the fact that an organisation notorious for using mobile phones to target Muslims in drone strikes producing an app which geo-locates users to point them to Mecca is a case of cultural insensitivity rather than a sinister targeting ploy.

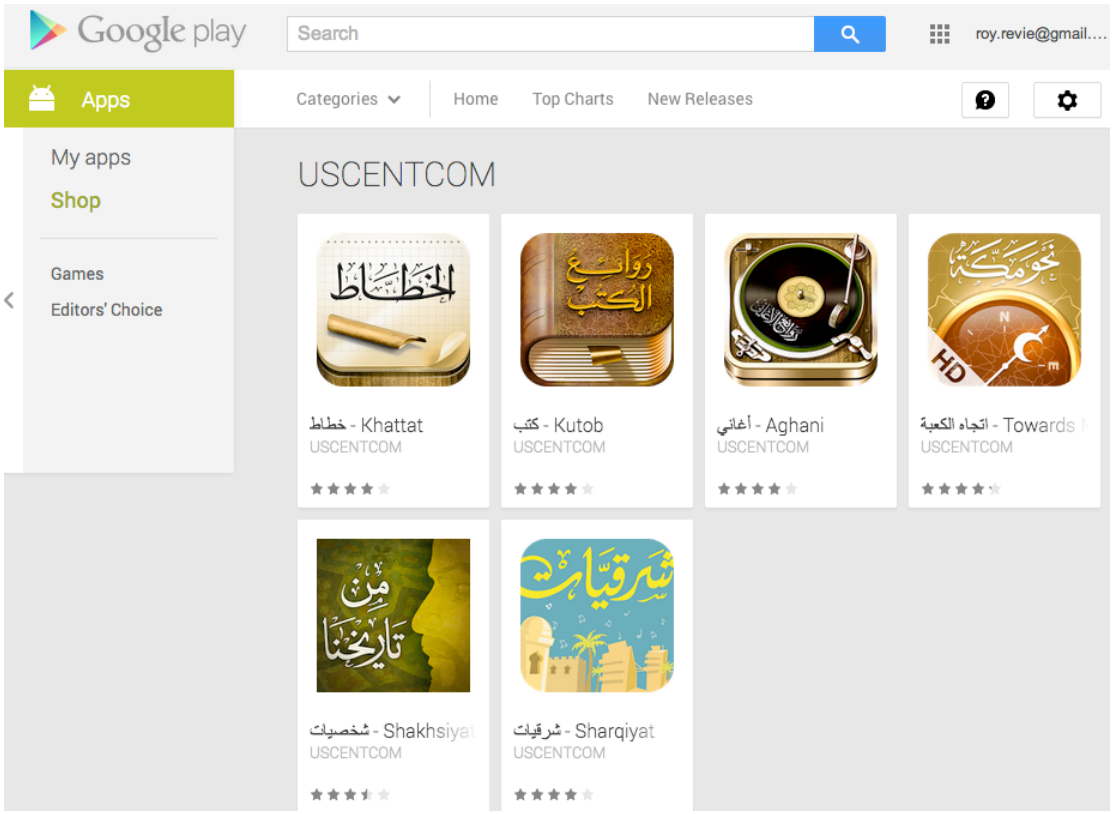


Figure 11: USCENTCOM Google Play store

Another common way to measure the popularity of websites is using Alexa web analytics. Alexa provide a number of metrics on website usage – particularly important here are a break down of the percentage of site visits from certain countries and the rank of that sites popularity within those countries. Alexa rankings are a rough guide (based on popularity over the previous 3 month period and in some cases with underdeveloped infrastructure country information is missing), however it offers some insight into the popularity of TRWI websites. Data for all TRWI websites is presented in Table 2, showing a variance in popularity between websites and locations. The most notable relative successes (I have highlighted those in the top 1500 websites in a country – a generous interpretation of 'success') are Al-Shorfa in Iraq and Yemen, and Magahrebia which is relatively popular in a number of countries across North Africa – particularly in Mauritania and Libya. Some other sites are relatively popular in one country: InfoSurHoy in Costa Rica, Khabar South Asia in Bangladesh, and Sabahi in Kenya. Though in this later case it is worth noting that the stats on this site are skewed by the popularity of a single article on quail farming[71], which suggest that the amount of traffic in cases where websites are around the 1000-mark in terms of popularity – if it can be skewed by one popular article – is not very large. These statistics show that while TRWI sites cannot claim to be wildly popular in any of the countries they cover (and in most cases would be unlikely to be commercially viable) they do have a significant share of audience in particular countries.

[71] 34.27% of searches recorded by Alexa which led to Sabahi were for "Quail farming", this links to the most popular article on the site by far which is about the rise of quail farming as a small business in Kenya.

Website	Percentage of Audience (rank in that country)
Al-Shorfa	Egypt: 24.6% (3,181); Iraq: 14.2% (1,118) ; Yemen 10.6% (988)
Mawtani	Sub-domain of Al-Shorfa
Central Asia Online	Pakistan: 47.6% (4,121); US: 10% (207,831); Iran: 8.1% (23,084)
Magharebia	Algeria: 23.3% (1,136); Libya: 22.7% (395); Morocco: 15.9% (1,008); Tunisia: 12% (831); US: 6.6% (151,543); Mauritania: 4.6% (150)
Sabahi	Kenya: 47.7% (952)
Southeast European Times	Turkey: 28.5% (18,119) U.S.: 27% (176,569); Greece: 10.1% (16,423); Serbia: 4.9% (12,276); Bosnia and Herz: 4.8% (4,106); Albania: 3.4% (3,250); Macedonia: 3.0% (3,794)
SES Türkiye	Sub-domain of SETimes (hence large Turkish audience share)
Khabar South Asia	Bangladesh: 69.9% (1,414); India: 17.4% (118,278)
Khabar Southeast Asia	Indonesia: 83.3% (8,788)
InfoSurHoy	Costa Rica: 32.1% (1,002); United States: 13.8% (309,916)

Table 2: Alexa rankings for percentage of website users (and popularity ranking in that country) for all TRWI websites.

Another accessible way to measure success of the websites in connecting with a target audience is through analysing the popularity of social media profiles and integration which the sites use. All TRWI sites feature some level of Facebook and Twitter integration, which allow an assessment of popularity based on quantitative factors (numbers of 'likes' or followers) as well as a qualitative assessment of the activity (and inter-activity) on these platforms. An assessment of the Twitter presence of the TRWI found that all of them used Twitter only as a broadcasting platform, using an automated system to publish links to each article published on the site – it was not used as a platform for feedback or discussion. Consequently almost all of the Twitter accounts associated with the websites had very low followings, making them largely insignificant in the information environments in these regions (for example Al-Shorfa's 784 Twitter followers are dwarfed by Al-Jazeera Arabic's 1.4m and Al Aribiya's 3.1m).

Website Name	Facebook "likes":
Al-Shorfa	36,533
Mawtani	48,000
Al Aribiya (Arabic)	5,500,000
Al-Jazeera (Arabic)	6,100,000
Central Asia Online - Farsi	1,932
Central Asia Online - Russian	14,846
Central Asia Online - Urdu	45,932
Central Asia Online - Total	62,710
KhabarOnline.ir (Iran) Not TRWI	135,015
The Nation (Pakistan)	278,000
Dawn (Pakistan)	407,510
Rimmow (Mauritania)	17,873
Al Watan-Libya	95,002
Al Chourouk (Tunisia)	98,755
Ennahar (Algeria)	192,000
Tuniscope (Tunisia)	440,000
Magharebia - Arabic	504,619
El Khabar (Algeria)	733,000
Hespress (Morocco)	1,700,000
Youm7 (Libya)	4,000,000
Sabahi (Arabic)	6,188
Sabahi (Somali)	16,848
Sabahi (English)	20,575
Sabahi - Total	43,611
Balkan Chronicle	1,638
Independent Balkan News Agency	1,971
Balkan Insight	15,402
South European Times (English)	580,582

Website Name	Facebook "likes":
Sabah	327,000
SES Turkiye	413,191
Hurriet	698,674
Milliyet	744,089
Habertурk	978,638
The Himalayan Times (Nepal)	15,607
Khabar South Asia (English)	37,177
Central Asia Online - Urdu	45,932
Natunbarta (Bangladesh)	105,042
Bangla News 24 (Bangladesh) - Urdu	849,789
Indian Express	877,593
Times of India	4,500,000
Jakarta Post (Indonesia)	14,371
Khabar Southeast Asia (English)	46,598
Bangkok Post (Thialand)	145,000
The Inquirer (Phillipines)	650,000
Tribun News (Indonesia)	1,100,000
Merdeka (Indonesia)	1,300,000
InfoSur Hoy (Spannish)	44,095
El Pais (Costa Rica)	47,978
La Nacion (Costa Rica)	255,871
Milenio (Mexico)	261,000
El Spectador (Colombia)	658,600
El Tiempo (Colombia)	781,600
El Universal (Mexico)	1,030,000

Table 2: Showing number of Facebook "likes" for each TRWI website with comparable regional websites. There is no comparable site for Sabahi.

On Facebook, however, every TRWI website has a significant presence. Table 2 charts the number of 'likes' that the Facebook pages of each TRWI site has, and for comparison the equivalent metrics for other popular regional news outlets are included[72]. All TRWI sites maintain a Facebook account in at least one language, with most having between 36,000 and 62,000 followers. The strength of following in comparison to media competitors varies greatly – for example in Iraq and the Middle East Mawtani and Al-Shorfa's following appears insignificant next to the millions of followers of Al-Jazeera and Al Aribiya, while the two Khabar sites in Asia have followings towards the lower end of the spectrum compared to national news websites, but more 'likes' than the top English-language news websites in some of the countries they cover (The Himalayan Times in Nepal and Jakarta Post in Indonesia).

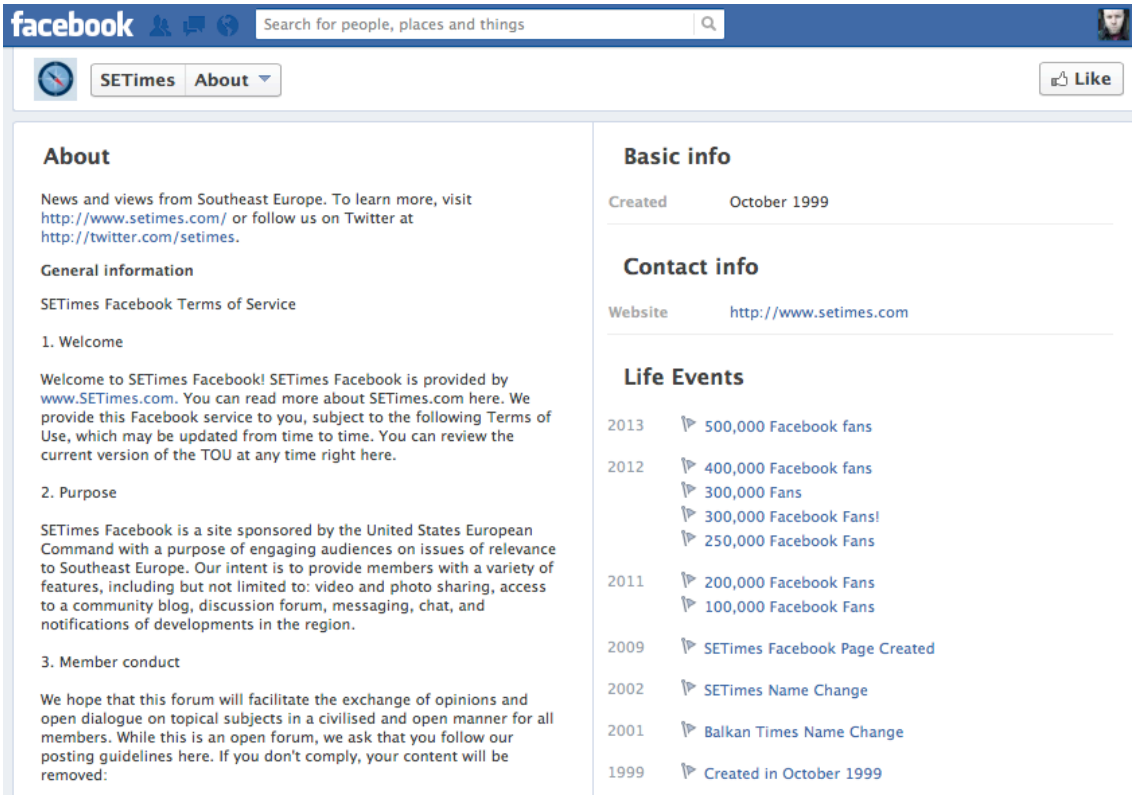


Figure 12 – SETimes very successful Facebook page's "About" section.

The real success stories in terms of Facebook following are the EUCOM-linked sites SES Türkiye, Southeast European Times (SETimes), and Magharebia[73] – with around half a million 'likes' each (e.g. see figure 12). While they do not surpass all regional outlets, the following of SES Turkiye and Magharebia place them in the middle of the rankings of national newspaper Facebook activity in their area of interest, with the later only being bested for popularity by the top news sites in Algeria and Morocco. This Facebook following is particularly significant when seen in conjunction with the fact that analytics for the site show that 49.5% of visits to Magharebia come via Facebook (according to

[72] These comparable sites were chosen as best comparators for the TRWI sites: ideally regionally-focused news sites available in multiple languages, though where such sites did not exist, the national newspapers with the biggest online market share and social media presence in the same language as the TRWI sites were used.

[73] Magharebia is run by AFRICOM, but was set up and previously run under EUCOM

Alexa analytics – for all other TRWI sites the figure for Facebook-linked visits is less than 10%). While Magharebia is a pan-Maghreb website and thus not directly comparable to any one national paper, SES Turkiye is focussed on one country and has a larger following than one of the country's largest news sites (Sabah) and around half the following of other more popular national news sites. The success of these Facebook pages implies a much more interactive, Web 2.0-based impact of the PSYOPS websites – something which practitioners have discussed in addressing developing CY-OPS approaches.

As well as providing one means for understanding the reach of TRWI websites, Facebook is also identified by influential PSYOPS practitioners as the "new influence frontier" (Efaw, 2009) and a key "tool in the influencer's toolbox" (Efaw and Heidger, 2012). Efaw and Heidger[74] (2012) published an article on their use of Facebook to built up the audience for the SETimes while working for EUCOM between 2009 and 2011, writing that from a military influence perspective "attitudes and behaviors cannot be changed overnight; doing so requires exposure to a persuasive message repeatedly over an extended period of time – a task social networking tools are perfectly designed to accomplish", specifically as part of a larger campaign for influence (Efaw and Heidger, 2012). The authors discuss how they built up the SETimes' Facebook following as a key element in drawing an audience to SETimes, as well as to "provide an additional forum that exposes our target audience to our themes and messages", and establish a platform on which the target audience "are comfortable and familiar" which can be used "during a crisis" as a more directly instrumental communication platform (Efaw and Heidger, 2012).

The authors describe how they used a PR approach, links on the SETimes site, and Facebook advertising to encourage people to 'like' the page. Capitalising on the technical possibilities of the platform, they incorporated a Facebook "like" buttons into SETimes articles – a simple yet important element that meant "when SETimes readers who are also Facebook users click that they "like" something, the action is indicated on their Facebook pages, and shows up on their friends' pages, along with a link to the "liked" content" (Efaw and Heidger, 2012) – providing an important form of free advertising and social endorsement. Once the Facebook following was built up, the team worked on the content: experimenting to find the best time of day to post links to "optimize views and reader interaction while minimizing the risk of becoming a nuisance", the forms of replies to audience members that worked best to keep people interested, and the introduction of 'hooks' like video essays, surveys and informal competitions (Efaw and Heidger, 2012).

As a user-base built up Efaw and Heidger realised they were moving from a platform for SETimes content propagation to something much more interactive. The authors note the success of this approach, meaning that by mid-2012 they had nearly 400,000 'likes', and that the Facebook page was driving a significant amount of traffic towards the site – even if they didn't click on links, users "would still be exposed, three times a day, seven days a week, to [SETimes'] themes and messages " via Facebook content (Efaw and Heidger, 2012). At a presentation at the Information Operations Global 2012 conference, Heidger said that in their assessment, in 7 of the 11 SETimes target-countries the success of the page meant that they were "1 degree of separation" away from *any* Facebook user – meaning that, statistically speaking, it was unlikely that any user in the Balkans or Turkey

[74] Efaw was one of the theorist mentioned in relation to 'information engagement' in section 4.6, we will come across Heidger again in relation to developing unconventional warfare practice in section 5.4.

did not have at least one Facebook friend who was a fan of SETimes (and was thus exposed to the content through the 'likes' of their friends).

When they polled their users for what they liked most about SETimes, the response was largely (72%) that it provided "a forum for an exchange of opinions and dialogues with others in the region" (Efaw and Heidger, 2012). However, it is not all about hands-off discussion, the authors note that the building-up of this audience was important for the direct use by PSYOP practitioners during times of crisis in the region – such as a "flare-up of tensions along the Serbia-Kosovo border" in September 2011 in which they were able to use the Facebook page to "inform the target audience of the actual situation on the ground, thereby discrediting rumors and disinformation". They had also built up enough of an audience that their coverage was the top hit on a search for the incident on Google news, showing an interesting dynamic between the success of PSYOPS programs and the search architecture of Google (Efaw and Heidger, 2012).

The use of Facebook as a tool to build up an audience who are then already involved in a relationship with the site which can be used for PSYOP purposes is explicitly stated: "the fact that our audience trusted the integrity of our information was key to our success" on occasions where direct messaging relating to conflict in the region was used (Efaw and Heidger, 2012). The authors conclude that Facebook is an important influence tool as it allows the exposure of the "target audience multiple times to the crafted content" (in the case of this news site this could be over a period of time up to years) such that in a self-reported poll of users 93% of users said SETimes content "sometimes" or "often" made them "think differently about an issue". The platform also "prompts the target audience to share the message with others", meaning that it both provides a conduit for PSYOP product and allows them to take on a life of their own, such that they found 89% of their audience had conversations at least weekly about SETimes content (Efaw and Heidger, 2012). Efaw had previously advocated – drawing on the concept of "Captology" (Fogg, 2002, see page 87, 181) - the use of social networking tools for "mass interpersonal persuasion", to "put [credible voices in the War of Ideas] into credible mouths" through using Web 2.0 platforms to harness public engagement in spreading US messages (see Efaw, 2009:6), and in this account it seems to been very successful and transferred to other TRWI websites linked to EUCOM.

When PSYOPS practitioners outline the importance of social media platforms in this way, it supports an analysis of CY-OPS as not just a matter of content or broadcasting extent. Instead, it can be seen as the development of a more subtle form of influence which focuses on long-term exposure to messages, the exploitation of peer networks, and the building of audience relationships to be leveraged at times of need for more traditional PSYOPS purposes. This is a form of PSYOPS which focuses on the form of communication as much as the content. It also ties in with the use of social media as used primarily in the attempt to "win relationships" rather than to "win arguments", as outlined by a public affairs officer as the key impetus behind CENTCOM's social media engagement, which is discussed further below (Miles, 2013).

5.3.6. Summary - TRWI and the Emergence of CY-OPS

This analysis presents the US military's largest strategic PSYOPS program as global in scope, producing a vast amount of news content, attracting global audiences with varying degrees of success, and deeply embedded in the information environment. In terms of attribution, content, and audience engagement, the TRWI cannot be properly understood using straightforward binaries relating to openness, instrumentality, or popularity. The websites are technically fully attributed to the regional military command in whose interests they operate – but an analysis of the site design and the integration of TRWI content within global and regional information flows shows that this attribution does not necessarily mean audiences are informed of the provenance of the material. The content of the articles is openly acknowledged as supporting US military interests – indeed is contractually obliged to do so - yet this does not lead to straightforward pro-US coverage across the board. There are some examples of where this agenda is clear, but the majority of articles are not directly related to US interests or activities, building up credibility with the readership in order to be more effective as a PSYOPS platform in the long term. Finally, audience sizes vary widely, in only a few cases making TRWI websites significant news sources at a national level. However a more significant element is the use of TRWI stories as social media content – aiding the building up of audiences on interactive platforms who are subjects of long-term influence, and become conduits of PSYOPS content, passing it into their own social networks.

This level of success has not stopped the TRWI coming in for criticism from domestic politicians who have said that "the costs to operate the websites […] are excessive. The effectiveness of the websites is questionable and the performance metrics do not justify the expense" (Altman, 2013). A US Senate committee recognised the importance of "strategic level information operations" but criticised military involvement, saying they should be the domain of the State Department "with support from USSOCOM, as necessary" (US Senate - *Report 113-004*, 2013). The White House has defended the TRWI, calling it "the [Defense] department's only synchronized online influence effort able to challenge the spread of extremist ideology and propaganda on the web" (Executive Office of the President, 2013:4), though their appeals seem to have been unsuccessful and at the time of writing it appears the initiative will be discontinued in 2015.

Despite this, in terms of our understanding of CY-OPS, the Initiative synthesises many of the ideas found in emerging discourse, and as the DOD's first long-term concerted effort in online influence is a milestone in Digital Age state communication power. It demonstrates a developing propaganda apparatus which must be understood in terms of how it is insinuated into online information flows, engaging with the information environment to both spread its own messages and reinforce its credibility. The Web 2.0 news ecology is used as a space to cloak the instrumental nature of the PSYOPS messages, and to spread messages through a network of conduits – which must be understood in the Web 2.0 context not as individuals who could plant stories or pass on messages, but as an intrinsic feature of the contemporary information environment. That is, in a space of routine hyperlinking, content replicated across platforms, and constant 'sharing' and 'liking' of media material, the concept of 'conduit' is abstracted as Web 2.0 norms and flows supplant what were previously personal or intellectual choices or acts. The TRWI may not remain in its current form, but the developing forms of CY-OPS it has instantiated –

embedded in and born of deep Web 2.0 engagement – are here to stay, and present challenges to the way we think about and analyse contemporary propaganda.

Furthermore, the White House has perhaps over-emphasised the solitary nature of the TRWI, with SOCOM and CENTCOM also involved in a number of other efforts which tackle "extremist ideology and propaganda on the web" in a much more head-on manner. These programs are discussed in the following sections.

5.4. SOCOM's PSYOPS Forces Enter Web 2.0

5.4.1. The Military Information Support Operations Command

As well as being the organisational hub for the TRWI, SOCOM is home to the only full-time PSYOPS units in the US military (Rumbaugh and Leatherman, 2012:17). Like SOCOM, these special operations PSYOPS forces are of interest due to their global focus, their enhanced technological awareness, and the 'indirect' approach to conflict in which the role of broader civilian populations is a major element. The organisation of interest here is the Military Information Support Operations Command (MISOC), which sits within US Army Special Operations Command (USASOC). Within MISOC, the two operational units of interest are the 4th and 8th Psychological Operations Groups (ShadowSpear, 2014), which were known throughout the research period as (until mid-2014) the 4th and 8th Military Information Support Groups (MISGs, see GAO, 2013:8).

The 4th MISG is the more established unit, with responsibility for PYSOPS activity in the CENTCOM, EUCOM, and AFRICOM areas, while the 8th was created in 2011 to take over control of the other regional PSYOPS roles (see SOCOM - *FactBook*, 2012; GAO, 2013:2). The 4th MISG has a long history and expertise in traditional tactical PSYOPS such as surrender messages to adversary troops, leaflet-drops and broadcasting PSYOPS messages on civilian radio frequencies (Zimmerman, 2012). It also has a highly-developed cultural engagement capacity, is well integrated into regional communication initiatives (Bostick, 2011), and – as we will see - is making moves towards further integration of Web 2.0 capabilities. In the context of SOCOM's organisational embrace of online influence tools, the changes within its most active PSYOPS units are an important element of understanding contemporary US military activity in this area.

The role and activity of 4th MISG is laid out in detail in a U.S. Army War College paper by its commander, Colonel Reginald Bostick in 2011[75], who describes 4th MISG as "the only active entity in the Department of Defense (DoD) whose unique mission is to directly target and influence audience behaviours, perceptions, and dispositions, and which operates across the full spectrum of military operations" (Bostick, 2011:1). "Full Spectrum" means that SOCOM PSYOPS forces have influence beyond the direct tactical areas which is traditionally their realm – moving outside of conflict zones and operating during 'Phase 0' in support of the indirect approach. MISGs provide PSYOPS support to

[75] Bostick wrote the paper under the supervision of Micheal Waller, the military academic and author of the post-9/11 PSYOPS call to arms *Ideas As Weapons* (Waller, 2007), and after graduating from the College went on to become commander of 4th MISG, where he had previously been deputy commander (DVIDS, 2011)

regional Theatre Special Operations Commands across the world and joint task forces (that is – supporting SOCOM's global operations) and provide Military Information Support Teams (MISTs) to "various U.S. Embassies worldwide" to support regional communication initiatives, which are deeply embedded in civilian communication programmes (Bostick, 2011:5, SORBHQ, 2013).

5.4.2. Military Information Support Groups, Web 2.0 Intelligence, and Unconventional Warfare

Military Information Support Teams (MISTs) are the most sophisticated of SOCOM's PSYOPS elements. Bostick describes them as SOCOM's "primary instrument to build support within, and counteract extremist overtures towards, local populations through the creation and dissemination of culturally appropriate narratives", they work with U.S. Embassies and "at the highest levels of foreign governments" and "specialize in building partner nation's information capability" (Bostick, 2011;4). Bostick says of these teams that "no other influence force in the U.S. Army can match the cultural, linguistic, and intellectual skills" (Bostick, 2011:4) and describes how they draw on the work of "Cultural Intelligence Cells" which are staffed by analysts trained to the doctoral level, providing analysis from various perspectives (anthropology, political science, history, etc.), fluency in local languages, and the routine production of "regionally-oriented, MISO-related analytical documents" (Bostick, 2011:3) and "social or behavioural expertise (an understanding of how behaviour is influenced)" (Bostick, 2011:10, see also Luce, 2012; US Army, *ATP 3-05.20,* 2013:3-7). This integration of experts echoes the integrated intelligence and psychological operations paradigm at a micro-level, demonstrating the importance for a holistic understanding of contemporary PYSOPS practices and requirements.

Turning to Web 2.0, Bostick discusses both the intelligence value of social media and its importance as a channel of communication: saying that "MISO, along with the rest of [special operations], must adapt to this means of communication", noting that "social media have shed unprecedented light onto what people think and, more importantly, why they think it" (Bostick, 2011:12). Bostick tends to focus on the intelligence value and social effects of social media – echoing the work of Unconventional Warfare writers in saying that it allows "more opportunities to engage in public speech and an enhanced ability to undertake collective action", meaning that target audience analysis (a key element of guiding PSYOPS campaigns) can become "a living document, not something tied to a static piece of paper" which "serves as a dynamic and detailed method for gathering not just intelligence, but also insights into audience vulnerabilities, accessibilities, and susceptibilities in a given culture" (Bostick, 2011:12). In terms of information engagement, we can see the intelligence value of social media is appreciated within the elite of the PSYOPS community, providing easy access to the means to craft and perfect communication strategies, as well as to feed into broader intelligence work.

At the level of special operations education, the 4th MISG is in the process of establishing a "Master Influence Practitioner concept" within its *Intelligence Support to MISO* training course (a requirement for all MISO teams). This is a 4 week course which gives graduates the ability to advise MIS teams on full integration with "DOD and interagency intelligence activities […] with emphasis on target audience analysis and joint targeting" and to use

intelligence software to perform analysis that "will drive the MISO process" (Otwell, 2013:7). An article by Souter and Heidger[77] (2013) on the integration of Web 2.0 into PSYOPS training notes that 4th MISG is "invested heavily in the evaluation of [Web 2.0's] role in 21st century unconventional warfare". Showing practical developments in line with discourse on UW in section 4.6, they describe how strategists within 4th MISG have studied the example of the Arab Spring to develop "contemporary UW tactics, techniques and procedures [TTPs] grounded in historically-sound UW principles to apply to" Web 2.0 in denied or hostile environments as the "emerging conditions of the 21st century UW information environment" (Souter and Heidger, 2013:7).

Souter and Heidger discuss a number of areas which UW theorists drew on. Firstly, in looking for theoretical work on which to base an understanding of the post-Arab Spring information environment the 4th MISG planners drew heavily in the "influence-based revolutionary tactics theorized by Gene Sharp […] a proponent of nonviolent revolutionary activism" (Souter and Heidger, 2013:7)[78]. Sharp's most famous work, *From Dictatorship to Democracy* (1994) outlines almost 200 tactics for nonviolent protestors to take on oppressive governments and has been credited with influencing the 'Colour Revolutions' in the 90s and 00s (see e.g. Polese and Ó Beacháin, 2011; Sussman and Krader, 2008) and the tactics of protestors during the Arab Spring (Gray, 2011; Gay Stolberg, 2011 cf. see Amr, 2011; AbuKhalil, 2011). Sharp's work has been the subject of a number of unfounded theories, suggesting it has been promoted by the CIA to pursue regime change in countries from Serbia to Venezuela (see e.g. Meyssan, 2005, cf. Zunes et al, 2008), and it seems that in this case that SOCOM PSYOPS and UW practitioners are just about to catch up with the conspiracy theorists.

Souter and Heidger note that Sharp's "techniques can be used to unify disparate resistance groups … and mobilize the masses", and that his most visible techniques are "the application of protests, marches and demonstrations […] which are arguably some of the most powerful psychological actions trending in modern times" (Souter and Heidger, 2013:7). In the training exercise, 4th MISG worked to "validate many operational concepts and TTPs based off [sic] Sharp's work", which the authors note they will need more research and training "prior to application to a real-world UW operation" (Souter and Heidger, 2013:7). Nevertheless, the adoption of tactics of nonviolent social movements and their adaptation to a post-Arab Spring information environment and political situation by the main PSYOPS unit in the US military is a significant moment in the use of Web 2.0 for military ends – outlining a military attempt to harness Web-enabled activism in pursuit of US policy goals.

During the development of these new procedures, Souter and Heidger report a particular focus on Web 2.0 tools: including "emerging dissemination methods [and] diaspora-supported social-media messaging"; and "using a combination of social media and boots-on-ground MIS forces" to build up "indigenous resistance-force propaganda cells […] to exploit the combat actions of resistance guerrilla forces, promote the resistance locally

[77] Heidger is the same PSYOPS practitioner who pioneered the use of Facebook to build a following for the SETimes, see page 117.

[78] Other key texts included Guevara's *Guerilla Warfare* (1961). Mao's *On Protracted War* (1938), Kitson's *Low Intensity Operations* (1971), and Gustave Le Bon's *The Crowd: A study of the Popular Mind* (1895). See also Lee (2013) for similar writing on social movements and unconventional warfare

and conduct divisive operations to degrade the hostile regime" (Souter and Heidger, 2013:7). Another key element is identified by others[79] writing on the same topic as "Virtual Pilot Team Operations" (Butkevics and Hannaford, 2013:9) – a Pilot Team being a functional unit in the UW process which assesses the "resistance potential" of potential US allies on the ground. This element is of particular interest as it lays out the social media equivalent of a doctrinally defined activity undertaken in UW, and examples it are found in new technological development discussed in the following chapter.

According to Butkeviks and Hannaford, the new "virtual space connectivity" offers the opportunity for a new approach to UW, meaning that before pilot team actually go into a hostile country they can produce virtual analysis of the human terrain as the basis for a process in which "MISO practitioners can identify, analyze the sentiment of, and virtually link up with, key communicator in the UW operational area" (Butkevics and Hannaford, 2013:9). This provides a "decreased risk" to pilot-team operations, and a capability in "an operational environment where physical pilot-team operations are not feasible or there is a requirement for information faster than a pilot-team operation an be planned and executed" (Butkevics and Hannaford, in Souter and Heidger, 2013:9). In short, the increased use of social media to allow intelligence and communication for PSYOPS operations make UW less risky, quicker to execute, and consequently a potentially more attractive option to planners and strategists.

All of this UW research was incorporated into a large DOD training exercise in 2013 (called JRTC 13-01)[80], demonstrating that UW and PSYOPS practitioners within SOCOM have tested the conception of Web 2.0 and UW outlined by Petit in both education and practical training exercises. Butkevics and Hannaford describe how during the exercise 4th MISG experimented with "enhanced target audience analysis" to fully engage with audiences in the "virtual space" through an "open-source monitoring and analysis cell in order to enhance target-audience analysis and provide near real-time data to inform" the PSYOPS process. This model will "be applied to all the other regionally aligned MISO battalions" once it is fully developed (Butkevics and Hannaford, 2013:8-9). They also reveal that 4th MISG is in the process of acquiring the software and hardware for this type of analysis - likely the sort of software which the subject of extensive R&D within the DOD, examined as a key element of chapter 6.

The revelation that practitioners have studied the Arab Spring for lessons in the use of Web 2.0 technology to influence mass protest strongly links controversial clandestine special operations practice with Web 2.0 and social movements in foreign countries. While this development appears to be in the early stages, in addressing US military practice to foreign dissident populations in such a direct way it is potentially problematic for those groups. The Internet is already represented as a site of US imperialism by many authoritarian leaders, and its (real or imagined) instrumental use by the US to meddle in other country's affairs has already been used as a justification for crackdowns on internet

[79] Janis Butkevics was at the time a PSYOP sergeant with 6th Military Information Support Battalion (Airborne) – a subordinate element of 4th MISG responsible for EUCOM area (see DVIDS, 2012). Hannaford was "serving in the United States Army in Military Information Support Operations", at the time of publication (Hannaford, 2013).

[80] During the research I tried, through both personal and formal avenues, to find more information about this training and experimentation – but secrecy and sensitivity surrounding special operations made disclosure impossible in this case.

users (see, e.g. Price, 2012; Morozov, 2009; 2010). The UW conception of foreign dissident groups as a population to be examined for revolutionary potential and manipulated in certain directions is thus potentially disastrous for those who might wish to use Web 2.0 as a tool for activism – demonstrating the potential consequences of military activity in even a relative niche area on the broader information environment as a space of social and political engagement.

5.4.3. Military Information Support Teams' Strategic PSYOPS Programmes

While the development of Web 2.0 practice in UW is in the early stages, there is an element of SOCOM PSYOPS practice that is well established and adapting to the new information environment: Military Information Support teams. MISTs – small teams of SOCOM PSYOPS specialists - are an important element of SOCOM's 'indirect approach' to building influence across the spectrum of US foreign and military policy. A leaked 2013 Government Accountability Office report (GAO, 2013) studied the role of MISTs and found that in 2012/13 they were located in 22 embassies worldwide (GAO, 2013:9), identifying teams in Afghanistan, Bangladesh, Colombia, Djibouti, and Nepal (GAO, 2013:4). The teams are "comprised of 2 to 10 special operations forces soldiers", and conduct activities "to instil confidence of local populations in their law enforcement, and supporting programs that offer rewards for information, among others", as well as broader messaging governed by SOCOM counterterrorism priorities. Countries with a MIST presence are also the focus of a "global assessment program that focuses on in-depth target audience analysis" (GAO, 2013:10).

Examples of MIST activity in the report include working with USAID in Bangladesh to "incorporate counter-radicalization messages into disaster response exercises"; working with the US Drug Enforcement Area (DEA) in Peru to tie combatting Sendero Luminoso into operations against drug traffickers (GAO, 2013:11); and working with the Colombian government to promote the latter's rewards program in counter-FARC activities (GAO, 2013:12). Additional examples I identified include a MIS team based in Mauritania promoting "good governance" after a military coup (Office of Inspections, Department of State, 2009); and one in Nigeria working on "counterterrorism, countering violent extremism, and promoting Muslim-Christian tolerance" through pubic affairs training for Nigerian security forces, "providing Hausa language educational textbooks for Islamic children", "producing thematic programs with Nigerian radio stations" (Office of Inspections, Department of State, 2013) and "commemorative transcripts and DVDs" of Obama speeches in Cairo and Accra, and setting up a "Yes Nigera Can" Google group with podcasts for "civil society leaders" (U.S. Embassy Abuja, 2009).

MIS teams also operate in support of JTF-Trans-Sahel (the SOCOM and AFRICOM task force combatting militants in the Sahel) through a "countering violent extremist ideology" programme. This activity focuses on the "identification and vetting of credible local voices already active within the community who are advancing themes and messages consistent with the MIST's desired attitudinal or behavioural change", and promoting "messages already organic to the environment in lieu of creating new and foreign messages" (Boehnert and Nasi, 2013:12). These "credible voices" are then brought on as 'partners' (or conduits) and MIS teams support them through ensuring "the proper targeting and scope of desired target audience" and providing "subject-matter expertise and technical

advice in target-audience selection, message construction, product development" and measuring effectiveness " (Boehnert and Nasi, 2013:12). In support of these initiatives MISTs can also access "production assets" back home which are "capable of producing and editing radio and TV broadcasts, as well as printed media", though practitioners in the area note that "as new communications platforms and their use continue to increase in the Trans-Sahel region, MIST teams are drafting plans and implementing series that capitalize on the growing popularity of the Internet and, specifically, social-media platforms" (Boehnert and Nasi, 2013:12). MIST members working in the Sahel describe social media tools as likely "the future of messaging and … an ever growing area of interest and activity for MISTs who will sit at the intersection of time-tested messaging practices and emerging technologies in the evolving media landscape" (Boehnert and Nasi, 2013:12). The form of such engagement with Web 2.0 technologies is likely to draw on the lessons of the TRWI and development of UW techniques – placing cutting-edge CY-OPS practice in the heart of a key area of complex conflict, and at the heart of the 'indirect approach' which MIS teams represent.

One example found during research demonstrates the convergence of MIST practice and Web 2.0 technologies well: it comes from a classic piece of dirty data', a tendering document posted online from the MIS team stationed at the US embassy in an African country involved in a conflict with Islamist militants[81]. The document asks for a provider to run up a number of youth events, including film viewings, entertainment, and speakers, aimed at an audience of young people from a community perceived as supportive of the Islamist militants – a community which has been identified by journalists and human rights groups as the target of a campaign of clandestine violence by the police and military of the Western-backed government. As well as seeking a contractor to run these events and produce and disseminate publicity material for the forums, the document also stipulates that the contractor will create, manage, and edit a multi-platform website, produce a radio show to be aired on national radio, and run social media presence on all major social media platforms to promote the "peace" events.

The contract outlines all the required pages to be contained on the website, including an "about us" section which is to include the contact information of the contractor or

[81] In the version of this thesis submitted for examination, the African MIS team and the specific country and area of conflict was identified. I also provided references to the primary MIS team tendering documents referred to in this section, as well as contextual material by journalists and human rights groups. Following discussion with examiners it was decided that this example should be anonymised in the final version of the thesis due to the risks associated with identifying youth groups working with US Special Operations teams in an ongoing regional conflict in which civilians are all too often the innocent victims, drawn into the conflict against their will.

This puts the researcher in the somewhat ironic situation of having to redact work which itself seeks to penetrate the veil of state secrecy. It also highlights an important dilemma about the responsibility of academic work to expose injustice. It can be argued that by not publishing details in this case it allows a dangerous situation to be perpetuated (I did contact multiple US military sources for comment or guidance on how to deal with this information, to no avail). However by publishing these details the thesis would be the catalyst for the potential harm identified in the work - the exposure of the programme and endangering of civilians implicated in it.

The ethical code governing academic work demands first that we do no harm, and thus the protection of information which could directly endanger people takes precedence. The anonymous example is strong enough to support the analysis of the treatment of different *populations* on pages 126 and 137, through which the work provides a broader critique of military practice which endangers certain groups of civilians by broadening its approach to conflict.

subcontractor and other pertinent information and a 'partners' link which will identify a number of partners in the initiative, including the contractor/NGO and the local US Embassy. The website is also to have a discussion section in which the MIS team has full power to edit or delete comments, and give final approval for all posted content on social media. Thus, we have a situation in which social media and the MIST-system of embedding in embassies allows the role of a SOCOM PSYOPS team to be hidden very deeply indeed. In this case there is a public forum with various entertainment and speakers, ostensibly run by an NGO or other front group, which also has substantial social media presence, behind which is a website with a single link in the "about us" section which simply lists the US Embassy as "a partner" - when in fact the entire enterprise is being funded and directed not by the NGO, or even the US Embassy, but as a PSYOPS programme by US Special Operations Command.

Like most SOCOM activities, details of MIST programs are not generally in the public domain, and while this was the only project directly related to social media found during the research, it is exemplary in the context of what practitioners have said about MIST development into the social media space. It shows a militarisation of what would traditionally be State Department activity – with the relaxed budget constraints, technical expertise, and clandestine role of SOCOM PSYOPS practitioners allowing them to take over ostensibly civilian outreach programs in areas outside of combat zones. In a sense it even problematizes the notion of what a "combat zone" is, as SOCOM's regional task force extends military thinking from the definite combat zone of in the region in which conflict takes place to the security situation in the broader region. It subsumes social and political space in countries in the region into the 'battlespace' of the regional conflict, which is addressed through the 'indirect' approach's three main elements: working through training and equipping partner nations to fight for US interests, the surgical and clandestine application of US force at key points in the conflict, and the ideological war fought by PSYOPS practitioners.

What this investigation into SOCOM PSYOPS structures shows us is that the broad regional websites run under the TRWI are supplemented by much more targeted efforts to engage on Web 2.0 which more directly pursue US strategic aims through PSYOPS practice. While the TRWI programme is formally transparent, and uses the flows and links of the online news ecology to embed its content in the information environment and enhance its credibility, the work of PSYOPS forces is more clandestine. Material based on military publications on training and development shows the early stages of highly controversial engagement with Web 2.0 in the area of UW. The few examples of activity underlines both the clandestine nature of this new form of engagement and also the potential risk it entails through the militarisation of social and political life. The consequences for the aid workers who are unwittingly drawn into a SOCOM anti-extremism programme in Bangladesh, or the youth workers in an African country fronting a SOCOM-sponsored counter-extremism project are potentially damaging, even disastrous. We have seen, for example, the terrible consequences for health workers (and patients) after the CIA was exposed as using vaccination schemes for spying in Pakistan (see Gambino, 2014; Edwards, 2014) – demonstrating blowback from the instrumentalization of important social programmes. The potential damage to activists, social workers, opposition politicians, and civil society in general is plain to see in developing SOCOM CY-OPS programmes which see Web 2.0 as

a way to manipulate social space and gain access to populations which would otherwise be inaccessible.

5.5. US CENTCOM – CY-OPS Practice in the Heart of the GWOT

While SOCOM plays a key role in overseeing the "global" part of the Global War on Terror, much of the war has been situated within a distinct geographical area – that which covers the Middle East and Central Asia. This region falls under the responsibility of the US Central Command (CENTCOM), the largest and most active geographic combatant command of the US military. Of particular interest to this research is CENTCOM's sizeable psychological operations component, which operates under the umbrella of *Operation EARNEST VOICE*, and spends 10-20 times more than any other command on PSYOPS[83] (Rumbaugh and Leathermman, 2012:20). The TRWI elements through which SOCOM supports CENTCOM activity are the news websites *Central Asia Online, Al-Shorfa*, and *Mawtani* covering the area of operation in Arabic, English, Urdu, Russian, Farsi. There are a number of other programs under CENTCOM, however, which go further in pursuing information engagement through both clandestine and overt means.

In a 2010 statement to the Senate Armed Services Committee, then-CENTCOM commander General Petraeus briefly described two elements of PSYOPS operations. These were the Regional Web Interaction Program (RWIP) and the Credible Voices Program (CVP) (Petraeus, 2010:829), which are described in budgetary material as "USCENTCOM's primary and enduring non-kinetic weapon in its irregular warfare arsenal for countering adversary information operations" (House Appropriations Committee - *Reprograming Action Omnibus*, 2010:58). These are programmes which draw on the commanders privilege outlined in the 2007 IIA guidance (page 80), avoiding attribution and using clandestine means to engage on foreign-language websites for influence purposes, they are discussed below. A separate, public affairs programmed based on transparent engagement with civilian websites – the Defense Engagement Team – is discussed afterwards. These programmes provide further insight into the range of CY-OPS forms, with this scope becoming a significant element in our understanding of how the propaganda apparatus addresses the Web 2.0 information environment.

5.5.1. The Regional Web Interaction and Credible Voices Programmes – Classified Clandestine CY-OPS

Information available about the Regional Web Interaction (RWIP) and Credible Voices Programmes is limited, however that which *is* available allows the development of understanding of another hidden area of CY-OPS activity. These classified[84] programs

[83] For FY2013 CENTCOM's budget for VOICE operations and other "Public-Diplomacy-Like Military Activities" was £29.4m, compared to £3.0m of AFRICOM and $1.5m of NORTHCOM. SOCOM's PSYOPS budget (which includes the TRWI) was $58.9m. In addition to this, a further $122.8m was separately budgeted for PSYOPS in Iraq and Afghanistan, within CENTCOM's area of responsibility.

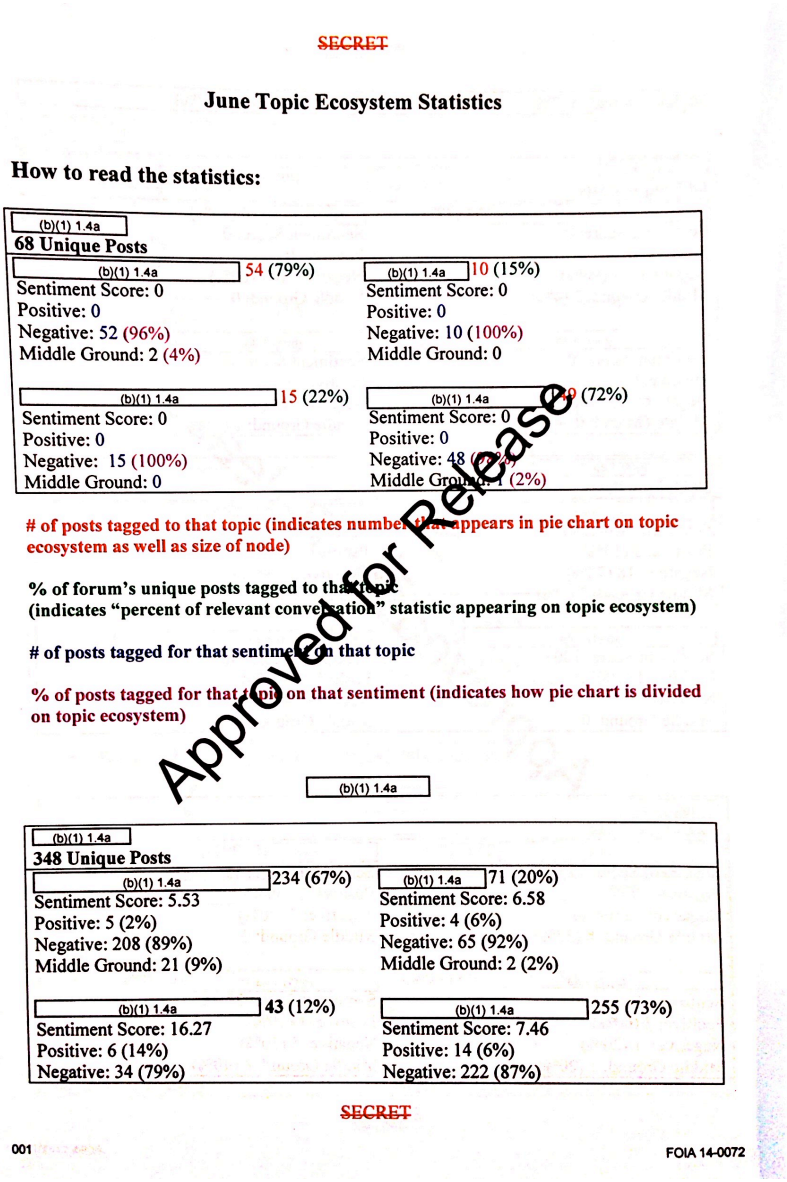
[84] We know they are classified as information on them is suppressed in the transcript of a 2012 congressional hearing (House Committee on Armed Services - *Budget Requests from US CENTCOM, US*

were outlined only in general terms by Petraeus, who said that "RWIP focuses on informing and influencing foreign target audiences to counter violent extremist ideology and enemy propaganda, and amplify messages of credible voices to reduce VEO [Violent Extremist Organization] effectiveness in soliciting recruits and financial support for their operations" (Petraeus, 2010:829). Petraeus stated, further, that "monthly assessments of the RWIP show the positive effects the program has on the tone of discussion threads by shifting sentiment away from support of VEOs" (Petraeus, 2010:830). Information obtained from CENTCOM under the FOI Act confirms these monthly assessments took place (see figure 13) – I was supplied with heavily redacted notes of these assessments from June to December 2010, showing an analysis of 29 un-named internet forums (though one group of forums is tagged as "Taliban Arabic"), listing their post per-month and assessing these posts in terms of their sentiment ("positive", "negative" or "middle ground") relating to a number of topics (all of which were redacted in the material I received apart from "TB [Taliban] Ideology" and "TB A/A Military Operations"). Though the identity of the forums is redacted, from the number of posts-per-month it appears that most of them are small, with the majority having less than 200 post-per-month and between 2-4 forums a month consistently producing more than 1000 posts.

While this material does not provide much insight into the targets or subject of the RWIP operation, it does confirm the existence of a classified PSYOPS programme consistently monitoring and, by we may infer from Petraeus's statement, engaging actively, on these forums. In a 2013 posture statement, the new CENTCOM commander General Mattis described CENTCOM VOICE operations as including "media analysis, internet video products, and multi-media campaigns that include attributable social media *and* the Regional Web Interaction Program" (Mattis, 2013, italics added) which implies that the RWIP includes a multi-media social media element which is *not* attributable (i.e. one where CENTCOM's authorship is masked)[85], emphasising the clandestine nature of this CY-OPS element. A budget request for the RWIP from 2010 gives slightly more detail, saying it "provides capability to engage audience on native language (Arabic & Urdu) web blogs, chat rooms, and social networks", and that staff based in Tampa (CENTCOM shares a base with SOCOM at MacDill Air Force Base in Florida) and Qatar (CENTCOM has a major base in Doha) "continuously engage" on 5 native language forums, carrying out operations on 6 key themes or objectives over the course of a year. This 2010 budget request was for an extension of the program (through a staff increase) to 15 native language forums and more extensive operations-per-theme which was denied by the House Appropriations Committee (House Appropriations Committee, Reprograming Action Omnibus, 2010:58), though FOIA information shows it *has* since expanded at least in terms of forums covered (from 5 to 29).

SOCOM, and US TRANSCOM, 2012:142), and a Freedom of Information Act response I received (see Figure 13) is heavily redacted for reasons of classification.

[85] That these communications are non-attributable also coheres with the data on them having positive effect in 'shifting sentiment': in a study of the *attributable* online engagement of a State Department Digital Outreach Team (see page 135) in 2009, Khatib *et al* (2011) found that the more frequently US-identified commenters engaged in a comment thread the more likely other users were to display negative attitudes towards the US (Khatib *et al,* 2011:11).


SECRET

June Topic Ecosystem Statistics

How to read the statistics:

(b)(1) 1.4a
68 Unique Posts

(b)(1) 1.4a 54 (79%)
Sentiment Score: 0
Positive: 0
Negative: 52 (96%)
Middle Ground: 2 (4%)

(b)(1) 1.4a 10 (15%)
Sentiment Score: 0
Positive: 0
Negative: 10 (100%)
Middle Ground: 0

(b)(1) 1.4a 15 (22%)
Sentiment Score: 0
Positive: 0
Negative: 15 (100%)
Middle Ground: 0

(b)(1) 1.4a (72%)
Sentiment Score: 0
Positive: 0
Negative: 48 (
Middle Grou (2%)

# of posts tagged to that topic (indicates number that appears in pie chart on topic ecosystem as well as size of node)

% of forum's unique posts tagged to that topic (indicates "percent of relevant conversation" statistic appearing on topic ecosystem)

# of posts tagged for that sentiment on that topic

% of posts tagged for that topic on that sentiment (indicates how pie chart is divided on topic ecosystem)

Approved for Release

(b)(1) 1.4a

(b)(1) 1.4a
348 Unique Posts

(b)(1) 1.4a 234 (67%)
Sentiment Score: 5.53
Positive: 5 (2%)
Negative: 208 (89%)
Middle Ground: 21 (9%)

(b)(1) 1.4a 71 (20%)
Sentiment Score: 6.58
Positive: 4 (6%)
Negative: 65 (92%)
Middle Ground: 2 (2%)

(b)(1) 1.4a 43 (12%)
Sentiment Score: 16.27
Positive: 6 (14%)
Negative: 34 (79%)

(b)(1) 1.4a 255 (73%)
Sentiment Score: 7.46
Positive: 14 (6%)
Negative: 222 (87%)

SECRET

001

FOIA 14-0072

Figure 13: The front page of an analysis of RWIP obtained through FOI from CENTCOM, showing key details gathered under the programme. Details in the boxes are redactions, with the relevant reason for withheld information being a clause referring to classified information concerning "military plans, weapons systems, or operations".

The online CV of a CENTCOM civilian employee describes how she worked for SOCOM Central Command "in support of the Regional Web Interaction Program" at Interactive Internet Activity – Joint Psychological Operations Task Force based in Doha in 2009-10. She also had previous experience as a "middle eastern cultural advisor" working for CENTCOM, translating articles into Arabic for public affairs, monitoring Arabic media, and establishing the Arabic version of the CENTCOM Facebook page (Abdulhade, 2014). The only other employee working on the RWIP who identified themselves as such online worked for a company called Concepts and Strategies, Inc (ConStrat) (who also worked on the TRWI, see page 102), she worked at MacDill Air Force Base in 2011-12 in support of RWIP, where she "tracked and analysed regional blog sites", mapped the influence of "key communicators (media outlets, journalists, academics, terrorists, government officials,

NGO leaders, etc.)", tracked "penetration and resonance of quotes and statements to measure viral effectiveness", and used understanding of "the regional media environment and different technologies to engage in weblogs" (Warnso, 2014).

A number of other individuals have identified themselves as working for ConStrat for CENTCOM between 2011 and 2012[86], from these online CV's we can see that ConStrat's activities included the tracking and analysis of Russian, Urdu, and Arabic-language social media, the production of Arabic texts for SOCOM Central Command (see Drame, 2014), and general foreign media analysis (Kogan, 2014; Jones, 2014). ConStrat' contract was awarded for general support contract to the Information Operations division of CENTCOM (See FBO-CENTCOM, 2008, ConStrat, 2010) and supported a number of CENTCOM online engagement practices including RWIP, general online public affairs translation, and the Digital Engagement Teams discussed below. Thus we can see that both these RWIP contractors have links to more generic online monitoring and engagement, including pubic affairs, suggesting a continuity between open attributable programs and classified un-attributed ones which empowers CENTCOM to work across the spectrum of attribution in countering 'violent extremist ideology' in online conversation.

From these official statements, FOIA material and contractor-derived information we can deduce that the RWIP has the following features: it uses social media, blogs, and forums to challenge or counter what CENTCOM describes as "violent extremist ideology"; it judges initial success on measurements such as changing "the tone of discussion threads" and "shifting sentiment" in web forums; it likely includes un-attributable engagement through social media platforms in Arabic and Urdu (and perhaps Russian); it draws on the work of analysts who identify key communicators in specific areas, as well as the "viral effectiveness" of messages. It has been operated by a relatively small Arabic and Urdu-speaking staff based in Tampa and Doha who drew on a media-analysis support staff (shared with other more transparent public affairs element) providing intelligence on key communicators and forms of communication in the target information environment. It is reasonable to surmise then, that it is a Web 2.0-based influence program in which CENTCOM employees, masking their true affiliation, engage in debates with foreign publics around areas of US military interest, backed up by a group of language and communication analysts - representing a distinct and advanced form of CY-OPS not seen elsewhere.

The second programme Petraeus mentioned in 2010 is the Credible Voice Program – which uses "web-based operations to link disparate credible networks and organizations to counter our adversaries' message of violence" and aims to "amplify moderate messages within the contested information space to reduce extremists effectiveness in soliciting recruits and gaining financial support" (Petraeus, 2010:829). This programme runs in tandem with the RWIP, and aims at boosting friendly voices to join the military-produced messages of its sister program – Petraeus identified it as requiring $38.5 million to run in 2011[87]. Even less information about this program is in the public domain, though one job

[86] CONSTRAT also had an earlier contract to run Digital Engagement Teams – an attributable CENTCOM social media engagement – see below.

[87] Given that the entire CENTCOM budget for VOICE operations and "other Public-Diplomacy-Like Military Activities" was only $31.4m in 2010/£25.5m in 2011, this funding likely came through "Iraq and Afghanistan" funding (Rumbaugh and Leatherman, 2012:20).

advertisement from the Abraxas Corporation from 2011 seeks open source intelligence analysts to work with CENTCOM, with tasks including developing "open source biographical products supporting the Credible Voices Program to make CREDIBLE VOICES product updates" (Abraxas, 2011).

Though this is all the information in the public domain about the Credible Voice Program – the involvement of Abraxas links to the only other publically-known element of CENTCOM's clandestine online communication programs. A relatively new company called Ntrepid, spun off from and set-up by founding members and executives of Abraxas (see Sec.gov, 2010; Current Events Inquiry, 2011), is the contractor who runs the most publically controversial element of CENTCOM's PSYOPS operations. Originally reported as "Operation Earnest Voice" (e.g. Fielding and Cobain, 2011), a controversy developed in 2011 around a contract advertised by CENTCOM soliciting for a company to provide "Persona Management Software" – which would allow military users to mask their identities and assume realistic and verifiable online personas (known as *sock puppets*) to engage in clandestine online communication.

Figure 14. Persona Management Software contract from Federal Business Opportunities

Unlike the TRWI, the sock puppet program was highly secretive, and was only uncovered when hackers from the online-activist group Anonymous broke into the system of a would-be bidder on the DOD contract and discovered the tendering documents and

associated discussions (Webster, 2011a; Rockefeller, 2011)[89]. The contract (see figure 14) solicits for bespoke software that would allow one user to control 10 online 'personas' from a single computer, with 50 user licences, and thus 500 total 'sock puppets'. According to the contract, the personas will be "replete with background, history, supporting details, and cyber presences that are technically, culturally and geographically consistent" (FBO-CENTCOM, 2010) – thus sophisticated enough to withstand background checks from suspicious users. The personas "must be able to appear to originate in nearly any part of the world and can interact through conventional services and social media platforms" (FBO-CENTCOM, 2010), allowing a broad choice of guises for operators to use to engage in online debate.

The required tool is one which allows the creation and management of authentic-seeming fake people, while providing the operator with sufficient intelligence to be able to manage these accounts, and interact like a 'real' person in a non-superficial way. The contract is based at MacDill Air Force Base in Tampa, as well as Kabul and Baghdad. It was awarded to Ntrepid (Webster, 2011b), which advertises itself variously as a privacy and identity protection firm and national security contractor, who were paid $2,760,000 to carry out the contract (Webster, 2011b). Though it was never reported which element of EARNEST VOICE operations this contract was to be used to assist, Commander Bill Speaks, chief media officer of CENTCOM's digital engagement team said it would support "classified social media activities outside the U.S., intended to counter violent extremist ideology and enemy propaganda" (quoted in Webster, 2011b).

Speaks' description of the aims of the programme fit with those of the Regional Web Interaction Program and Credible Voices programme developed above. The described technology also seems designed to work with what we know of the operation of the RWIP – it would aid a small group of users engaging in a number of different forums, the users would be speakers of foreign languages (there is no translation requirement in the contract), and directly addresses the problem of "shifting sentiment" and altering the "tone of discussion threads". CENTCOM would not comment on whether the Ntrepid contract is linked to the RWIP and Credible Voice programs – though on this evidence it would be surprising (indeed, organisationally negligent) if it was not – especially given the integration of the intelligence and media-monitoring facets of CY-OPS activity across various programmes. At the very least, we can say that these capabilities and aims are coalescing under the same operational imperatives and organisational structures, and thus represent a key area of clandestine CY-OPS – enriching our understanding of the breadth of possibility of potential military activity.

5.5.2. Digital Engagement Team – "winning relationships, not arguments"

While there is little information about the above programmes in the public domain, another CENTCOM online communication program about which the Command has spoken publicly, the Digital Engagement Team (DET), can be understood through its identifiable public activity. This is a fully-attributable group of public affairs personnel who engage on

[89] The contract had actually been on Federal business Opportunities since June 2010, but had not received any media attention until this point (see FBO-CENTCOM, 2010), demonstrating the "archive of unpredictability" of online dirty data for military organisations.

web forums, in the comment sections of news websites, and on social media to directly address discussion of US foreign policy. The team was established in 2008 and is said to include between 10 and 20 speakers of Arabic, Dari, Farsi, Pashto, Urdu and Russian (Biggs and Feve, 2013:15; Shanker and Schmitt, 2011) – and it operates as a social media branch of traditional public affairs, with particular Web 2.0 features which enhance our understanding of CY-OPS practice and theory.

When the DET started it was reported in a CENTCOM press release as "Twittering and Facebooking in order to better reach the people around the world and get the word out about operations", it also included a YouTube and Flickr account (Nelson, 2009). In describing the rationale, its first head, Bill Speaks describes the fact that "the internet is increasingly becoming a primary source of news and information" and "a shift" to Web 2.0 as a key driver behind the rise of the DET (Nelson, 2009), although at this time most of the activities were simply a Web 2.0 version of traditional PA practice: providing information about US deployments and military news to US audiences via press releases on Facebook, posting press photos on Flickr, etc..

By 2011, however, the New York Times was reporting that the DET was the body through which the "U.S. Military Goes Online to Rebut Extremists' Messages" (Shanker and Schmitt, 2011) – signalling a shift from U.S. audiences to those in the CENTCOM area, and a move beyond fairly mundane maintenance of CENTCOM social media profiles to an approach based on communicating on non-US websites and forums. Shanker and Schmitt reported on one Farsi-speaking Team member "patrolling two dozen Persian-language Web sites, hunting militant adversaries in cyberspace", tasked with scanning "news reports, blogs, social media and online essays" to identify those he viewed as "containing lies, misinformation or just misperceptions" about American military operations or policy (Shanker and Schmitt, 2011). However, this differs markedly from the covert programmes discussed above in that all posted responses are required to "carry an official stamp acknowledging sponsorship by Central Command" (Shanker and Schmitt, 2011). The examples of content given are rather formulaic and dry – one analyst responds to a Farsi thread with "theories of Great Game conspiracies pitting spy vs. spy" in Pakistani-US relations with "a response drawn from Pentagon and State Department policy statements" describing "shared American and Pakistani security interests" (Shanker and Schmitt, 2011). It was also noted that the team also does not work "at network speeds because translation and approval takes hours" (Shanker and Schmitt, 2011). In this reading, a side effect of US policy seems to be the threat of a CENTCOM contractor popping up on a forum or news website and (slowly) boring you to death by regurgitating dry policy discourse.

However, the process of engagement seems to have accelerated and got smarter since these reports. By 2013 the DOD's own internal media was reporting that the DET was engaging on "some 120 social media sites" connecting with "more than 100,000 people from the Middle East and Central Asia every week, occasionally hitting the half-million mark with a particularly compelling posting" (Miles, 2013)[90]. Miles also details a shift in focus around this time, from engaging on "intellectual and academic sites" with rebuttals

[90] The DET maintains CENTCOM Facebook pages in Urdu (with 787 likes) and English (with 51,760 likes), the later of which shows a maintained focus on traditional US-targeted public affairs; as well as CENTCOM YouTube pages in English (with US-audience focussed public affairs material), Dari and Urdu (both with very few views). The DET Flickr page is also active (Flickr – CCDET, 2014), featuring mostly internal publicity (photos of military graduations, CENTCOM social events, etc.).

and arguments challenging "mistakes or flagrant misinformation", to a broader and less confrontational discourse which is more about engagement than rebuttal – a CENTCOM public affairs officer describes the approach: "we are not trying to win arguments. We are trying to win relationships" in order to "improve our access to the theatre" (Miles, 2013). He says, further, that "this is not about trying to establish U.S. culture [...] this is about establishing credibility and making a connection [...] which help to give Centcom a credible voice with an audience it might not otherwise have", meaning that "when [they] have something the command needs to communicate, [they] can do that across a large audience in seven different languages (Miles, 2013)[91]. This approach is recognisable as sharing a strategy – of "winning relationships", "establishing credibility" in the long term for the times when that connection is needed, and emphasising engagement as an end in itself - with the social media element of the Trans Regional Web Initiative. Indeed, 'winning relationships, not arguments' serves as a good shorthand for this new form of long-term and subtle pursuit of influence online through "information engagement".

Figure 15: Thread started by US CENTCOM on PakDef.org – featuring video showing relations between military and Muslims around US CENTCOM and SOCOM base in Tampa

[91] One analyst, who worked as a contractor for the DET (see Yousufzai, 2014) went public about his role after being denied security clearance on what he says were discriminatory grounds in 2012. He was working on the CENTCOM base in Tampa (De Benedetti, 2012) in 2009-10 as part of a team which "wrote essays and posted pro-US comments on foreign-language blogs and social media websites. They wrote in English and Urdu […] promoting the military's positive efforts and countering anti-American opinions" – "the analysts used pen names that cloaked individual identities while openly identifying themselves as American government employees" (De Benedetti, 2012). This statement, coming from someone who has a grievance with the programme, offers good triangulation to military statements on the project.

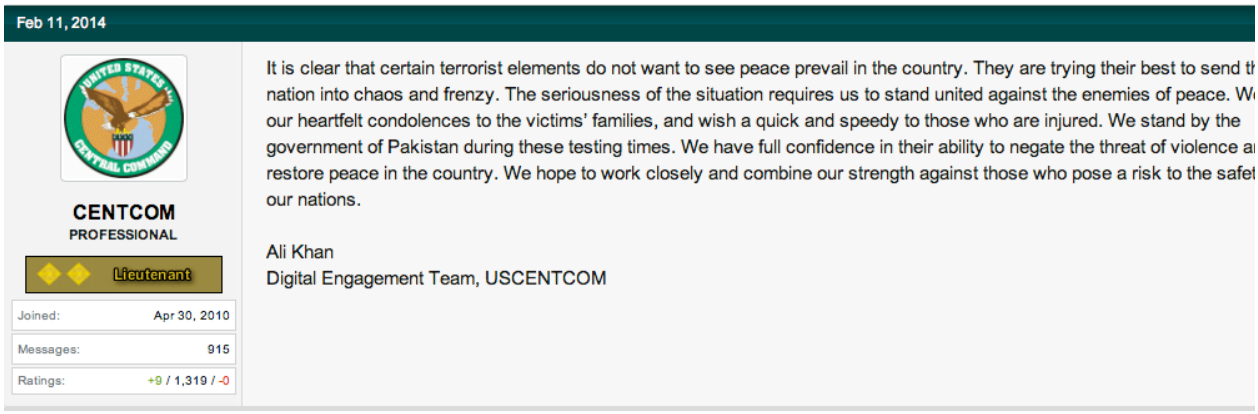


Figure 16: CENTCOM reply to post on Defence.Pak

A substantial amount of Digital Engagement Team material can be located online. For example the username "US CENTCOM" is active on a number of English-language Pakistani forums such as *Pakistan Defence* (Defence.pk), *Pakistan Affairs* (PakistanAfairs.pk), and *Gupshup* (Paklinks.pk). Posts on these forums (see e.g. figure 16) are fully-attributed to CENTCOM and vary from updated versions of traditional public affairs products such as online press releases and YouTube videos (in English with Urdu subtitles, e.g. figure 15) featuring soldiers offering Eid greetings (e.g. Gupshup – CENTCOM, 2012) or answering questions posed by users (e.g. Pakistan Affairs – US CENTCOM, 2012); to more *ad hoc* posts such as the sending of condolences when other users report on terrorist attacks (e.g. Pakistan Defence – CENTCOM, 2014) or expressing support for Pakistani security forces attacks on militants (e.g. Pakistan Defence – CENTCOM, 2012).

In these posts, we can see a different approach taken within CENTCOM than that found in the similar program run under the State Department's *Centre for Strategic Counterterrorism Communication* (CSCC), which also has a Digital Outreach Team. As has been well-reported (see McCants, 2013; Clayto, 2012, Axe, 2012) the CSCC also operates in a transparent way in the same languages as the DET (with the addition of Somali), but rather than "winning relationships" seeks to use forum posts and social media platforms to directly challenge supporters or promoters of violent extremist groups online through an approach which seeks to "contest the space, redirect the conversation, and confound the adversary" (Fernandez, 2012:5, see also US Advisory Commission on Public Diplomacy, 2011:16; LeBaron, 2012; CSCC, 2013). The example of CSCC provides an interesting counter-point – of an alternative approaches to using transparent engagement in social media with more adversarial messaging, emphasising that the DET approach based on "winning relationships" is a choice based on the belief that it is a more effective approach to achieving military objectives, and one which better compliments other CY-OPS activities.

5.5.3. Summing Up CENTCOM

As the largest and most active geographic command, CENTCOM cannot be understood as typical of broader military practice; but as at its cutting-edge. It is the part of the DOD bureaucracy, along with SOCOM, where the context of Digital Age conflict has presented the strongest challenges and opportunities. While available information is partial – it is clear that CENTCOM is running both a transparent social media engagement campaign

under the Digital Engagement Team, and an unattributed one under the Regional Web Interaction and Credible Voices programmes. The former is carried out by Public Affairs staff and is transparent and often aimed at US audiences, while the later is carried out by PSYOPS practitioners and aimed at audiences in the CENTCOM area, likely exclusively in languages native to that area.

The programmes share a number of common features. Both work through employing native language speakers to engage on social media, web forums, and news website comment sections to engage in discourse in support of US military interests. Both programs are also supported by linguistic and media 'target audience' analysts, with the evidence suggesting that the same analysts support both missions. While the DET's engagement are transparent and accessible to research, those of the unattributed programs – very likely supported by "persona management" software – are not. However, we can reason that many of the limits usually placed on US military communicators for pragmatic reasons - the necessity for truthfulness, civility, consistency – do not constrain RWIP and Credible Voices, as the possibility of being 'outed' and damaging broader US credibility is slim (indeed, it is what the technology is designed to protect against).

Thus, we can see that CENTCOM has the capability to engage across the spectrum of attribution – through official spokespeople on traditional media, official social media profiles, unofficial but attributed presence on regional forums and social media sites through the DET, and in a clandestine way across social media platforms and web forums. This allows CENTCOM communication staff not only to influence information flows in the traditional way through statements from war zones, but to engage at a more granular level – using their accumulated authority and legitimacy on certain platforms when it is deemed useful, and disguising spokespeople as normal Web users when it is not. Thus we can see within CENTCOM the potential increased *range* of developing CY-OPS practice, which – when we also take into account the TRWI platforms and traditional media relations role – can shape the Web 2.0 information environment from the level of the spokesperson, through the news reporter, and right down to the news website commenter or web forum debater. This demonstrates a potentially pervasive and highly effective form of information engagement – which compels us to expand the scope of the communicative spaces relevant (from the mainstream media, right through to social media debate) in the analysis of contemporary military influence operations.

5.6. Assessing A Digital Age Propaganda Apparatus

Taken together, the SOCOM and CENTCOM programmes outlined constitute part of a propaganda apparatus which acts in a comprehensive way in the Web 2.0 information environment through a variety of approaches, and seeks to optimise the potential of new platforms to coherently produce a complex form of communication power. The programmes address the *space* of Web 2.0 in a range of ways. The TRWI website network creates online news spaces where military communicators have complete control over content. However this only a superficial understanding of their operation (in which we could simply discount those with poor readership as failed PSYOPS tools). Much more important is the manner in which the websites become – through both concerted

promotion and the nature of Web 2.0 news flows – embedded in the weft and weave of the online news environment. This has the mutually-reinforcing effect of increasing the reach of TRWI content, and of boosting the legitimacy of the websites themselves by masking their SOCOM-authorship and allowing them to piggy-back on the credibility of those in the network who share or replicate their content.

Furthermore, the importance of the TRWI sites as an element in building up an audience for PSYOPS products has been demonstrated in the case of the *Southeast European Times,* where much of the content becomes secondary, simply acting as a 'hook' to draw in and maintain an audience with whom PSYOPS practitioners can nurture trust and credibility – the holy grail of military communicators. This is the idea behind the "winning friends, not arguments" approach taken by CENTCOM DET to transparently engagement with online forum users or commenters. Thus we can understand PSYOPS *construction* of particular online web spaces as only one element of an apparatus which is much more interested in the *insinuation* of PSYOPS messages, influence, and credible communicators within existing online spaces. That these spaces include Facebook pages, web forums, news comment threads, and Twitter accounts shows that in parallel with an approach to the Global War on Terror which blurs the lines between the military, political and the social, there is a move of military communicators into previously non-military communication spaces.

As well as the expansion of platforms, I have described the *range* of CY-OPS communication which affects our understanding of how the apparatus influences the online information space. The guises in which PSYOPS comes are now many: the traditional statements of spokespeople or engagement with the mainstream media; the quasi-transparency of the TRWI websites; the informal yet still attributable engagement of military communicators through the DET and Facebook pages associated with TRWI websites; and the clandestine and underhand engagement on web forums or social media using persona management tools. This leads to the development of an understanding of the space of military communication beyond that of the media or battlefield-specific PSYOPS such as radio or TV stations. The world of social media, often seen as that of first-hand accounts of conflict and secondary debate about "the media" itself, must be understood instead as a deeply integrated and contested space which CY-OPS practices increasingly address in a concerted and coherent way. These social spaces of Web 2.0 are understood from a CY-OPS perspective as simply another part of the information environment in which influence can be pursued.

In the theory section I outlined *population* as another important concept for understanding the implications of particular regimes of power. In this case we can see that one way in which CY-OPS works is through the understanding of its subjects not simply as an *audience,* but (and here the case of the *SE Times* Facebook page is again exemplary) as a force multiplier, an army of conduits to spread and give credibility to military messages, a population which must be gathered within a sphere of influence, kept on side (through building of credibility and trust) and primed for situations in which it can be more directly instrumentalised. When important strategic aims must be achieved this population then *becomes* an audience in the traditional sense, but is also used to spread messages in a form of viral CY-OPS. Here it is helpful to understand particular PSYOPS audiences not simply as

the subjects of particular messages, but as a *medium* through which reach or influence can be achieved in the online information environment.

It is also evident that being understood in line with particular military imperatives – that is, as the *population* to which a particular strategy or policy refers – can have potentially significant consequences for individuals who make up that population. While the majority of the subjects of CY-OPS campaigns are anonymous and addressed simply as a mass whose opinions are unknown but contested, there are a few distinct populations – addressed through SOCOM MIS team programmes – who have been identified as key "counter violent extremism" (CVE) populations and thus require special attention. I have identified cases in which MISTs have instituted regional CY-OPS programs in line with particular counter-terrorism objectives. The case of the MIS sponsorship of youth groups in the anonymised example is illustrative, with the context of developing unconventional warfare practice providing a example of the potential scope of such an approach. In this case, the niceties of declaring military sponsorship prominently on websites or the profiles of those working in CY-OPS programmes are done away with, instead local community organisers are co-opted to act (potentially unwittingly) as conduits for US special operations, and an unknown nuber of young Web users are engaging in a forum run for SOCOM as part of a concerted influence operation. Having been identified as part of the population requiring CVE-intervention, Web users and project partners are deceived, made unwitting accomplices in US military power, and are potentially endangered through becoming implicated in a program run by the same organisation which is a key player in a brutal and complicated war in the region. In such a situation, the burden of the risk of discovery – often highlighted as the reason to avoid deception in traditional PSYOPS – falls almost entirely on the unwitting participants on the ground, whose political and social lives are militarised without their consent.

Finally, there is the issue of *knowledge* in examining apparatuses of power. Throughout the chapter I have identified emerging intelligence practices tied to the development of CY-OPS. We see the rise of a much more nuanced form of 'target audience analysis' in TRWI websites which engage with and poll audiences (and of course have access to back-end traffic analytics). A much more direct form of this analysis can be seen in practices which guide the engagement of DOD commenters in online forums and social media – requiring the identification of key sites of interest, knowledge about the appropriate structures and subjects of conversation, and constant monitoring to track changes in sentiment in larger campaigns of surreptitious influence. In developments in UW training and research, we can see further links in which the deep study of protest and dissident movements becomes a key factor in guiding potential future engagement strategies in the post-Arab Spring strategic environment. This is a key aspect of "information engagement" – one in which the proliferation of information online provides not just a challenge to military communicators, but an opportunity to monitor and refine communication practices.

Towards the end of the research period another development highlighted the deep links between intelligence and communication in this developing propaganda apparatus. SOCOM has its own research and development capability (see Olson, 2008:14; SORDAC, 2014), and in early 2014 it announced interested in acquiring a number of new

capabilities, all related to social media intelligence[92]. The Command requested capabilities in "social media research and analysis, … customised social media website development and execution, … detailed social media data-mining, social media monitoring and analysis, target audience analysis … and social media platform operations" to support activities against "extremist influences" in Europe emanating from other conflict zones (FBO – *USEUCOM,* 2014). It sought information on a "psychometric approach to deception detection in social networks", seeking documentation, information and/or software "pertaining to sociological, psychological and cultural knowledge of deception in social media" (FBO-SPAWAR, 2014). Finally, directly relating social media to intelligence, the Command sought the development of tools in "Social Media Intelligence Analysis" to aid "finding, selecting, acquiring, and potentially translating information" from social media "and analysing collected information to produce actionable tactical intelligence in support of [Army Special Operations] mission sets" – including "influence activities" (SOCOM – *TE 14-2,* 2014:37). While these announcements came too late in the research period to yield any substantive examples (they were still in the preliminary contracting stage at the time of publication), they demonstrate a growing interest in Web 2.0 within special operations practice, and represent the key link between intelligence, research & development, and the developing propaganda apparatus of the DOD. A deep investigation of these links forms the basis of the following chapter.

[92] Demonstrating the link between knowledge and power at both the material level (the ability to run an R&D system), and the more practical level of intelligence as the most direct example of the "knowledge is power" maxim.

6. US Military Research & Development and Digital Age Conflict

This chapter moves on from active military units to explore a less direct but equally active area of military evolution, that of research & development (R&D). The vast sums of money invested in R&D and the influence it gives the DOD outwith official military structures make it an important area of analysis in studying the process and impact of any form of military adaptation. This importance is heightened when use of advanced ICTs are our primary concern. R&D also forms a key part of the propaganda apparatus in directly addressing the area of *knowledge* in supporting and producing military communication power in the new information environment.

In the case of Digital Age conflict the area of R&D is particularly important as there are a number of programmes which directly address the new information environment and the technological and strategic challenges which make up the problem field. This chapter explores significant developments in the fields of intelligence and PSYOPS, including: new forms of operational intelligence based on Social Network Analysis; strategic intelligence based on mining social media data; and a range of "information engagement" practices, from large projects to understand memes in social media flows to new CY-OPS tools. This R&D is situated in a context of the emerging strategic paradigms of "Phase 0" operations and the "indirect approach" of the GWOT, link to emerging intelligence practices discussed in section 4.4, and in many cases is directly linked to areas of special operations discussed in the previous chapters.

6.1. Research & Development in the DOD: A Key Source of Data on Institutional Change

Military R&D is an important area of interest for this thesis, both as key site of military adaptation, and as a point of access to data and insight into broader military thought and practice. The R&D projects studied in this chapter account for at least $170m in DOD spending since 2008[93], and the influence of this research budget is important in driving military, academic and commercial research, much of which is in the public domain and thus offers access. R&D is driven by institutional need and must constantly be justified to policymakers and broader audiences as relevant and value for money, meaning it must be responsive to changes in organisational thought and practice. Consequently there is a wealth of documentary material which provide vital context for adaptation to new technological or strategic environments, as understood by military planners, where DOD strategists and project managers must put their mouth where their money is - highlighting and justifying work in areas which have received substantial funding and institutional engagement. This allows further insight into the military construction of the problem field of Digital Age conflict, as well as access to a key area of military activity where parts of the propaganda apparatus - knowledge, techniques, and tools – are developed.

[93] This is the combined budgets of the HSCB and SMISC programmes, the only ones which are available as distinct budget items, the true figure is significantly higher once other programmes are taken into account.

The examination of developments in military thought and practice in the previous chapters has aided the identification of the key areas where Web 2.0 and contemporary military practice interact: in concern with irregular and asymmetric conflicts "amongst the people", in understanding the contemporary information environment, and engaging in it for the purposes of both intelligence and psychological operations. An examination of the DOD bodies and programmes which work in these areas identified a number of key sites where the issues of military involvement in Web 2.0 is the subject of significant R&D – this chapter identifies and focuses on two broad research initiatives called the Strategic Multi-Layer Assessment (SMA) Program and the Human Social Cultural Behavior Modeling (HSCB) Program; as well as more distinct research projects called Social Media in Strategic Communication (SMISC) programme at DARPA[94], and the CORE Lab at the Naval Postgraduate School.

These areas of interest were identified based on a search of all relevant DOD budgetary documents for keywords identified based on research for the previous chapters as likely to signal an area of interest[95]. For the major programmes of interest the research was able to draw from a relatively structured body of material. The research was conducted after a 5 year report into the HSCB program was published (MITRE, 2013) which discussed its context as well as listing over 500 publications which had resulted from its funding. Similarly, for DARPA's SMISC programme the research benefited from the organisation's new "Open Catalogue" initiative under which extensive lists of all papers produced under certain projects are released (see DARPA – *SMISC List*, 2014). Demonstrating the importance of elite engagement, the SMA program is not promoted publically and does not publish documents on its website, however it is not classified and upon requesting information I was placed on the programme's email list and was able to download all papers produced under it, as well as conference proceedings and other additional material. This level of access to data allowed understanding of all major programmes to be developed based in their own comprehensive documentation. The analysis also drew on all open source data available in order to cross-reference and add to that produced within the programmes themselves.

Taken together – this material provides a wealth of largely unreported[96] and unexamined material documenting the institutional impetus, process, and practical outcomes of a deep engagement with the contemporary social and technological environment in which the military seeks to operate, including significant Web 2.0 developments. In recognising that

[94] DARPA is the Defense Advanced Research Projects Agency, the DOD's premier R&D agency which has historically played a crucial role in the development of robotics, the Internet, and a number of more directly combat-related technologies (see Belfiore, 2010)

[95] Searches were run on all "Research, Development, Test and Evaluation" budgetary documents for DARPA, the Office of the Secretary of Defense, the Joint Staff, and the U.S. Special Operations Command, from FY2012 until FY2015. This identified major programs and areas of interest. Further searches were carried out using the same keywords on the Federal Business Opportunities website which carries all public military procurement contracts, and on SBIRSource.com which publishes all information on DOD small business-specific contracts. These searches allowed for the collection of details on smaller projects of interest which may not have been identifiable in official budgetary material. Keywords used for these searches were: *"social media", "MISO", "PSYOP", "psychological", "behavioral", "cognitive", "social", "information operations", "interactive", "internet", "influence", "cyber", "web", "voice", and "virtual"*.

[96] The first reporting in the mainstream media or online of the SMISC research, for example, was a 2014 article in The Guardian based on some of the research for this chapter (see Quinn and Ball, 2014).

such material provides insight into both developing military *thought and concepts* as well as *practice,* this chapter presents comprehensive discussion of the rationale and approach of the projects of interests, as well as their outcomes in terms of active R&D projects (methodologically, exploring both the *problem field* and *apparatus*).

This chapter begins by exploring the institutional basis for military engagement in Web 2.0-focussed R&D, discussing the theoretical and conceptual background to the programmes, exploring how they outline the problem field of Digital Age conflict from an R&D perspective. The section which follows demonstrates the impact of these programmes outside of the DOD itself, identifying links to developing forms of knowledge and academic disciplines as an important outcome. The chapter then examines in detail the range of practical outcomes – firstly in the area of intelligence, and then in that of military communication. There is significant activity in both areas, exhibiting a range of new intelligence activity, enhancing our understanding of information engagement and CY-OPS, and allowing us to situate these R&D programmes within the context of a Digital Age propaganda apparatus.

6.2. Institutional Context: R&D as Focal Point for Coherent Change

Rather than providing a comprehensive analysis of the entire US defence and intelligence R&D apparatus[97], the analysis in this chapter focuses on detailed investigation of selected programmes with a level of transparency and open source documentation that allows the development of an *in-depth* and *contextualised* understanding of developments. The focus on a number of relatively large and transparent research programmes (in which there is a lot of overlap in personnel, projects, and subject matter) facilitates the study of military R&D as a reasonably coherent body of though and work: providing data not just on the outcomes of research projects, but also on the institutional driving forces behind these projects, key actors involved, and relationships with other programmes and intellectual currents. Thus, while there are almost certainly research projects of interest to the research which are omitted due to being classified or simply too obscure to show up in public documents, the focus on a smaller number of large programs provides an empirical basis for understanding the context and direction of travel of DOD research in relation to Digital Age conflict. This chapter presents data tying together developments in special operations intelligence practice with cutting edge Web 2.0 analysis, linking academic developments in Social Network Analysis to a number of tools used by soldiers in Iraq and Afghanistan. It also allows discussion of diffuse projects at the cutting edge of Web 2.0 communication research cohering under emerging paradigms in intelligence (developing a "social radar") and communication (what I identified as "information engagement"). Ultimately, this approach which necessarily focuses on a *deep* analysis of specific programmes (as comprehensive *breadth* is difficult to achieve and even harder to verify),

[97] This apparatus is extensive, complex, and often inaccessible to research due to classification or obscurity. For example the revelations in the leaks by NSA whistle-blower Edward Snowden exposed a massive hidden system of online intelligence gathering previously unknown to the public (see Greenwald, 2014). As these leaks are curated by a select group of journalists and thus inaccessible to further research they provide context only for this chapter.

provides enduring insight into emerging paradigms, practices, and technologies across the area of interest.

In developing this coherent understanding the most important example is the DOD's HSCB Program. This is a 5-year programme funded by the Office of the Secretary of Defense (OSD) between 2008 and 2013, which administered over $120 million worth of academic and commercial contracts for R&D in the broad area of the collection, analysis, and exploitation of sociocultural data for military operations [98]. The programme is administered by the MITRE Corporation (a Government-funded not-for-profit corporation), and has links to other military research institutions such as the Office of Naval Research and the Air Force Research Laboratory which, along with other Federal contracting initiatives, it distributes contracts through. The programme is more than just a funding vehicle however. It features a regular newsletter discussing R&D strategy and showcasing various projects (see, HSCB Newsletter List, 2014); a strong identity and coherent presence in the area of defence and intelligence research (e.g. see logo in Figure 17); regular conferences bringing together contractors, military officials and researchers; and produces key documents acting as milestones to showcase, analyse, and guide the progress of the project (see National Research Council, 2008; DSB, 2009; Schmorrow, 2011b; MITRE, 2013).

Figure 17: Human Social Cultural Behavior Modeling Logo

Budgetary documents for the programme describe it as "a vertically integrated effort to research, develop, and transition technologies, tools, and systems" to military users "to

[98] This figure is the total of annual expenditure listed in Office of the Secretary of Defense budgetary justification documents – taking the most up to date figure for each year since FY2008, MITRE put the total expenditure slightly lower, at $118m (MITRE, 2013:1). The program was only initially outlined to run between 2008 and 2013 (see HSCB Newsletter, No15:1) due to its genesis in DOD *Strategic Planning Guidance* for this timeframe, however the ethos of the program continues under the "social radar" paradigm (see section 6.4.3), and at the time of writing the Senate Committee looking at its budget for FY2014 was arguing for a continued $15m annual allocation for the programme (Senate Report 113-044, 2014).

optimize U.S. forces' ability to perform population-centric sensing, understand behaviors driven by social and cultural variables", driven by the need for "understanding the increasingly complex global environment to address national strategic challenges such as instability, aggression, proliferation of weapons of mass destruction, and violent extremism" (OSC RTD&E FY2015, 2014:77). The programme funds projects spanning everything from concept development or theory testing to the development of computer programs or tools – which attempt to collect military-relevant data about the social world (demographics, opinions, social networks, cultural factors), process the data in some way (translate, quantify, standardise), and apply it to various forms of military thinking (operational research, modelling situations or populations for testing courses of action, training), or military practice (to assist cultural sensitivity, intelligence collection and analysis, targeting, or PSYOPS)[99]. In short, it is a well-funded attempt to harness and develop a multi-disciplinary knowledge base for the advancement of military understanding and practices concerned with the human element of conflict. Within the programme there are a number of projects addressing the online information environment, many of which are discussed prominently in the programme literature, making them a key subset of research and a significant area of interest for this thesis.

The analysis focuses on examples of the collection or use of sociocultural data which engages directly with data from the Web 2.0 environment – such as that which attempts to automate the analysis of blog or Twitter content for intelligence purposes (Carley et al, 2013); aid PSYOPS personnel in crafting social media messages (Bernardi, 2012); or understand flows of online information such as memes or viral messages (McCormack and Slater, 2010). In the area of statistical approaches to understand sociocultural data, we are also interested in the proliferation of studies based on social network analysis (SNA) to visualise and analyse small and large social groups – an area which is also important in projects under the SMISC programme and the Navy's CORE Lab. In a number of projects in these areas Web 2.0 data is found to be increasingly important. This is not surprising, as Web 2.0 is both an increasingly important part of the social world, as well as an excellent source of data required to understand it. As this chapter demonstrates, new ICTs are providing both the capability to enhance existing military practices and driving the development of new activities exploiting the novel possibilities of information and communication online.

Social Media in Strategic Communication (SMISC) focuses more directly on ICTs, taking as its focus the development of tools to enhance the US military's ability to understand and engage in the Web 2.0 communication environment. It began in 2011, with an announcement (FBO-DARPA, 2011) looking for contractors to conduct primary research into trends and memes on social media and the identification of "persuasion campaign structures and influence operations" online (Rawnsley, 2011). The stated impetus for the programme is the belief that the spread of social media technologies are likely to result in

[99] The "modeling" in the title refers to an interest at the heart of the program in computational, statistical and virtual modeling. This interest grew out of a National Research Council recommendation for military investment in this area (NRC, 2009), though the program moved beyond this particular focus to more general interest in formalising and working with social and cultural data. It did, however, support some work focusing specifically on modeling (e.g. Bronner and Richards, 2008; Geddes and Atkinson, 2009; Murray et al, 2011; Belov et al, 2010). Where this work addresses new technologies as a sociotechnical environment (rather than as, for example, a platform for modeling virtual soldier training exercises (e.g. Pollock et al, 2011)) it is included in the analysis in this chapter.

"profound" changes in the "nature of conflict" – and the need for developments in military communication practice to address Web 2.0 (DARPA, 2011:4). Like the HSCB Program, SMISC has funded a large amount of academic research, almost all of which has been published, providing a wealth of information about developing military practice (DARPA – *SMISC List,* 2014).

Elsewhere, this chapter draws on activity at Defense Analysis department at the Naval Postgraduate School – a military educational body headed by the netwar theorist John Arquilla - which houses the CORE Lab, an important site of the application of social network analysis tools to special operations activity with an increasing focus on Web 2.0. Finally, data comes from the Strategic Multilayer Assessment programme, a research body working to provide reports to senior military decision-makers (the Joint Staff and combatant commanders) which "provide planning support […] with complex operational imperatives requiring multi-agency, multi-disciplinary solutions", focussing on political, social, and cultural problems (Cabayan, 2012; Béen, 2013:9). The SMA programme focuses on particular areas of interest identified by military policymakers, those with a significant Web 2.0 component include "socio-cultural analysis" in reconnaissance, surveillance and intelligence (Ehlshlaeger, 2014); "influence and deterrence in a networked world" (Cabayan et al, 2014); the relevance of "behavioural & social science to DOD missions" (Canna, 2013); and "the effects of CyberNeurobiology and CyberPsychology on Political Extremism" (Orlina and Desjardins, 2012). At the end of the research period there was an SMA conference announced for late 2014 called "A New Information Paradigm? From Genes to 'Big Data' and Instragram to Persistent Surveillance ... Implications for National Security" (SMA - *2014 Conference Proposal*, 2014). As it acts as a think tank for senior planners and commanders in the DOD, the SMA programme offers key insight into the significant interest in Digital Age conflict at this level, as well as cutting-edge research guiding the development of military practice.

The programmes have a number of structural, personnel, and disciplinary links (demonstrated in the references throughout), and they are also united by a shared ideological and strategic context. This can be seen in the theoretical and strategic background provided in the material produced by the programmes. Key figures consistently outline the impetus as coming from the strategic imperatives of the growing importance of irregular warfare and special operations in US military planning and operations; the growing and continuing importance of information, communication, and public opinion in conflict; and the increasing emphasis on "Phase 0" or "shaping" operations. All of which are key elements of the Digital Age problem field.

Beginning in 2008, at a time when the counterinsurgency paradigm was on the rise on American military thought, the HSCB program is very much of its time. Its programme manager (Dylan Schmorrow) identifies the "shift from conventional to irregular warfare" as *the* reason the DOD "[saw] a need for [the HSCB] program" (Schmorrow, 2009a:5, see also Flynn, 2012:1-2). Figure 18 shows Schmorrow's outline of the perceived change in focus, he channels the contemporary military zeitgeist (later in the same presentation referencing both the COIN training manual and the "GWOT Slide", see page 68) in describing the contemporary operating environment as one in which "leading actors may well be small groups or even individuals, connected and perhaps driven primarily by cultural or social factors … these actors will be geographically distributed perhaps only

loosely affiliated with one another, embedded in general populations, and will use local networks, economies, and sympathetic governments for cover and support. They will also exhibit … an emphasis on influencing general popular sentiment through culturally anchored communication" (Schmorrow, 2011a:vii). It is in this context that the DOD seeks to develop sociocultural and behavioural knowledge[102] – if you are going to wage war "amongst the people", you need to understand who "the people" are and what they want.

Figure 18: HSCB Slide showing changing emphasis of Irregular Warfare – all key factors in the perceived importance of sociocultural factors in contemporary conflict (Schmorrow, 2011b)

Platitudes paid to understanding "the people" proliferate in military discourse, often without much substantive change proceeding. However, Schmorrow stresses the value of HSCB research in an irregular warfare situation, describing "mastery" of HSCB factors as enabling a situation in which "U.S. forces would have the data on indigenous populations and the training they need to move easily in those populations", they would have access to cultural and social intelligence and "integrate those with conventional mapping of the physical terrain", as well as being able to "detect often complex and dynamic networks, where adversaries and civilian populations are intermingled" and "possess non-kinetic and well as the ability to anticipate both the near-term and long-term impacts of applying those tools" (Schmorrow, 2011a:vii). The key outcomes linked to Digital Age conflict are found here: changes in intelligence practice which emphasise social and cultural intelligence; the detection of "complex and dynamic networks" and focus on differentiating enemies within civilian populations; and changes in military communication practice in which this intelligence is used to produce dynamic

[102] As well as to *institutionalise* advancements it had made in the area since the beginning of the GWOT – a Defense Science Board Task Force report on *Understanding Human Dynamics* laments that the US military is constantly relearning the lessons of counterinsurgency after neglecting the lessons of the Philippine and Vietnam wars (DSB, 2009:4,vii)

communication strategies which are presented as "non-kinetic" weapons applied in a controlled way. The HSCB programme came at a time when these fundamentally *social* problems plagued US efforts in Iraq and Afghanistan, and addressed them in a *technical way,* as the influence of Web 2.0 grew in importance since 2008 this technical approach situated the programme well to address the new information environment.

Although Web 2.0 is not always mentioned specifically in discussions of new population-centric paradigms, the role of Web 2.0 becomes key as populations start to move online, as is demonstrated in a number of the research projects featured in this chapter. As "the people" adopt Web 2.0 tools as a key part of their lives, the data they produce becomes the most accessible way to collect the information on which new intelligence and communication strategies are based. This was show in relation to Flynn's conception of "Phase 0" intelligence[103], guided by a shift in focus from COIN to concerns around Arab Spring-style 'strategic surprise', where it was a key element in the theoretical construction of the Digital Age conflict problem field in section 1.3. The importance invested in Web 2.0 in contemporary military understandings of irregular warfare is demonstrated comprehensively in the following sections – and is hinted at in the imagery used in the cover of the HSCB program literature reproduced in Figure 19.

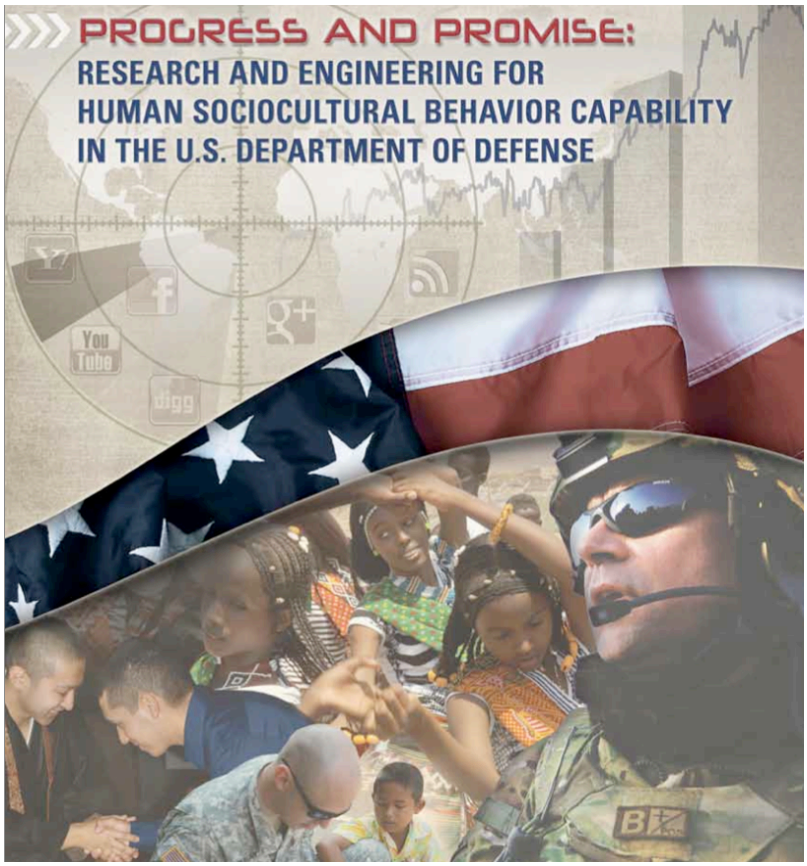


Figure 19. Front cover of MITRE report on HSCB Modeling Program, showing social media logos prominently within graphics (MITRE, 2013:Front Cover)

[103] Flynn's formal role as Director of the Defense Intelligence Agency mean his influence is significant across the areas these research programmes cover. He has given speeches, presented awards, and been the source of key ideas driving the HSCB program (see Poole, 2011:10; HSB Focus, 2011; Schmorrow, 2011b:12); and has been active in the SMA programme.

In discussing the relationship between science and conflict, the influential military analyst (and former Major General) Robert Scales writes of distinct periods of conflict characterised by their relationship to certain disciplines (drawing on Beyerchen, 1992). WWI was the "chemists war" for use of poison gasses, and WWII was the "physicists war" for the development of Radar and the Bomb. Scales calls the current phase of conflict the "social scientists war", in which "psycho-cultural factors" comprise the battlespace in the post-RMA age. In such a situation, Scales writes, "understanding and empathy [become] important weapons of war", and "perception control will be achieved and opinions shaped by the side that best exploits the global media" (Scales, 2006). So far, so similar to what we have seen in COIN discourse. But in the programmes examined here we see a further recognition that in the vast repositories of potentially significant information, platforms of engagement, and a huge number of people whose "psycho-cultural factors" matter in Digital Age conflict – this focus on the social goes global. In discussing the application of social science to the GWOT, an organiser of the SMA programme notes that "the [US Government] must understand socio-cultural situations across the entire planet to as high or higher level of fidelity that we did in Iraq and Afghanistan: without spending equivalent resources [which will…] require innovative techniques that don't require socio-cultural experts hand massaging ALL the data into actionable information" (Ehlshlaeger, 2014:xiii). Here, the programmes represent a broad approach to developing forms of *automated* (to varying degrees) socio-cultural data collection, analysis, and even engagement – further changing our understanding of military development and activity in the Digital Age, and thrusting a new type of social science integrated with computing and 'big data' analysis to military prominence.

The link of the R&D programmes to the problem field are clear throughout this chapter, which shows the development of tools for broad, sociocultural, predictive and PSYOPS-relevant intelligence. There are also links to developments in unconventional warfare thought in that Web 2.0 is also seen to be important in facilitating access to "denied environments" (Schmorrow, 2011a:x). HSCB documents frequently refer to the imperative to develop tools to gather data in environments which military researchers cannot access for reasons of political or practical infeasibility, as well as and the imperative to mine larger pools of open source data in all relevant environments (including those in which the US military is active) via semi-automated methods "with particular emphasis on social media" (Schmorrow, 2011a:x). Thus as well as seeking to "take advantage of an environment where useful information may be in 'plain sight'", in some cases social media tools may "serve as a viable alternative to surveys or polling in denied or difficult-to-penetrate areas" (OSD, RTD&E FY2015, 2014:80) – allowing, as has been suggested by UW special forces practitioners, new ways to access and influence populations in unfriendly foreign states.

This latter example suggests that social media tools are being retrofitted to enhance traditional intelligence activity – replacing polling, surveillance or vetting of potential allies, monitoring the literature produced by potentially restive groups, etc.. However, the scale of the shift to an intelligence paradigm which takes "phase 0" as its area of interest suggests a shift so substantial it becomes *qualitative*: one in which the subjects of intelligence shift from specific populations of enemies, their supporters, and select audiences of potential allies or adversaries; to one in which *everyone* is of potential interest. Building from country-wide COIN campaigns in which the "hearts and minds" of

the population were the key battleground; to the post-Arab Spring strategic environment - in which an ill-understood cocktail of dissent, outrage, networked public, viral messaging, and revolutionary momentum led to the overthrow of US allies in the region and a seismic shift in the strategic environment of the Middle East – the developing approach to 'sociocultural' intelligence and engagement found in these R&D programmes is one which vastly expands the interests of intelligence practices and potential military activity.

The focus on the ideological, social, and communicative elements of conflict, which generally takes civilian populations as they key area of interest, provides key context for the examined in this chapter. In the contemporary information environment where Web 2.0 is increasingly the best source of information about populations, and the best means by which to reach them with messages, this shift in strategic focus to civilian populations during peacetime matches the shift in platform with a shift in emphasis, foreshadowing a perfect storm of pervasive online data and communication couple with a powerful military actor in need of just such information and just such an audience. This chapter progresses with a presentation of the two key areas of development in this situation: the increased focus in sociocultural intelligence twinned with the rise in availability of open source population data; and the increased focus on psychological operations in the context of the rise of the Web 2.0. As we will see, as the focus of intelligence and influence moves "left of bang", a number of approaches are developing which call for a reassessment of the place of intelligence and communication in Digital Age conflict.

6.3. Academic Links: The Rise of 'Social Computing'

Before examining key developments in intelligence and military communication however, one important outcome in terms of the broader impact of military R&D which must be taken into account is the discernable effects on academic research. Much of the data for this chapter comes from academic contractors working on military-funded research projects, providing a useful repository of data and an example of the impact military R&D has on broader areas of social and intellectual life. All programmes involved in the study have substantial academic links: with the HSCB and SMISC programmes both sponsoring a large amount of academic research, the CORE Lab being based in a military university, and the SMA programme paying academics for bespoke research 'white papers' (e.g. Egan and Handenberg, 2012), and having a long-running series of weekly conference calls in which academics present research on areas of interest (see SMA – *TeleCon Booklet,* 2014). This extensive academic work is referenced throughout this chapter, however one particular area of note is the influence of military research on developing academic work at the conjunction of social research and computing science.

This influence is clearest in relation to the HSCB programme, where it is extensive and long-running. Figure 20 shows the breakdown of academic disciplines of HSCB awardees for the duration of the programme, who together account for the almost 500 articles and scientific reports listed in the HSCB bibliography of papers produced under the programme (see Mitre, 2013:67), these same disciplines predominate in a list of SMISC papers published by DARPA (DARPA, 2014, see page 169). Papers published under these projects have appeared in a range of conferences and journals, from the specialist (e.g. *Journal of Artificial Societies and Social Simulation,* e.g. Spraragen et al, 2013) to the general popular journals like *Science* (e.g. Song et al, 2010) and *Nature* (eg. Ahn et al,

2011). However, an examination of the HSCB Program shows that this academic influence goes beyond just creating a market for its preferred form of research. Rather, the DOD has been instrumental in producing a *platform* for this research to be developed and expanded within academia, producing a much more pervasive form of influence.

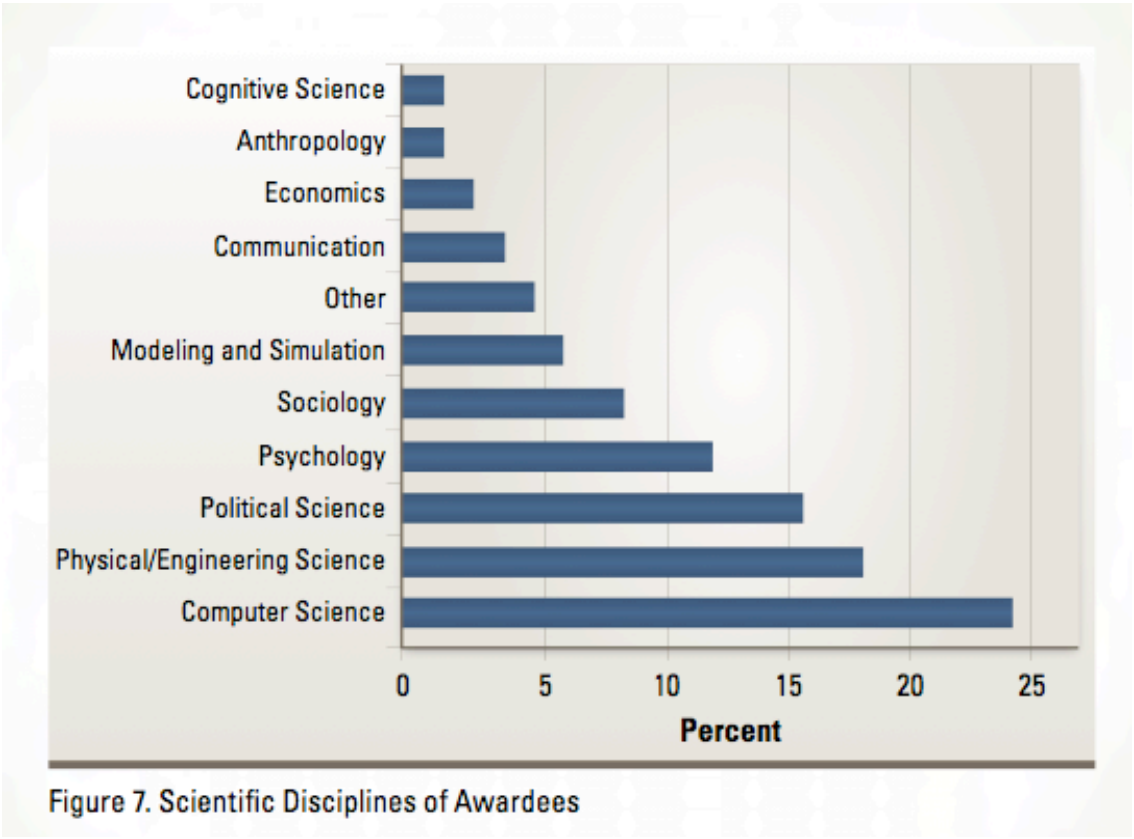


Figure 20: Academic disciplines of HSCB awardees (MITRE, 2013:13)

The links between military funding and the development of new areas of academic research has been studied by others in relation to propaganda and communication studies (Simpson, 1996), radar and advances in physics and computing (Pickering, 1995, Barnes, 2008), and in behavioural modelling and game theory (Robin, 2001). In each case emerging academic disciplines have been midwifed by the US military attempting to produce a knowledge base deemed necessary to face the perceived defence and security challenges of the age. In the case of the HSCB Program, involvement in the development of the field of *social computing* is a contemporary example of this phenomenon. Here, the DOD's role in the formative stages of a new discipline is instrumental in the direction of development of the discipline itself.

Social computing is a term applied to an area of academic research interested in the relationship between social interaction and computing science[105] – the area of interest here is that which "harnesses the power of computational methods to study social behaviour within a social context" (SBP2015, 2014). This is the subject of an annual international conference on *Social Computing, Behavioral-Cultural Modeling & Prediction,* which began in 2008. The first international conference in 2008 was introduced as "an

[105] For example in some cases it can apply to the 'computation' power of social groups, as in the aggregate decision-making of Surowieki's *Wisdom of Crowds* (2004), and in others to the role of computers in mediating social phenomena, which is the area of interest here.

interdisciplinary venue that set the stage for sociologists, behavioral scientists, computer scientists, psychologists, anthropologists, information systems scientists, and operations research scientist to exchange ideas, learn new concepts, and develop new methodologies" (Liu, Salerno and Young, 2008:i). Since then, it has become a key forum of discussion and the primary international conference for the presentation of research in the area.

The conference is also deeply entwined with the HSCB program, as can be seen by examining the editorial team, sponsorship, and content of the conferences. Two of the three editors of the journal which documented the first conference, John Salerno and Michael Young, are principal researchers in computing and psychology respectively at the Air Force Research Laboratory (AFRL, a key site for coordinating the HSCB Program); and the third, Huan Liu, is a key member of a team based at Carnegie Mellon and Arizona State Universities working on a long term DOD-funded program on blog and tweet-tracking (see Kumar et al, 2010; Carley et al, 2013; section 6.4.2). The 2008 edition of the journal documenting the conference – which became an annual publication – has an introduction written by two Office of Naval Research scientists (Tangney and Lytle, 2008, ONR is another key HSCB coordination site) who are thanked for helping to guide "relevant research activities with their insights and visions" by the journal committee, who also acknowledge the support of the director of the AFRL – John Graniero – "for encouraging us to organize" the workshop "and for providing ideas and funding to get it started" (Liu, Salerno and Young, 2008:ix).

DOD influence is also evident in the proceedings of the conference itself. The first and second conferences featured presentations by an anthropologist working for the Office of Naval Research asking for ideas on how the DOD can exploit Web 2.0 elements such as the blogosphere (Goolsby, 2008) and Twitter (Goolsby, 2009). At the opening conference she declared that "social computing is exploding and the imagination of the Department of Defense is overflowing with ways to exploit this brave new world" (Goolsby, 2008:25). This demonstrates a role for HSCB-linked figures in the funding, thematic guidance, organisation, and recording of *the* key conference in social computing, beginning with its foundation in 2008. This involvement is long-standing. The program committee for the conference every year since 2008 is roughly split 50/50 between academics and those associated with the military element of the HSCB program (e.g. see Liu, Salerno and Young, 2008; Yang, Greenberg and Endsley, 2012). For the 6 years of conference proceedings examined (2008-2013 inclusive) there were frequent changes in editors, however the military influence on the programme committee remained, as did acknowledged support from a number of DOD research bodies, including the AFRL, ONR, Air Force Office of Scientific Research, and Army Research Office[106].

There are also a further journal and conference in a related field with significant organisational or funding links to HSCB-related programs. The *International Conference on Computational and Cultural Dynamics* (ICCCD) began in 2007, sponsored by the Air Force Office of Scientific Research, and with a programme committee including Salerno, Liu, and ONR HSCB programme manager Ivy Estabrooke (see ICCCD 2007, 2009). The third

[106] Echoing the key link between special operations and much R&D, one of the 2013 editors is Nathan Bos of Johns Hopkins Applied Physics Laboratory, that year he was also editor of an update of the Army Special Operations Command's seminal *Human Factors Considerations of Undergrounds in Insurgencies* (see Tompkins and Bos, 2013)

conference in 2009 also included a keynote speech from Dylan Schmorrow on the value of computational modelling in providing support for "understanding and reasoning about the human terrain of battlespaces" (Schmorrow, 2009b), and presentations on the HSCB-linked W-ICEWS program (Kettler, 2009, see page 167) and from the influential Westpoint-based military computing scientist Paulo Shakarian (see Shakarian, 2014) discussing the use of computer models to locate IEDs in Baghdad's Sadr City (see Shakarian et al, 2009). Shakarian's co-author on this paper went on to edit the 2013 book outlining the state of the art in military and security applications of computer modelling – the *Handbook of Computational Approaches to Counterterrorism* (Subrahmanian, 2013). Another book, co-edited by Dylan Schmorrow, which presents the state of the art in the modelling and computational elements of "Cross-Cultural Decision Making" features many of the same topics and authors as the ICCCD conferences – demonstrating a leading figure in the HSCB program in a further role curating and publicising texts in the field (Schmorrow and Nicholson, 2010).

An analysis of the process and impact of military sponsorship in the development of this emerging discipline is beyond the scope of this research, as engagement with Web 2.0 is only a small part of this area. Where military-sponsored work (much of which is published in the titles mentioned above) does deal with Web 2.0 issues then it forms part of the data discussed in the following sections. However, it is important to that the role of the DOD in producing both *a market* and *a platform* for social computing research is a significant element in understanding the broader impact of its sponsorship of specific research programmes. In an emerging discipline this means one cannot go far without coming into contact with military-funded research, a fact that studies on previous iterations of military-social science development (Robin, 2001; Simpson, 1998, Solovey, 2001) have found to be significant in disciplinary development. Indeed, the analysis of bibliographic information and authorship above identifies the network of powerful actors behind what this chapter shows is a broadly coherent development in military R&D focussing on the intersection of Web 2.0 and sociocultural factors. These themes and developing networks are highlighted throughout this chapter.

The funding that these military programmes provide clearly produces a strong effect on the academic interests of those who rely on that funding – adding a military imperative to their research. Elsewhere in GWOT era scholarship, this process has been the subject of critique and controversy. A military funding project called the Minerva Initiative, which draws on social science to improve the "DoD's basic understanding of the social, cultural, behavioural, and political forces that shape regions of the world of strategic importance to the U.S." (Minerva – Program History, 2014), has been the subject of academic critique based on the concerns about military influence on and use of academic research (see Albro, 2008; Krebs, 2008; Gusterson, 2008; and Asher, 2008), including the channelling of funding into projects focused on Islam and 'foreign' ideology in a way which overstates and essentialises these as elements of national security thought (Tirman, 2008)[107]. The project also has links to the controversial development of counterinsurgency thought widely criticized by academics as anthropologically myopic amid concerns of the

[107] Similar criticisms have been made of HSCB-like projects in the DOD as based on "an outmoded model of reified, neatly bounded, homogeneous culture that doesn't really exist" (González, 2013:78).

"weaponisation" of social science in Iraq and Afghanistan (e.g. see Network of Concerned Anthropologists, 2009)[108].

This concern with "weaponisation" is not simply academic in the case of social computing. The HSCB Program has instituted a *Social Network Analysis Reachback Capability* (SNARC) cell which connects HSCB academic researchers directly with in ISAF intelligence cell which is part of the Information Dominance Center in Afghanistan, with the academics providing subject matter expertise and practical analytic support for the processing of Afghan social network data into military intelligence products (see HSCB Newsletter No 9, 2011:2; Mathieu, 2011:3; Schomorrow, 2011b:38; MITRE, 2013:33). Though such direct links between academia and military are potentially dangerous, they are relatively few (those which *do* exist are discussed in this chapter), and the more general influence on academic research is potentially of greater consequence in the long term: driving research agendas of military interest and producing a knowledge base within a military context where intelligence, surveillance, and influence are key areas of policy development (see Whitehead and Finnström, 2013:10). The current relationship between military R&D and social science seems to be re-playing the dramas of that relationship in the 20th century, Solovey notes that during the Cold War "psychology's most important extra-university patron was the military" interested in the "hearts and minds of individuals" in conflict (Solovey, 2001:175), and that military funding of communication research built it into a "science of coercion" (Simpson, 1998 in Solovey, 2001:177). The most controversial instantiation of this relationship - Project Camelot, which would have seen social scientists produce country-wide analyses of the revolutionary risk or potential of foreign countries – was directly based in counterinsurgency thinking which wanted to study "factors involved in the causation and conduct of small wars" ("small wars" being a synonym for insurgencies, Solovey, 2001:180). As this chapter demonstrates, the R&D programmes under analysis grow out of precisely the same concerns, and in the data below we can see how they are addressed in a thoroughly Digital Age manner.

6.4. Web 2.0 and Developing Intelligence Practice

In discussing the strategic context of Digital Age conflict I identified military intelligence as an important area of development. Intelligence is information instrumentalised for military purposes, it can pick out targets, surveille, and assess the physical, political or human terrain. It can support forms of tactical activity from lethal targeting (such as drone strikes or JSOC raids) to psychological operations (through intelligence on cultural norms, narratives, or potential emotive issues), and the area of social network analysis (SNA) was picked out as particularly influential in Digital Age conflict discourse. Intelligence also works at the more strategic level to provide warnings to policymakers or planners on events or developing situations of interest, which in turn facilitates different forms of intervention. This section shows how contemporary R&D in military intelligence

[108] Two of the first Minerva Chairs – funded academic research positions at American defence establishments – were Montgomery McFate, the architect and chief ideologue of the controversial Human Terrain System (see e.g. Price, 2013); and John Nagl, a key counterinsurgency theorist and one of the authors of Counterinsurgency Manual (Minerva Chairs Program 2014).

addresses both ends of the spectrum – retrofitting existing SNA-inspired intelligence practices with Web 2.0 tools, and developing new paradigms of strategic intelligence. Taken together, they show military reaction to the rise of Digital Age conflict with a number of important outcomes for our understanding of the relationship between knowledge and power, and the way populations are understood and addressed within military thought and practice.

6.4.1. Social Network Analysis and Web 2.0 Intelligence

The most prominent organisation within the DOD addressing operational intelligence in relation to Web 2.0 is the Common Operational Research Environment (CORE) Lab, which sits within the Defense Analysis Department at the Naval Postgraduate School[110]. The Lab is tasked with supporting US military operations in helping "to develop a comprehensive understanding of the Irregular Warfare environment" (CORE Lab – *The Lab*, 2014) – meaning that it focuses on producing analytic tools for this type of data in support of COIN and special operations. The Lab performs both an education and R&D role, training officers and NCOs in the use and development of intelligence analysis tools[111], promoted as "made by operators for operators", with efforts "directly applicable to special operations, intelligence, information operations, psychological operations, civil-military operations, counterinsurgency, counter-terrorism, and irregular and asymmetric warfare" (CORE Lab – *The Lab*, 2014). It is thus a key R&D location for the development of intelligence related to special operations, unconventional warfare and other areas of military practice central to Digital Age conflict. Due to its interest in relational data, SNA is a key area of development within the CORE Lab (see Figure 21), which it seeks to operationalize to operators with "a deep understanding of the indigenous population, social networks and the human domain in the operational environment" (CORE Lab – *Certificate Program*, 2014). The Lab seeks to build understanding of this human domain from what we might call a 'big data' perspective – focussing on relational, geospatial, and temporal data as opposed to anthropological or linguistic studies of other societies or cultures, which are found elsewhere in the military structure (see, e.g. Army Human Terrain System, 2014).

[110] This department is at the forefront of thinking on developments in information age warfare. The heads of department here are key information warfare theorists Dorothy Denning and John Arquilla, and a number of recent Masters theses address the issue of information and influence operations in the contemporary information environment (see Brown, 2012; Duncan, 2013; Lopacienski et al, 2011; Stoebner and Wedlake, 2012). The CORE Lab is run by a Special Forces Colonel, Greg Wilson, and Sean Everton, a prominent "dark network" theorist and author of the first book "in which counterinsurgency theory and social network analysis are coupled" (Everton, 2012b: back cover).

[111] It has also trained staff from US allies. See, for example, work by Major Carlos Padilla of the Colombian military which uses SNA and geospatial data to hypothesizes the position of FARC camps (Stewart, 2012) and mines relational information to identify "several [potentially key] FARC members who appear to be flying below the conventional wisdom radar" (Cunningham et al, 2013:492).

Members of the Naval Postgraduate School's Common Operational Research Environment (CORE) Lab are working on innovative ways to analyze open source information gleaned from social network sites. This information is allowing researchers to visualize troubled regions with greater fidelity than conventional intelligence analysis methods.

Figure 21: Image from Navy promotional material for the CORE Lab (Stewart, 2012).

The Lab has produced a number of tools which have been applied to contemporary military activity. *Lighthouse* is the most significant, and provides a good example of how SNA has been applied to the COIN situation. Lighthouse is an iOS and Android app which allows operators in the field to use smartphones to log and share biographical and relational data about individuals in their area of operation, and analyse it using commercial and military intelligence analysis tools. It has been used by US forces in Afghanistan, the Philippines, and "domestically to support counter-gang activities" (see Lighthouse – *Collecting Data*, 2011; Lighthouse – *About Lighthouse*, 2012; and Goode, 2012 and Weineberger, 2012 for articles on domestic use). A presentation by one of Lighthouse's developers describes how it has been used in Afghanistan to support COIN operations by mapping links (business, tribal, family, etc.) between individuals in various areas of operations (YouTube – ccpnmike, 2012). He describes how it has supported decision making on whether it would be beneficial to have a particular bad apple "removed from the community" (i.e. killed or captured) through mapping his social relationships in SNA form and assessing the impact his 'removal' would have (see Figure 22). It was also used to map the ego network around a recalcitrant tribal elder in order to figure out who the military might empower around him to undermine his influence (YouTube – ccpnmike, 2012, see also Everton, 2012b:xxvii-xxviii).

Another article describes how Lighthouse has been used at a more general level to identify powerbrokers and key leaders, map local grievance networks, and visualize "human dynamics" such as trust and affiliation amongst important local actors (MacCalman et al, 2013). Duffield has written how in the COIN age "anthropological tools are retrofitted to guide drone attacks and destroy enemies' social capital" (Duffield, 2011:7). These examples demonstrate both potential outcomes, showing the blurred line between "population-centric" and "enemy-centric" SNA. It shows that large-scale social-level SNA *can* incorporate the application of precise violence, but also provide non-kinetic ways to 'target' individuals through manipulating the social fabric to undermine or exclude them. In such circumstances, we can see a military intelligence system which incorporates the whole of society into its analysis, and *all* operational options (from a charm offensive to a military one) into its arsenal.

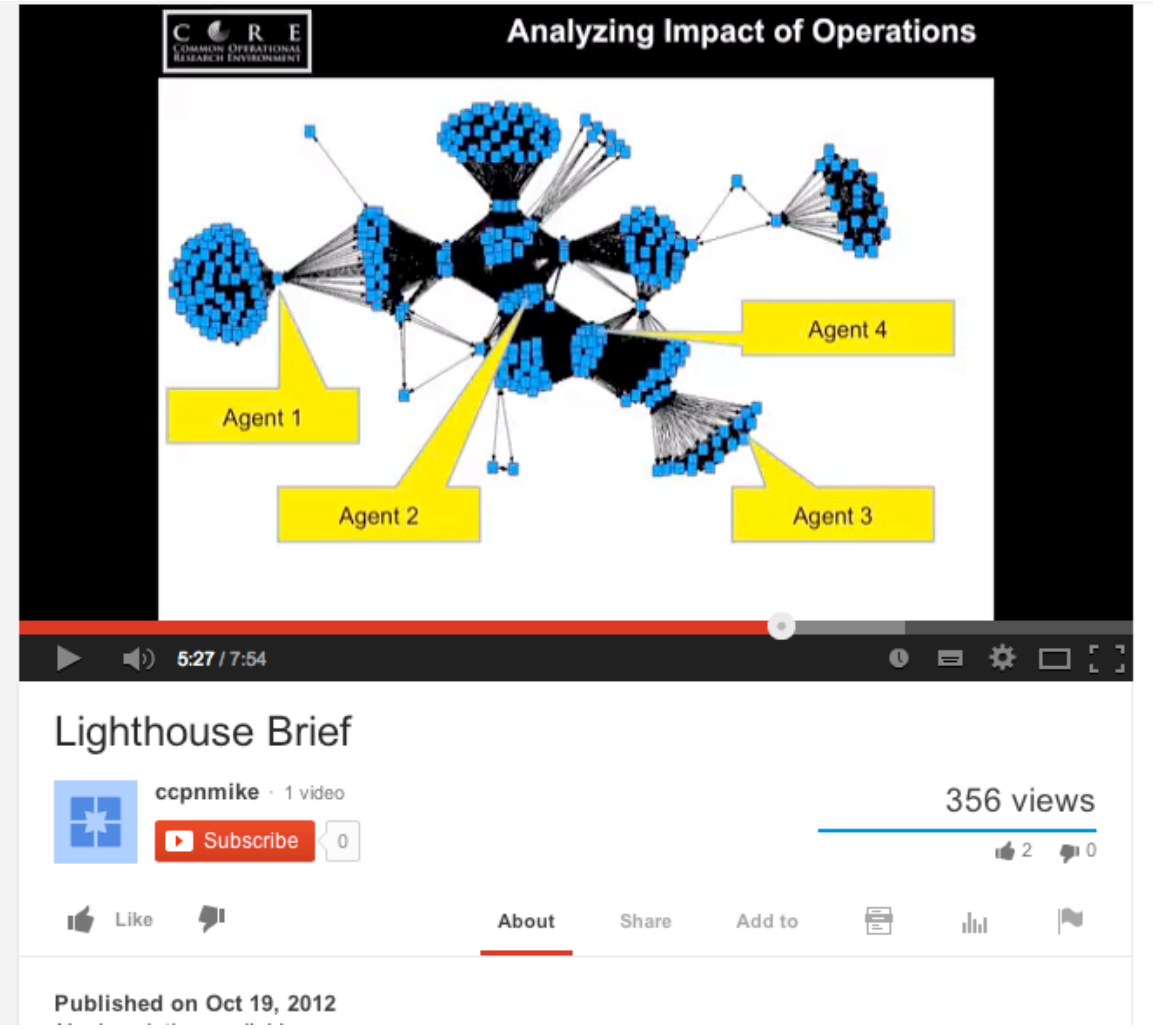


Figure 22: Screen capture from Cpt Carrick Longley's presentation on Lighthouse – the tool was used to assess what would happen if Agent 1 was "removed from the community"

This contexts underlines the necessity of examining how this type of tool is being adapted and applied to the Web 2.0 environment. Since 2012 the work of the CORE Lab has increasingly been based on the analysis of Web 2.0 sources as a form of intelligence data. Everton, one of the course directors, notes in an article on "social media, dark networks, and counterinsurgency" that "network data culled from publicly available micro-blogging

tools such as Twitter can help analysts and operators identify individuals worth tracking, and ideally improve knowledge of the network. This kind of knowledge is essential to improve the crafting of disruption strategies over time" (Everton, 2012a:71). As the Lighthouse example shows, in special operations thought "disruption strategies" include everything from PSYOPS to assassination, reinforcing the understanding that monitoring Web 2.0 for social knowledge and using it for the targeting of physical or psychological disruption are not conceived of as separate in a special operations approach. Thus any system of Web 2.0-derived intelligence and SNA-based analysis must be understood as potentially facilitating the full spectrum of military activity.

Demonstrating the CORE Lab's turn to Web 2.0-based SNA, is a paper on 'mining Twitter data from the Arab Spring' (Schroeder et al, 2012) which performs a social network analysis of Twitter accounts using Egypt-relevant Arab Spring hashtags as a data sample. While the turn to Web 2.0 within the CORE Lab is interesting in itself, the analysis presented in the paper is very weak, the main 'finding' being that the popularity of a Hosni Mubarak parody account "suggests" it "may have helped frame Mubarak as a corrupt and incompetent leader [and] may have contributed to people's sense that the moment for change (opportunity) had come" (Schroeder et al, 2012:61). While this is an almost ludicrously vacuous analysis of one of the defining revolutionary moments of the a generation, it does demonstrate that a shift to an engagement with online social network data comes with a shift away from a narrow focus on "dark networks" to a broader examination of much wider communities of interest – and consequently a wider analytical focus which seeks to understand cognitive or social facets of a situation (an expansion of both the *subjects* and the *subject* of analysis). However, it also cautions us to be aware that institutional importance and pre-Web impact do not necessarily translate into a sophisticated engagement with Web 2.0 – perhaps highlighting why insight is sought from academia.

A more comprehensive but similarly contradictory development at the CORE Lab is the development and promotion of a new program – the Dynamic Twitter Network Analysis (DTNA) tool. The tool is the Lab's first concerted effort to use Web 2.0 data for intelligence analysis, and has been the subject of a number of articles and presentations since 2012 (Stewart, 2013; Davis, 2012; Dudas, 2012; Lucente and Wilson, 2013). The DTNA is outlined in Figure 23, and is a fairly straightforward tool providing similar capabilities as many commercial off-the-shelf products: it collects tweets in real-time which match certain parameters (key words, hash tags, geographic location, etc.) and saves them in its database. These tweets can then be represented and manipulated in three ways: as a curated Twitter feed, as geo-located messages on Google Maps, and as a network visualisation based on Twitter relationships produced using the ORA tool (discussed in the next section) (Dudas, 2012:1). While this tool is weak in comparison to many commercial programs, its application within a military lab which directly supports special operations, and which is tasked with developing new intelligence practices for irregular warfare, is significant, providing a potential basis for the development of more bespoke intelligence tools which tap into the CORE Lab's significant SNA experience. We can also see, in a number of other R&D projects discussed later, the military-sponsored development of further tools and practices which have the potential to increase the utility and power of this form of social media analysis.

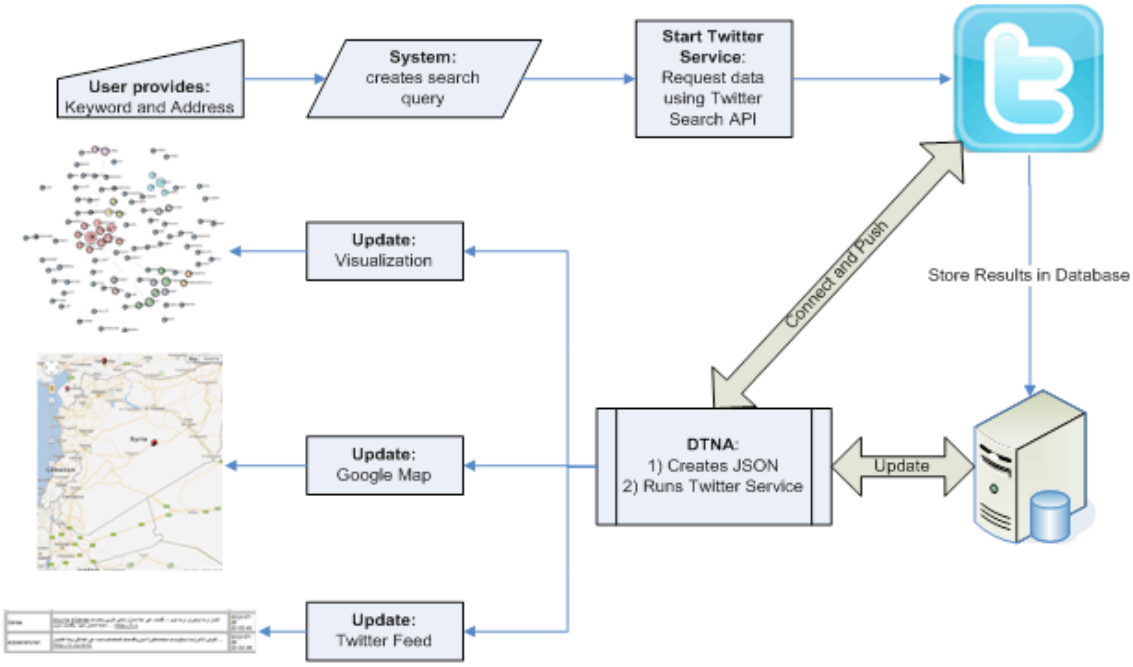


Figure 23: "Architecture of DTNA" (Dudas, 2012:3)

Military scholars working on the DTNA project describe how "social media users are freely and enthusiastically posting a trove of information about themselves. In fact, social media users are providing much greater clarity than can be achieved by conventional means" – noting that in relation to the civil war in Syria "open source media (Facebook, Twitter, YouTube)" provide "valuable insights into what is happening on the ground" (Lucente, in Stewart, 2013). This will comes as no surprise to anyone who has followed the news from Syria, where photos and videos posted on social media make up much of the news on the conflict. The work of open source-based journalists such as Elliot Higgins (aka Brown Moses, see Raden Keefe, 2013) have provided meticulous analysis of major events of the conflict. To demonstrate the operational utility of this, CORE Lab researchers have used DTNA to assess Syrian rebel groups in order to provide advice on a hypothetical larger US military intervention in the country (Lucent and Wilson, 2013; Steward, 2013).

The importance of the work using DTNA to examine the Syrian opposition does not lie in its dubious novelty or insight – it simply assesses links between well known rebel groups on Twitter as well as their known geographic locations. Rather, it lies in the discussion of the application of these methods to a broader range of situations related to irregular and unconventional warfare. In Syria, Lucent argues that in assessing the rebel groups the program can be used for "enabling U.S. special forces operators to quickly highlight potential partners in a troubled region", and to identify those "who share common values with U.S. interests in the region" (Lucente in Stewart, 2013; see also Lucente and Wilson, 2013:23). The tool was used to identify which local militia US special forces could conceivably work with in order to "protect potential weapons-of-mass-destruction sites in Syria"[114]. Identifying and liaising with regional proxies to fight wars on the DOD's behalf is

[114] Again, the research itself is not groundbreaking – they identified the potential of working with the Farouq Battalion in Homs – at the time a powerful FSA-affiliated militia which held territory close to suspected WMD sites (Davis, 2012). A suggestion which one could have come to by simply reading the news from Syria.

a key element of special operations where Web 2.0 is being significantly addressed, the DTNA provides both another tool and further impetus to this endeavour.

Further underlining the UW links of the tool, in another article DTNA authors write of how the tool could be used to provide intelligence for "assisting an ongoing rebellion", which "requires in-depth knowledge of a country's socio-cultural dynamics, social structure, resistance potential, and how those willing to take up arms against their government might align with U.S. policy objectives" (Lucente and Wilson, 2013:21). Social media also has the bonus of providing detailed insight into the "socio-cultural dynamics" of a region, and what "issues or grievances [are] resonating with the local populace" (Stewart, 2013). Indeed, the DTNA has already been "field tested by three Defense Department units overseas to help gauge public opinion" (Davis, 2012), demonstrating the active application of the tool in PSYOPS-relevant intelligence practice. Thus, the use of DTNA – while currently limited – represents a move within a key education and research branch of the special operations community to "leverage[…] open-source social media (YouTube, Twitter and Facebook) along with advanced analytical methodologies like social network analysis to increase [the special operations community's] understanding of both the political and armed opposition" (Lucente and Wilson, 2013:21). It provides easy and expansive access to "denied areas" where potential special operations interventions may take place, and facilitates a range of activities from identifying potential conduits or partners, to the refinement of PSYOPS activities.

While Web 2.0 development at the CORE Lab is not very technologically sophisticated it is nevertheless a significant growth area for special operations practice and Web 2.0 intelligence. The flexible approach to SNA within the Lab seeks to optimise the range of military options their analysis can provide – in the warzone of Afghanistan this included everything from kinetic targeting to manipulation of social capital. The engagement with Web 2.0 in terms of UW practice for accessing denied environments and gaining PSYOP-relevant intelligence is the low-hanging fruit of adaption of SNA online – as case studies of both Syria and the Arab Spring proliferate in the literature (see e.g. Lunch, 2014; Guerrini, 2014; Aday, 2012; Petit, 2012). They are also relatively uncontroversial areas of military engagement with online social networks ("US military school studies Syrian rebel groups" is not a news story without context, "US military school identifies targets via social media posts" would be). However, pre-Web use of SNA shows that once understanding of the tools and networks is developed, these two types of activity (general broad intelligence and targeting) can take place in the same conceptual universe, suggesting potential future activity in this area entails serious consequences for populations included within the purview of special operations intelligence.

6.4.2. Web 2.0 and SNA in Broader Military R&D

While the CORE Lab provides the institutional example of the most direct application of SNA-enabled intelligence to irregular warfare, its lack of technological and analytic sophistication makes it of interest more for its intent and context than its outcomes. However, such is the interconnected nature of the Web 2.0-focussed R&D community in the DOD that we do not have to look far for more sophisticated tools based in the same institutional context. The analytic platform underlying both major CORE Lab projects (Lighthouse and DTNA) is a computer program called Organizational Risk Analyzer

(ORA)[115], a tool developed at the Computational Analysis of Social and Organizations Systems Center (CASOS) at Carnegie Mellon University. It was developed under the leadership of Dr Kathleen Carley, the director of CASOS, and both she and the Center are key entities in the wider sociocultural, SNA and Web 2.0 military research community (see, e.g. Carley, 2014; HSCB Newsletter No 2, 2009:12-13).

ORA was developed as a tool for what Carley calls "metanetwork analysis" (elsewhere she calls it "Dynamic network analysis" (Carley, 2005)) – an analytical technique that moves beyond the purely relational data of SNA (which is of limited application to military problems) and incorporates network metadata. Ading to the "who" of classic social network analysis the "what" of event analysis, the "where" of geospatial analysis, the "how" of semantic networks and the "why" of belief networks (see Carley, 2008:6). It also incorporates sociocultural elements such as norms, attitudes, gender, and age in a process that goes "way beyond general social network analysis" (Carley in Bohannon, 2009:411). The tool has been applied extensively in automatically extracting such data from bodies of text to produce much richer networks of entities and relations than classic SNA (Carley, 2005, Fusco, 2010). It uses natural language processing and other entity-extraction techniques to, for example, automatically identify ideological positions associated with certain figures of speech, or formalise location data based on textual cues. Basically it expands the relational analysis of SNA to the range of elements that can be extracted from data about individuals or groups through automated processes, and uses advanced computational methods to sort and analyse the data into a form useful to human analysts.

HSCB literature reports that ORA has been used "for analysing large scale dynamic networks" by "various law enforcement units, government agencies, the military, and various corporations". The tool has been used to identify emergent leaders, key locations of enemy activity, links between gangs, and vulnerabilities of terrorist cells (HSCB Newsletter No 2, 2009:12). The sophistication of this tool in mining network data beyond the purely relational analysis of structured data-sets can be seen in the work of Carley and McCulloh (a PhD student and Army officer) who used it to mine over 1500 YouTube videos of insurgent attacks in Iraq and extracted all the metanetwork data they could to produce an extensive network analysis. McColloh says that at this level "when you go back and look at the videos in [extracted cluster] groups, you see forensic clues that identify who some of the insurgent cells were", and says that he and Carley "worked with the U.S. military to "operationalize" the technique in Iraq" (Bohannon, 2009:411)[116]. This advanced form of SNA, aimed at insurgent bombing videos (one of the paradigmatic examples of Digital Age conflict), and put into practice in Iraq, shows a much more serious and sophisticated form of SNA than anything at the CORE Lab.

Carley and McCulloh's work has been further integrated into developing GWOT practice. The use of ORA for metanetwork analysis has been integrated into intelligence classes at the United States Military Academy at West Point "to determine what persons in a terrorist network hold the most valuable information" (Fusco, 2010, see also Boguchwal,

[115] A large section of Sean Everton's book is also basically a manual for using ORA for the analysis of 'dark networks' (Everton, 2012b:69)

[116] This work has not been published and requests for access to it were unsuccessful due to military sensitivity, though the references to Carley's work provide extensive information on the tools and practices the project was based on.

2012). It is also used in the DOD's anti-IED organisation "where [they use] ORA to track down chief IED makers and key connections in the terrorist network" (Fusco, 2010), and McCulloh himself went on to be deputy director of the Counter-IED Operations Integration Center in Baghdad (Gjelten, 2010). In these applications, ORA has been applied directly to the kinetic, enemy-centric, end of the spectrum in military intelligence. One article quotes McCulloh describing someone as a "highly central node", noting that "when the US military is looking for key people to capture or kill, you do not want to be identified as "a highly central node"" (Gjelten, 2010).

While not all uses of ORA discussed above use Web 2.0 data in their analyses, the practice of metanetwork analysis drives a thirst for *any* data which can be yielded. Carley says that the system requires all the information it can get, including from phone intercepts, informants, and detainees: "you try to find things about who else they know [...] who they're related to, where they've been in the past, where they were trained, what other kind of group did they belong to, things like that" (Carley in Gjelten, 2010). In a situation where Web 2.0 data is increasingly accessible and rich – as seen in the DTNA example – the utility of such data under this analytic system is clear.

The thirst of such intelligence practices for data has led to accusations by a whistle-blower that as these tools were emerging there was an increasing pressure for intelligence collection in the GWOT being run on the basis of a "mosaic philosophy" in which detainees were interrogated simply to provide general network background data, in situations in which "it did not matter if detainees were innocent" (Wilkerson, 2009). The approach was to "extract everything possible [...] to have sufficient information about a village, a region, or a group of individuals [...] thus, as many people as possible had to be kept in detention for as long as possible" for it to work (Bohannon, 2009:410). Lawrence says that this philosophy was not widely applied in the military due to allegations of torture leading to aversion to systematised unnecessary detention (Bohannon, 2009:410). However, it is significant that the turn to Web 2.0-enabled SNA offer an alternative, less intrusive, application of the "mosaic philosophy", allowing a new and less-controversial form of persistent surveillance and comprehensive data collection. We know that ORA is used in YouTube-based analyses to hunt IED cells, in the CORE Lab's Twitter analysis tool, and is taught in military intelligence courses – in the context of the proliferation of Web 2.0 data the potential application to a wide range of military activities is clear.

We need not rely on *potential* applications however, as under the HSCB program and other military R&D initiatives the work of CASOS has been directly applied to Web 2.0. Collaborative work by CASOS and Arizona State University is some of the most extensively funded under the HSCB programme[117], and the two have collaborated in developing advanced tools to gather and analyse social media data for military application through tools called BlogTracker and TweetTracker (see Agarwal et al, 2008; Agarwal, 2009; TweetTracker, 2014). The first project, BlogTracker, was funded by the ONR explicitly to address US military information needs and ensure it stays at "the frontier of stability operations" (a term referring to the 'end game' of a counterinsurgency war, see DOD - *JP 3-07,* 2011) through assessing information in the blogosphere relevant to such operations and "identifying conflict indicators and potential threats" in blogs (BlogTracker, 2014).

[117] e.g. see DOD-funded projects presented in papers by Abbasi et al (2012), Abbasi and Liu (2013), Liu et al (2013), Barbier and Liu (2011), Zafarani et al (2010), and Goolsby (2008, 2009).

The project goes far beyond the rudimentary analysis of DTNA – and includes three funded PhDs addressing both the 'big data' computational analysis of social media such as detecting communities and groups (Wang, 2013), and tools for automating the qualitative elements such as assessing sentiment of bloggers and trustworthiness of their information (BlogTracker, 2014; Agarwal, 2009; Moturu, 2009).

The project was followed by TweetTracker (also funded by the ONR), which builds on the previous project and adapts the tool to the Twitter platform – developed by researchers who have also published a key text on Twitter data analytics (Kumar et al, 2013)[118]. TweetTracker has been presented as a tool for assessing population needs and military priorities during disaster relief (Kumar et al, 2011; Abbasi et al, 2012), used at the Naval Postgraduate School to monitor Web 2.0 activity around the 2014 Afghan elections (TweetTracker, 2014), and for a training exercise at US European Command analysing social media data relating to the attack on the US Embassy in Benghazi in 2012 (Carley et al, 2013). In the later case, in a paper co-authored by Carley, Liu (a key HSCB-sponsored researcher at Arizona State), and Goolsby (the ONR anthropologist who initially pitched the military's interest to the social computing community)[119], the authors describe the use of TweetTracker in conjunction with ORA to train EUCOM intelligence analysts to monitor social media in unfolding regional crises, asking "how can the analyst or policy maker get early insight into a crisis as it unfolds? What information is available? How can that information been tracked? Finally, are there any early indicators or warning signs of crisis?" (Carley et al, 2013:1). In the Benghazi example, the paper identifies "key influencers", early "indicators" of unrest, and tracks general population sentiment in relation to the protest in Benghazi and the subsequent Embassy attack (Carley et al, 2013:8). A similar paper outlines the use of the tool in monitoring the 2013 Kenyan elections, where it was used to identify emergent leaders, cliques, various organizations and groups, the connections between them, and key locations of potential unrest (CASOS, 2013).

Here we can see the direct application of SNA-based analytical tools driven by Web 2.0 data, produced by computing and information scientists at the cutting-edge of academic practice with substantial links to military R&D programmes examined, offering insight far more developed than the strictly military-based operation of the CORE Lab. In the research papers the tools are applied to 'softer' military operations such as disaster relief, election/stability monitoring and crisis response. However the intelligence they produce – the identification of surges in public opinion, instability indicators, attack precursors, key influencers and individuals, cliques and groups of interest – are applicable to a much wider range of military practices, covering the whole spectrum of potential military interaction with individuals, from guiding regional PSYOPS campaigns to targeting. The links of those involved in producing these tools to DOD special operations R&D compels us to take this possibility seriously.

---

[118] Further demonstrating key links between military R&D funding and the cutting edge of social computing: individuals involved in these projects are also the authors of *Social Media Mining: An Introduction* (Zafran, Abbasi and Liu, 2014)

[119] Carley, Liu and Goolsby have also been among the HSBC-linked people promoting social computing as a tool to deal with "crisis in the new information age" to European military and intelligence officials – having key presenting and chairing roles at an October 2013 conference on the subject aimed at a NATO audience (see ISC, 2013).

Work in this area under the projects examined here – focussing on entity-extraction from social media data, natural language processing, sentiment analysis, and other aspects of online communication - is indicative of broader research trends within the HSCB and SMISC programmes, lending important context by providing an example of the direct military application of such tools. HSCB literature outlines the growing importance and possibility, of "population-centric sensing" in the contemporary operational environment, and has sponsored a number of projects focused on "analysing patterns of life, social media and social networks" for "countering violent extremism" and "forecasting instability" (MITRE, 2013:42). A look at the research projects carried out under the HSCB and SMISC programmes demonstrates that while tools like DTNA, ORA and TweetTracker are the most prominent in that their direct application to military operations has been reported, they are supported by and incubated within a much broader range of military-sponsored research at the cutting edge of social media analytics.

One of the most basic capabilities that social media allows is open access to the public opinion and sentiment of large civilian populations, the understanding of which is key to US military planning. In this area the DOD has funded a number of projects exploring the use of social media data to provide real world insight into the opinions of foreign populations: such as a project at Johns Hopkins Applied Physics Laboratory examining whether Twitter in Nigeria can be analysed as an effective (cheaper, less intrusive and reflexive) proxy for opinion polling and surveys (Fink et al, 2012, see also Steckman, 2014 for a similar project in the SMA programme), and one which seeks to identify particular blogs as "bellwethers" for broader public opinion and behaviour (Ulicny, 2008). At the more advanced level, projects at Arizona State (separate from those discussed above) examine whether social media data is a more effective means than surveys to anticipate not just populations opinions, but their *behaviour* (Abbasi et al, 2012; Liu et al, 2013). This form of sentiment analysis meets the Digital Age intelligence requirements for accessing 'denied environments' through the Web and for developing intelligence more useful to PSYOPS processes.

The DOD also provides R&D funding for tools which focus on the individual- or enemy-focussed area of intelligence. For example a DARPA project on using social media to "track the evolution" of social groups online (including "terrorist and criminal organizations") (DARPA – *STTR 2012.b Topics*:12), has funded research which seeks to add an analysis of social media message content (attitudes "towards entities, issues, beliefs, and other participants") to existing SNA-based analyses (DOD - *STTR FY12.B*, 2012:29)[120], adding an automated analysis of individuals' opinions to their analysis as part of a social network project. Another focuses on using social media to produce SNA-based "signatures" (such as follower or retweeting patterns) rather than semantic content of messages to identify "anti-social activities" and "hostile actors" online (DOD - *STTR FY12.B*, 2012:26). This is based on the idea that such signatures are much easier to detect at scale than the automated processing of semantic content, basically making the identification of "hostile actors" an exercise in algorithmic pattern-matching. Both of these approaches automate what were previously manual tasks of understanding opinion and assessing actors' roles

[120] This project was performed by The University of Michigan and the Ntrepid Corporation – who performed the infamous CENTCOM "sockpuppet" contract discussed earlier.

in relation to military activity – suggesting more pervasive, extensive, and robotic forms of military intelligence.

Taking this one step further, in 2012 the Air Force funded projects which addressed the analysis of social media to identify "active entities" developing plans of interest to the military (USAF - *FY2012.1 Topics*, 2012:62). This included one which developed SNA tools to "detect and link multiple aliases" across social media, and "assist analysts in identifying threats" or "monitor events being discussed and planned online [and] understand[ing] who the protagonists are, what they have done, and what they are planning" (DoD - *SBIR FY12.1*, 2012:233). A similar project sought to apply SNA to identify and provide intelligence on "distributed terrorist activities enabled by social media" and to provide insight which could both "pre-empt a terror event" and "understand the geo-political situation within a dynamic environment (e.g. Arab Spring)" (DoD - *SBIR FY12.1,* 2012:233). Although in these cases only the project abstracts are available and thus we cannot fully understand their outcomes, this conflation of "terror events" and the Arab Spring highlights the dual-use nature of the range of social media and social network analysis tools we have seen throughout this chapter – facilitating both population-centric and enemy-centric intelligence practices through Web 2.0.

This proliferation of military R&D which directly addresses social media as an operational intelligence source demonstrates a broad effort to harness the possibilities provided by the new information environment. At the CORE Lab this has been developed to facilitate UW and other clandestine operations. The examples of the ORA and TweetTracker show that underlying the technically-unsophisticated developments of Web 2.0 intelligence within DOD institutions there is a strong knowledge base in military-sponsored research in academia and commercial sectors. The work presented here largely draws on a social network analysis background – both because of its prominence in contemporary military thought and its obvious applicability to the social networks of Web 2.0. However, Web 2.0 data has also driven a development of the military potential of SNA itself – away from an approach which focuses narrowly on the relational data of 'dark networks' of insurgent cells or terrorist groups, to one which incorporates new forms of data about the content of messages in networks, sentiment of actors, and new means of establishing identity. This developing approach greatly expands the size of the population relevant to intelligence analysts – with broader social networks within areas of interest offering an important new site of analysis which can be accessed via Web 2.0 and captured and analysed by developing tools. This expansion of relevant populations in military intelligence is taken even further in more strategic intelligence programmes – working on larger forecasting and predictive bases – to which the analysis now turns.

6.4.3. Social Radar and Strategic Population-Centric Intelligence

The SNA-derived research above represents Web 2.0-linked military intelligence at the operational and tactical level – those with the possibility for the most direct impact on the ground. However, other Web 2.0-based developments focus on the broader strategic level. These developments guide a significant amount of R&D under the developing paradigm of *social radar*. Social radar is, broadly speaking, a paradigm for thinking about population-centric intelligence at the strategic level – using social media and other open source data to monitor regional instability and guide broader military policy. The concept is one of the

key outcomes of the HSCB programme, which has promoted research in which the collection and analysis of open source data on population dynamics (changing social groups, opinions, information flows) at the regional or global level is seen as a key tool for guiding military policy, and attempting to meet the "Phase 0" intelligence imperatives of the Digital Age strategic environment.

Rather than a particular programme, social radar is a new paradigm or "organizing metaphor" for development in Web 2.0-related military intelligence (Maybury in Shachtman, 2012). It is a concept promoted by Mike Flynn as DIA head and key SMA ideologue (Flynn et al, 2012:15), HSCB head Dylan Schmorrow (2011), the chief scientist of the Air Force (and inventor of the concept) Mark Maybury (2010), and it has been adopted by key contractors MITRE Corporation[121] (MITRE – *Social Radar Technologies,* 2014) and Lockheed Martin (Lockheed Martin – *ISPAN,* 2014) as a framework for their own development. As organising metaphor it provides vital context for an array of military R&D projects which have direct relevance to the military exploitation of and engagement with Web 2.0, and seek full engagement with Web 2.0 in everything from predicting unrest to crafting state communication strategies.

Social radar was first outlined by Maybury in 2010, who described a new intelligence paradigm required in the context of a shift in the "center of gravity in modern warfare" to one which "includes perceptions, intentions and behaviors of citizen and leaders" (Maybury, 2010:1) – a population-centric approach to strategy in the age of a global information environment. The 'radar' is conceived as supporting two main aims: the forecasting and assessment of security-related events (such as political disruption and insurgencies) in other countries; and "to support smart engagement" with foreign populations in order to support the application of American influence through communication (Maybury, 2010:3, see also Costa and Boiney, 2011:3). The concepts and language are familiar from contemporary COIN and global insurgency literature, identifying global public opinion and perception as central to US strategic goals. Maybury says such a tool "needs to sense perceptions, attitudes, beliefs, and behaviors" of foreign populations (Maybury, 2010:3), describing it as a way to "see into the hearts and minds of people" (Schachtman, 2012) through exploiting open source population data (see Figure 24). As such, social radar is the quintessential Digital Age conflict intelligence paradigm – concerned with the role communication plays in driving events of strategic significance while providing intelligence to support engagement in the information environment in a dynamic way.

Whereas the interest of intelligence analysts in SNA came from the perceived networked enemies of the GWOT embedded amongst the population, the strategic imperative for social radar is more recent. The strategic shock of the Arab Spring looms large in social radar discourse, it "underline[d] the need for the United States and its allies to reliably monitor the global information environment, so that they can build sociocultural understanding, anticipate change before it happens, and plan for appropriate action" (Costa and Boiney, 2011:1). Tool developers focus on uncovering "unanticipated social

[121] MITRE has developed a number of tools under the Social Radar framework based on exploiting social media information, called *Pinocchio, Author DNA, Sentimeder, and MemeME,* and *MoodMiner* (see MITRE - *Social Radar Technologies,* 2014; MITRE – *AuthorDNA,* 2014; Flintbox – *Sentimedir,* 2014; Flintox – *MemeME,* 2014; Flintbox – *MoodMiner,* 2014; and Flintbox – *Pinnochio, 2014*)

events", and developing an understanding of "precursor indicators in open source news, blogs, and social media" (Matheiu et al, 2012:2). There is also a more operational utility in such a set of tools – they can act as "enablers of irregular warfare since they allow us to determine the networks, groups, key influencers, and audiences with whom we should engage" (Costa, 2013:2) – suggesting that "social radar" does not inhabit an altogether separate world from forms of Web 2.0 intelligence discussed in the previous section.

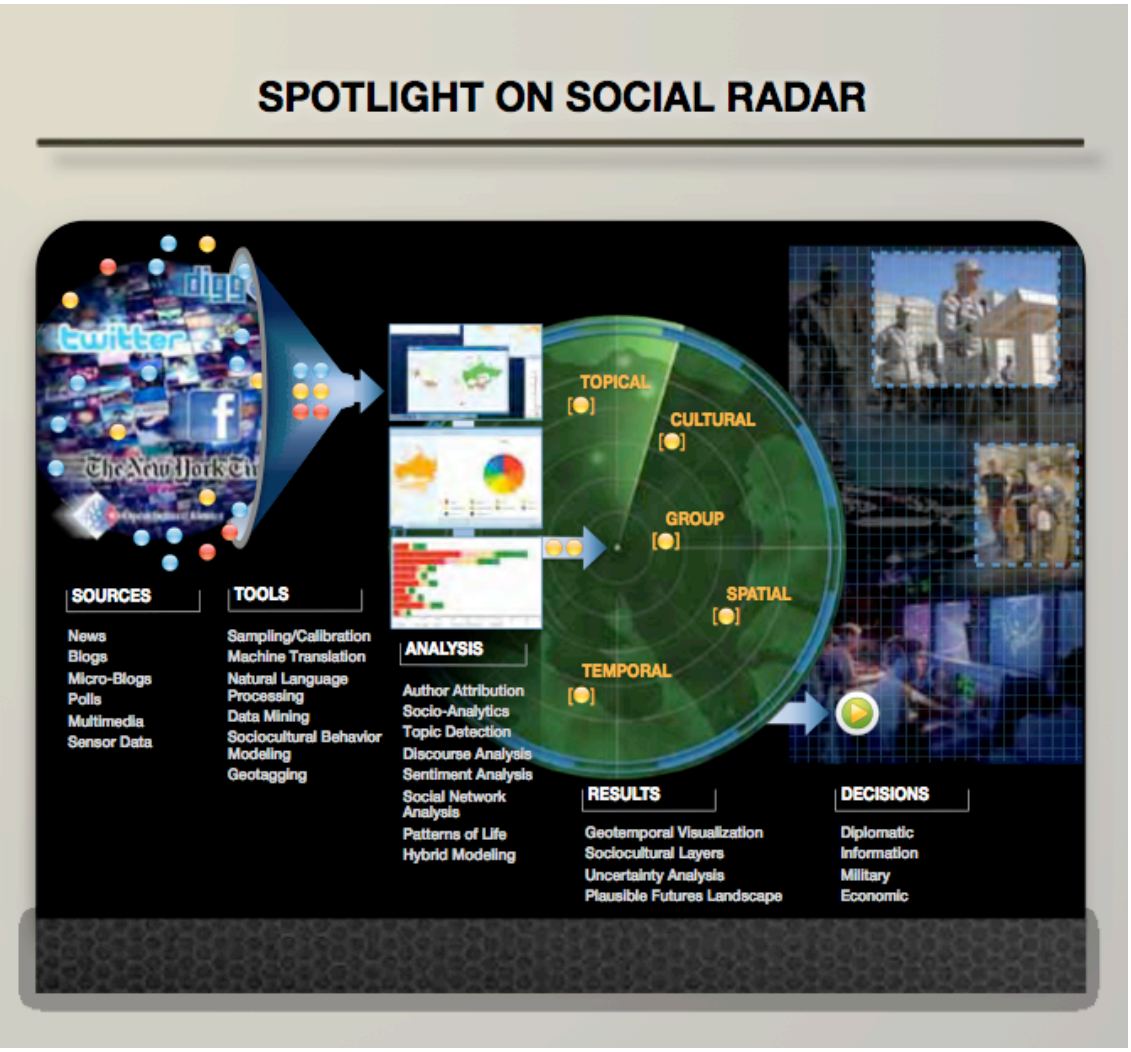


Figure 24: The Social Radar vision – from open source data to military decision making (Schmorrow, 2011b:49)

As the only viable source of real-time mass population and event data Web 2.0 is integral to the social radar concept - described in one introduction as the elements which "comprise the sociocultural behavioral landscape" (Schmorrow, 2011b:48). Social radar research is aimed specifically at the exploitation of the "multilingual, global, and real-time collected data" available "from open source – including social media" (Schmorrow, 2011b:47), and depends on "continuous access to global data on general population perceptions, attitudes, opinions, sentiments, and behaviors" through "internet-based sources, including, of course, social media" (Costa and Boiney, 2011:5). Maybury identifies "polls, and surveillance sources as well as user generated social media such as wikis, blogs, myspace, facebook, twitter, etc" as key sources, which should be "processed using a

variety of technologies and methods to support processes including media analysis, detection and tracking of signatures, and ultimately social indicator analysis", which may cover "groups or individuals to include measuring perceptions, attitudes, sentiments, and intentions" (Maybury, 2010-6-7).

The project which has been presented as the most complete instantiation of the social radar paradigm is one focussed on predicting global instability – a Lockheed Martin system called the World-Wide Integrated Crisis Early Warning System (W-ICEWS) (see MITRE, 2013:56). The system received $38m funding from DARPA before 2011 (Shachtman, 2011), and has been integrated into the US Strategic Command's "net-centric mission planning and execution system" which allows "commanders to monitor worldwide situations in real time, assess potential threats or areas of interest, and then plan and support execution of a swift response" (Lockheed Martin – ISPAN, 2014). W-ICEWS is part of a long line of DARPA and CIA-funded projects which attempt to extract "event data" (the who, what, when, where, how of an event, see Ward et al, 2013) from large amounts of text (generally international media reports) and merge it with other data such as demographic, economic and environmental trends, and apply analytic techniques in the attempt to predict instability within foreign states (see O'Brien, 2013:403; O'Brien, 2010). However, W-ICEWS is novel in that it ingests Web 2.0 data which allows it go beyond simple event data through an element called iSENT which extracts sentiment data about events from "blogs and various social media platforms" (O'Brien, 2013:408). This development is presented as a modern substitute for polling data used in previous prediction modelling efforts (O'Brien, 2013:412) – however the granularity and dynamic nature of social media means this is a significant increase in the quality and speed of modelling, which sees Web 2.0 become a key source of real-time strategic intelligence[122].

As a guiding metaphor in R&D social radar has had broad institutional impact – it has been adopted by the Assistant Secretary of Defense for Research & Engineering (the home of HSCB) as "part of its long-term vision for sociocultural behavior capability" (MITRE, 2013:56) – and, this chapter shows a number of projects across military and academia which address aspects of the problem. Indeed, in discussing the requirements of a social radar, Costa and Boiney mention a number of subjects found in the research examined in this chapter: "sentiment analysis and topic discovery", "ideology identification", "emotion analysis of social media for instability monitoring", "mapping influence via online postings", and "cluster analysis, ranking, and exploration for online postings" (Costa and Boiney, 2011:9). We can see for example: tools to extract useful information from raw online network data (OSD FY2014 RTD&E, 2013:83) or structured text corpora (MITRE, 2013:23); analytical tools to identify and explore sentiment (Poole, 2011:20), understand and track communication flows (Suen et al, 2013; Myers and Leskovec, 2012) and network influence (OSD FY2012 RTD&E, 2011:70, MITRE, 2013:29); and visualisation tools which allow analysts and decision-makers to use this data to support a range of activities (McKelvey and Menczer, 2013:2; Ware et al, 2013a).

[122] Another program focussed on predictive modelling of instability in foreign countries – IARPA's *Open Source Indicators* program – also seeks to harness contemporary Web 2.0 data flows for traditional strategic prediction, though this time focussing on predicting specific events rather than general instability (see FBO – IARPA, 2011; IARPA – *OSI Program*, 2014; Matheny, 2011:18; Seffers, 2014).

Social Radar drives an expansion of information understood to be interesting to the military – moving from event data or the "who" of small adversary networks to the sentiments, communication flows, and social and political dynamics of a potentially global population. Beyond prediction, the key military imperative supported under social radar is *engagement* in the global information environment. One of the vision's developers states in testimony to the House Armed Services committee that "it is critical to the security of the United States to understand the sentiments and actions of people throughout the world, to appropriately engage with words and deeds to positively shape the environment" (Costa, 2013:1, see also Ruston, 2012), emphasising the need to "understand *and engage* in the public dialogue created by [new web 2.0] communication media" (Costa, 2013:3). Similarly, Schmorrow identifies a key role for Social Radar tools in the "rapid recognition, tracking, *and countering* of adversarial narratives" (Schmorrow, 2011a:x), and Maybury foresees a situation in which "sophisticated adversaries will employ viral communications that both infect (rapidly distribute) and affect vulnerable populations. Countering violent and viral communications requires an ability to anticipate *and counter message*" (Maybury, 2010:7). The operational focus also shifts away from potential kinetic military activity to forms of information and communication intervention more associated with a population-centric approach – with intelligence potentially acting to identify key audiences; assess their sentiments; and guide the content and distribution of communication intended to engage them. This situates social radar at the key bridge between Web 2.0 intelligence and Web 2.0 engagement – providing key context for its discussion in the following section.

6.5. R&D in Military Communication: Facilitating Information Engagement

This section outlines R&D approaches to enhancing information engagement, moving from intelligence to communication, highlighting important new approaches and tools which enhance our understanding of CY-OPS in Web 2.0. A 2009 report by the Defense Science Board – which provides guidance on DOD R&D priorities - anticipates that increased information engagement will characterise future military operations, placing increased emphasis on the development of tools to "build trust, promote support for U.S. operations, and influence the perceptions and behaviors of many audiences" (DSB, 2009:11). As well as requirements of "ongoing data collection" (i.e. intelligence) to identify emerging issues and opportunities which will serve as essential underpinnings of new communication strategies, the increased importance of PSYOPS brings its own distinct R&D requirements, requiring "a sophisticated understanding of traditional media (print, radio, and video broadcasting), social media (e.g. wikis, blogs), collaborative media, as well as influence networks […] for understanding, tracking, and influence" (DSB, 2009:11, see also Cabayan, 2013:4; Yannakogeorgos, 2013; Schmorrow, 2011b:8).

Within both the HSCB program[123] and the SMA initiative there is interest in "how to leverage new technologies to influence and shape social behaviors through social media,

[123] Underlining the HSCB Program's social media credentials, a conference under the HSCB banner in 2011 hosted participants from Facebook, Google, and Yahoo (with a visit to Facebook's HQ for the enthusiasts) (see Lyon and Afergan, 2013:6), and a report on the conference explains how the DOD seeks

online entertainment, and other means that are now global in nature" that goes beyond simple "messaging" and based on an understanding of "how best to influence and shape the human terrain" (Canna, 2013:14, see also Canna and St Clair, 2012:4). The most significant programme here, however, is DARPA's *Social Media In Strategic Communication* – which has spent $49.2m[124] since 2011 funding academic and commercial research into "the effective use of social media to help the Armed Forces better understand the environment in which it operates and how to allow more agile use of information in support of operations" (DARPA, 2011:4). The programme funds original research, focussing on elements of online commination such as trends, meme-propagation, the identification of online personas, and the automated uncovering of online "persuasion campaigns and influence operations" (Rawnsley, 2011; DARPA, 2011).

Broadly speaking, SMISC is aimed at understanding how "blogs, social networking sites and media-sharing technology" effect the "conditions under which [U.S.] military forces conduct operations" (DARPA-SMISC, 2014). However, research goes further than this in developing understanding and techniques which also allow military actors to project their own influence in this environment. Echoing the HSCB investment in social computing, it seeks to "develop a new science of social networks built on an emerging technology base", and to develop tools "to support the efforts of human operators in counter misinformation or deception campaigns" (DARPA – SMISC, 2014). The programme's initial goals (and suggested tools) are presented in Figure 25, and include important elements in understanding communication dynamics, tools, and the process of influence in the Web 2.0 environment.

> 1. Aim: Detect, classify, measure and track the (a) formation, development and spread of ideas and concepts (memes), and (b) purposeful or deceptive messaging and misinformation.
>
> *Tools: Linguistic cues, patterns of information flow, topic trend analysis, narrative structure analysis, sentiment detection and opinion mining.*
>
> 2. Aim: Recognize persuasion campaign structures and influence operations across social media sites and communities.
>
> *Tools: Meme tracking across communities, graph analytics/probabilistic reasoning, pattern detection, cultural narratives.*
>
> 3. Aim: Identify participants and intent, and measure effects of persuasion campaigns.
>
> *Tools: Inducing identities, modeling emergent communities, trust analytics, network dynamics modeling.*
>
> 4. Aim: Counter messaging of detected adversary influence operations"
>
> *Tools: Automated content generation, bots in social media, crowd sourcing.*
>
> (DARPA, 2011:4, *5*).

Figure 25: Stated aims and tools required of DARPA's Social Media in Strategic Communication research programme.

"to use social media data in order to develop knowledge on the perceptions, attitudes, and beliefs of populations; forecast behaviors; … better understand the direct and indirect effects of potential actions; and formulate and deliver timely and culturally attuned messages" (Lyon and Afergan, 2013:6).

[124] Based on most recent budgetary material from the programme from FY2011 until FY2013 (See DARPA - *RTD&E-FY2013*, 2012)

Like many military communication practices, SMISC is presented as fundamentally defensive – to *detect* and *counter* propaganda (always used by other, less honest, actors). However, the research projects are much broader in scope and facilitate many forms of pro-active online communication activities. As the largest in-house R&D branch of the DOD, DARPA may claim ethical or non-controversial uses of the technology in its research – but the outcomes must be understood within the broader military context which it is organisationally required to serve.

Even from a purely theoretical perspective it is clear that research into how to detect "adversary influence operations" or "persuasion campaigns" produces knowledge which is helpful in avoiding the detection of one's own campaigns. Tracking the spread of "deceptive messaging" also allows the refinement of one's own communication practices. This is not to say that all DARPA-funded research projects are dishonest and secretively developing tools to assist the DOD in nefarious activity, rather that *structurally* DARPA is the tool of the military, and thus research it produces must be understood in this context. The original funding announcement gives an example of an altruistic use in which "rumors about the location of a certain individual began to spread in social media space and calls for storming the rumored location reached a fever pitch", but were by chance detected by authorities on social media, who dispelled the rumour and averted the attack before it happened (DARPA, 2011:5). In this case an attack was stopped, suggesting an altruistic aim, but in the context of conflict there are people you *want* to be attacked or places you *want* unrest to take place (as the UW examples show), what is really at issue is *control.* We also saw earlier in the chapter how population-centric intelligence facilitates a continuum of military action, that could range from the dispelling of rumours through to the 'removal from the community' of rumour-mongers.

The SMISC program was highly as a list of 132 papers sponsored by the project was published by DARPA under its "Open Catalogue" initiative in early 2014 (see DARPA, 2014b - Figure 26 shows a word cloud based on the titles these papers; Figure 27 shows a breakdown of the subjects of the papers). Research was conducted under research grants provided to IBM which were distributed to research projects in computing science departments throughout the US, Systems and Technology Research LLC, SentiMetrix[125], and Georgia Tech and Indiana universities. An analysis of these papers found that SMISC funds key projects in social media analytics – most notably the Truthy project run by the University of Indiana, one of the most popular open source tools used in social media analysis (see Ratkeiwicz et al, 2010; Silverman, 2011) – further demonstrating the importance of military R&D funding in another emerging area of academia.

[125] A company founded by key social computing figure V.S. Subrahmanian, see page 152.

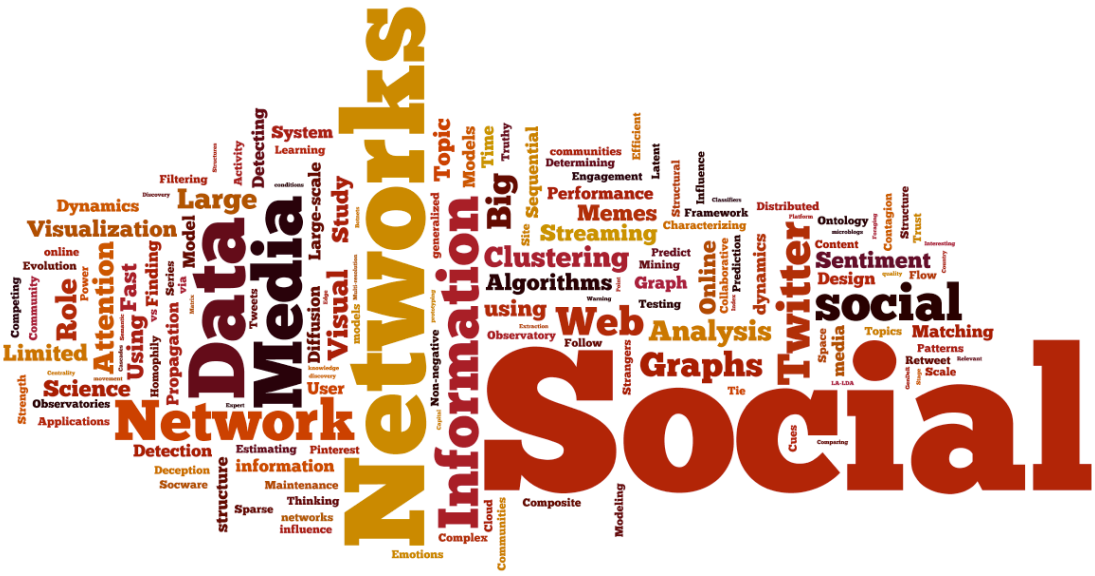


Figure 26: Word cloud produced from titles of all research projects published under the DARPA 'Open Catalog" of the SMISC project providing a visual guide to prominent themes (produced using the Wordle program).

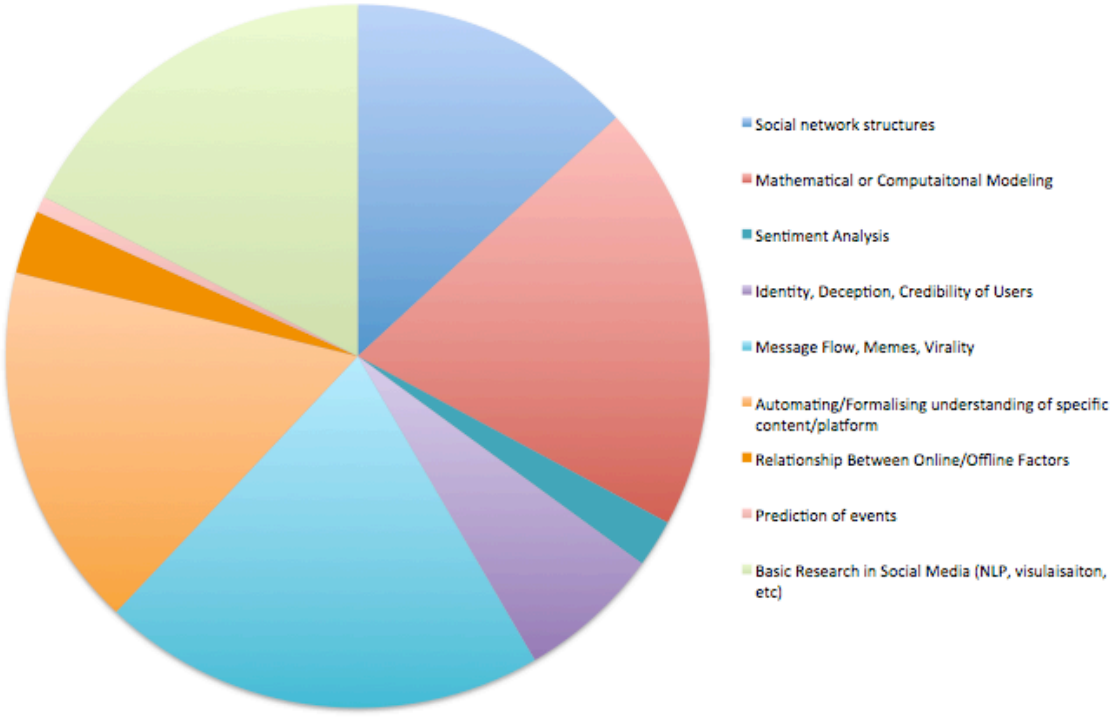


Figure 27: Breakdown of subjects of SMISC papers, based on an assessment of titles and abstracts.

The following sections assesses a number of projects funded under the HSCB, SMA, and SMISC programmes – outlining key research trends applicable (or indeed applied) to

military influence in the Web 2.0 environment. These include: projects on the development of basic understanding of Web 2.0 communication; platform-specific studies of influence; understanding features of online identity; and the study of memes and information flows as a key area of contemporary and future influence. Taken together, these subjects show the progression from foundational analysis of understanding Web 2.0 networks in a semi-automated way, through to understanding specific forms of communication and social practice online, and finally a deep engagement with understanding the key factors in the impact of communication in the Web 2.0 age – network influence, identity, and information flows. These developments demonstrate the application of cutting-edge Web 2.0 research to the problem of online communication at the cutting-edge of military theory and practice.

6.5.1. Foundational Research into Web 2.0 Social Networks and Platforms

Due to the novelty of Web 2.0 – a substantial number of DOD-sponsored projects address the foundational issues of how existing forms of measurement, assessment, or activity can be applied to the new information environment. A number of these approaches – like those in the area of intelligence – address the issue of adapting existing SNA concepts and practices to the Web 2.0 environment. These approaches seek to move beyond those based purely on relational data (such as Twitter follower networks), which have been a key element of Web 2.0 SNA (see e.g. Wheaton and Richey, 2014; Schroeder et al, 2012), to develop deeper insight relevant to processes of communication. For example, Romero *et al* (2013) examine how effectively traditional relational SNA structures map onto communities of interest (expressed through hashtags) amongst Twitter users, while another project mines Twitter data to examine how the study of communication flows (retweets and shared message content) can be integrated into the assessment of SNA linkage weightings (Weng et al, 2013). Working in a way which seeks micro-level insight within very large data sets, Zhou *et al* (2012) seek to develop the analysis of social networks identified based on semantic content rather than relational factors – basing their network analysis on use of key words and themes to locate users within active communities of interest and examine these communities. Such projects show an attempt to develop a much more dynamic analysis of online social networks, enhancing traditional forms of SNA with the capabilities of larger and richer Web 2.0 datasets.

The most advanced research in this area works from a massive dataset of "3.3 million mainstream media and blog sites" to examine how social networks cohere around particular information flows (Gomez-Rodrigues et al, 2013:1). Instead of tracking information flows through an assumed static underling network, these projects examine how information flows *create* "dynamic networks", finding that "clusters of news media sites and blogs often emerge and vanish in a matter of days for on-going news events" (Gomez-Rodriguez et al, 2013:1) [126]. This large-scale research project develops understanding of how information flows create social networks around particular news events or pieces of information – providing insight into important elements of contemporary information flows such as virality, information pathways, and the role of

[126] Two smaller-scale studies examine the similar topic of the convergence of influential bloggers on specific topics (Kumar et al, 2010; Yuce et al, 2013).

key nodes in shaping content about emerging news events (Gomez-Rodrigues et al, 2013). The development of this type of research in a military context – indeed, under a program (SMISC) explicitly aimed at enhancing military pubic communication practices – demonstrates that military research into the *process* of online communication is a key area in understanding contemporary changes, and is particularly interesting in the context of the TRWI which creates large platforms of content, and uses these platforms as the foundation of more interactive and dynamic forms of influence.

Further basic understanding of the Web 2.0 communication environment is developed in various projects which seek to examine specific features of social media activity. One examines interactivity as a feature of Twitter ("@" messages as opposed to broadcast ones) in order "to better understand online chatting behavior" as an element of enriching understanding of the weighting of links in online social networks (Macskassy, 2012b:226). Elsewhere, research examines how large social media data flows can be examined to identify key users of interest with which to communicate (Nichols et al, 2013; Chen et al, 2013). Nichols *et al* present work as part of the development of "a new class of crowd-powered information collection system" (2013:1) which identifies Twitter users who may have information relevant to a set of criteria and automatically solicits information from them. The same group of researchers also present a project which works from the opposite angle – a tool called *CrowdE* which uses an automated filtering algorithm to assist users in finding tweets the are interested in (beyond simple keyword or location searches). Both tools are presented in marketing or PR contexts, but it is clear that – sponsored by SMISC – they have more general potential in, for example, identifying witnesses to an attack or other incident of interest and engaging with them automatically. This illustrates the potential use of tools to develop more focussed and bespoke forms of military communication – basically bringing together insight into Web 2.0 communication platforms with new intelligence practices to provide a knowledge base suitable for a new generation of CY-OPS.

Other research seeks to build on the well-established field of sentiment analysis of social media, again seeking to adapt and enhance social network analysis to the Web 2.0 environment. One project examines how sentiment in the semantic content of Twitter messages is related to various elements such as retweeting behaviours, the characteristics of dialogues, and the identification of active advocates in political discourse (Smith et al, 2013). Another paper considers automated methods to track the spread of affective phenomena through blogs (Zafarani et al, 2010), while a more advanced project aims to produce tools to assess sentiment beyond the simple "positive v negative" approach to automatically assess a "manifold of human emotions" using the blogging platform LiveJournal to train machine learning algorithms (Kim et al, 2013). Another tackles the difficult problem of sentiment analysis of multimedia features (video and images) – and outlines the development of a tool based on using Flickr and YouTube to train machine learning algorithms by matching user comments or descriptions to visual cues (Borth et al, 2013a:2, see also Borth et al 2013b). While these projects – addressing the difficult issues of advanced sentiment analysis and automated image and video analysis – represent only small inputs into a much larger subject, military sponsorship of research in this area suggests that having a presence (through sponsoring research) in these advanced fields is itself seen as a benefit within military R&D structures.

The breadth of research and deep engagement with a number of social media-specific elements of the contemporary information environment - all of which aim to produce insight which would allow a user to communicate through these platforms with a deep understanding of communication processes and the particularities of online social networks - forms the basis of a comprehensive effort to adapt to the Web 2.0 world by US military communicators. While this foundational research is not evidence of the direct military use of these tools or practices – indeed most are only in the developmental phase – it does demonstrate a bottom-up approach to developing new practices to communicate strategically based on a thorough understanding of the audience and platforms in question. It also demonstrates the key role played by the DOD in funding research which forms the knowledge base in this emerging area of socio-technical research, entailing significant influence in driving research interest and strategies.

This influence is particularly interesting in relation to SMISC funding for the production tools to collect and categorise very large amounts of Web 2.0 data in what are termed "Web Observatories" (Gloria et al, 2013). A number of funded projects have included collecting real world social media data to populate these 'observatories' (see e.g. Gloria et al, 2013; McKelvey and Menczer, 2013; Tiropanis et al, 2013), mining and cataloguing Web 2.0 data "to enable the next generation of interdisciplinary Web Science research invoking mixed methods at a global scale" (Tiropanis et al, 2013:1), and providing "access to distributed repositories of data related to the use of the Web, open data, online social network data and Web archives" for the production and testing of analytic tools (Tiropanis et al, 2013:2). Such 'web observatory'-based projects funded under the DARPA scheme go from the small-scale, such as a database of Tweets by American users around a Californian referendum (Smith et al, 2013), to a huge project to archive 6.1 billion blog posts and online news articles to study online news flows (Suen et al, 2013:2) in what the researchers think is the largest dataset of its type in existence. After the programme was discussed in the press (see Quinn and Ball, 2014), DARPA released a statement clarifying that all personally identifiable information must be removed from any sponsored research projects, and that the data itself is not shared with DARPA (see DARPA – *SMISC Factsheet,* 2014) seeking to avoid implication in contemporary debates about online privacy – however the more fundamental issue of pervasive military sponsorship of such foundational projects in emerging disciplines remains.

Even foundational research based on the application of traditional SNA practices to social media is potentially controversial. While all projects dealing with social media data I examined are non-invasive, anonymised, and work entirely from open source material, they draw a wide range of social research into the military domain. For example research under the *Truthy* project (see page 177) involves the longitudinal examination of members Occupy Wall Street (see Conover et al, 2013a, 2013b)[127]. While the researchers have convincingly rejected any assertion the project aids military surveillance in any way (see Uberti, 2014), its funding by a DOD programme based on harnessing the power of the web "to help the Armed Forces better understand the environment in which it operates

[127] Another Truthy project looks at how geography influences the spread of trends on social media – using Twitter geolocation metadata to study the spread of trends through regions of the US, examining "the distribution, origins, and pathways of trends; the dynamics underlying trend production and consumption in different geographic areas; and the competition among trends to achieve global popularity" (Ferrara et al, 2013b:1).

and how to allow more agile use of information in support of operations" (DARPA, 2011:4) represents a problematic blurring of the lines between military activity and civilian research. It illustrates the depth of influence military funding can have, drawing cutting-edge social research into its own knowledge base and potentially influencing the direction future research may take. This extensive investment in research at the foundation of contemporary social media analytics underlines the subtle influence of military power on developing knowledge.

6.5.2. Dynamics of Influence

SOCOM's use of Facebook and CENTCOM's engagement on online forums demonstrated how the variety of Web 2.0 platforms can be seen as presenting opportunities for various new forms of military influence intrinsic to emerging online practices. This has led to widespread research under the SMISC and HSCB programmes building a knowledge base which addresses the dynamics of influence on different social network platforms (such as winning followers on Twitter or having others share one's content on Flickr), demonstrating an interest in building understanding about the *process* of communication in the new information environment, and thus producing the building blocks for more adaptive and engaging CY-OPS.

Studies of "the social dynamic of Digg", for example, explore how data from the social news website can be modelled in order to understand the relationship between user behaviour and the popularity of the links to news stories that they post (Hogg and Lerman, 2012), and look at how users' networks impact on the range of information they are exposed to through the site (Kang and Lerman, 2013), addressing the issue of personalised information environments in Web 2.0. Similarly, a study of another social news website, *Reddit,* examines how various features of a post impact on its popularity, seeking to understand how to "better *target* social media content: by using the right title, for the right community, at the right time" (Lakkaraju et al, 2013:1). A defining feature of the Web 2.0 information economy is the different dynamics that push stories to prominence – where elements such as viral stories or active promotion by well positioned users can rival the power of news editors and PR people in setting the news agenda. In these circumstances, it is easy to see how this type of knowledge could be useful to military communicators – their sponsorship of this research can enhance a developing CY-OPS practice grounded firmly in an understanding of Web 2.0 dynamics.

Addressing other platforms, we find a project focussing on the automated identification of opinion leaders in "contentious discussions" amongst Wikipedia editors (Jain and Hovy, 2013). Wikipedia has been a key site of struggle and controversy over the notion of objectivity in the new information environment, where government and private entities have been found engaged in unscrupulous practices in the attempt to skew online information and debate (see Watson, 2012; Corbett, 2012). DARPA's sponsorship of research in this area underlines the contentious position of open source knowledge bases in the contemporary information environment. The research itself – based on modelling the features which produce effective 'leadership' or "users who succeed in influencing the outcome of the discussions" (Jain and Hovy, 2013:6) in contentious online conversations, also lends itself to more general application in identifying leaders on other platforms (here we should note the importance of conduits in PSYOPS practice), and allowing users to

achieve leadership roles themselves based on the understanding this type of research produces (information which would be useful in programmes such as CENTCOM's RWIP).

By far the largest site of DOD-sponsored research on the dynamics of influence in Web 2.0 is Twitter. The platform is the site of research projects taking a number of different approaches. For example one paper collects data from a small number of active Twitter users over a 15 month period – examining how variables in their message content, social behaviour (i.e. replying to @ messages and retweeting), and network structures (follow-links to other users) impact on how successfully and quickly the win (or lose) followers (Hutto et al, 2013). This type of research is aimed at helping "technologists design and built tools that help users grow their audience" (Hutto et al, 2013:1) – an important element of influence in the online communication environment (see also Hogg et al, 2013). Again focussing on the relationship between the content of individual tweets and broader structural factors, Macskassy (2012a:1) presents research which examines how a profile produced based on the text of a user's tweets can be used as a predictive element in "retweeting models" – exploring the relationship between content produced and social sharing activity (see also Ver Steeg and Galstyan, 2011; 2013; Lerman et al, 2013 and Overbey et al, 2013). Much of the Twitter-based research is concerned with retweeting – the formal instantiation of virality or "social contagion" (Hodas and Lerman, 2012), which the infrastructure of the platform renders accessible to researchers. This is discussed further in relation to *memes* below.

Showing an imperative to remain contemporary in the social media scene, other projects cover emerging Web 2.0 platforms. For example a Georgia Tech project examines "what patterns of activity attract attention (audience and reposting)?" on the photo curating site *Pinterest* (Chang et al, 2014). This project collected data from over 46,000 Pinterest users and examined how their online social activity and content of their pages influenced gain and loss of followers. In the field of massively multiplayer online gaming, another project examines group dynamics and the evolution of social networks in *Second Life* (Shah and Sakhthankar, 2011). Another project examines the crowdfunding website *Kickstarter,* assessing the content of funding pitches (textual, multimedia, and design elements) and producing a model which automatically assess the chances of success of the product with "fairly high predictive accuracy" (Mitra and Gilbert, 2014:1).

In the latter project, the researchers released the key phrases and features identified as most likely to win funding as a public dataset (Mitra and Gilbert, 2014), demonstrating the need for nuance in our understanding of DOD funding of such projects. That is, they cannot be seen simply as a means for the military to directly produce and hoard information on manipulating or otherwise exerting influence over Web 2.0 communication. There is no secret plan for the militarisation of Pinterest. The publication of all SMISC papers under the "Open Catalogue" initiative (and the academic publication of many other project papers) means that this DOD research is far from secret – most of the information produced is now freely available. We must understand these developments then, in a more nuanced way, as the early investment in the production of an important knowledge base, and the pursuit of knowledge about the information environment upon which new communication strategies may be built.

6.5.3. Memes

The interest in the structure and flow of communication in the Web 2.0 environment is most comprehensively addressed in research into the phenomena of *memes.* Understood broadly as small pieces of information or ideas which spread through social networks and activity, memes are used throughout military (and broader) discussion of the contemporary information environment as a shorthand for the way information and communication travels. The amount of meme research under the programmes studied demonstrates the scale of interest in communication *flow*s of social media – a key element in communication effectively in the Web 2.0 environment and vital to information engagement.

There are a number of large meme-related projects, including those based on the examination of information on particular platforms. For example Myers and Leskovec study the *complete* set of messages posted on Twitter for a month in 2011 (more than 3 billion tweets) and study the spread of memes (in this case URLs posted by users are understood as representing memes) through networks of users (Myers and Leskovec, 2012:2). They conceptualise memes using an epidemiological ontology – of URLs being spread like infections – and examine how various memes "compete" with one another to "infect" the same network. "The goal of the model is to estimate the probability of a user being infected by one contagion, given the sequence of contagions to which the user was previously exposed" (Myers and Leskove, 2012:3, another project by Wei et al (2012) similarly assesses competing memes). They thus explore the 'battle of ideas' at the memetic level – building an understanding of the dynamics of this 'battle' and the salient features in producing success or failure.

Beyond platform-specific projects the Stanford-based *NIFTY* project develops a clustering tool to identify memes within broader flows of communication (Suen et al, 2013). The goal of this project is more expansive than any other found during the research, to "track information as it spreads across billions of documents on the Web and over time periods spanning many years", working from a dataset of 6.1 billion blog posts and news articles (Suen et al, 2013:1-3). The project operationalises the concept of the meme through identifying unique or distinct quotes, taking these to be ideas which can be tracked across media texts and time.

Another project, *Truthy*, is a highly prominent one which has received significant media attention for its development of tools (based on differing visual signatures developed by mapping how memes travelled through a network) to identify marketers or propagandists who used social media to produce "astroturf" (that is, fake grass roots) campaigns or social movements through their Twitter messages (see Ratkeiwicz et al, 2010; Silverman, 2011; Keller, 2010a). It gained funding as part of the SMSIC programme, and the research platform has been extended to study memes more broadly (McKelvey and Menczer, 2013:2). Still based on the premise that social media are "vulnerable to exploitation for spreading spam, rumors, slander, and other types of misinformation" (Ferrara et al, 2013a:548), new research extends the scope to take in Google Plus and Yahoo messages as well as Twitter. While the original Truthy project focussed on signatures from retweeting patterns of pre-defined memes such as URLs or Twitter messages (see Ratkeiwicz et al, 2010), new research focuses on identifying memes as they organically form through

"clustering" messages based on similarities in content, metadata, and network features (Ferrara et al, 2013a:548).

As such, Truthy has moved beyond its original role as tool for the analysis of specific memes, to a "system that collects Twitter data to analyze discourse in near real-time" aimed at "enabling citizens, journalists, and researchers to understand and study online social networks at multiple scales" (McKelvey and Menczer, 2013:1), and producing "sophisticated statistical tools to produce insights into the behaviour and interactivity patterns of hundreds and thousands of individual actors" (McKelvey and Menczer, 2013:2). The new tool remains open source, with large data sets available for download and analysis, again underlining the more nuanced relationship between military funding and academic research we are seeing through these programmes[128]. Indeed, if anything the sponsorship of this kind of project suggests an aversion within the military for quick-fixes based on superficial understanding or promises of transcending the complexity of online communication flows. This tool is intended to build deep understanding, but also to *expose* those who might be trying to subvert norms of transparency or legitimacy – a situation which potentially imperils less subtle forms of CY-OPS.

The only traditional end-to-end R&D programme funded under SMISC underlines this nuanced approach. Systems & Technology Research are contracted to develop "a tool to analyze and visualize memes based on social media data" (Ware et al, 2013a). This project has received $6.2m from DARPA to develop "Visual Thinking Algorithms" which seek to develop visualisations (based on geolocation, and the identification of "key players") for memes and related concepts and users (Ware et al, 2013b:1-3, see also Sandell et al, 2012). The tool under development is presented as one which will help intelligence and IO analysts in "monitoring the social media stream to become aware of properties of emerging memes" and then carry out an "exploratory analysis aimed at answering a specific set of questions [...] for example, the analyst may be interested in exploring the spread of news about a world events that has just occurred. From there, the analyst may which to identify the communities and users that originated or spread the meme, examine the meme's geographic footprint over time, or explore relative topics" (Ware et al, 2013b:2). This chapter began by examining intelligence based on online communication, then the importance of online communication itself, now it seems we come full circle to a multi-million dollar tool which seeks intelligence *about* memes – underlining the increasingly integrated nature of the two areas in the contemporary military environment.

Understand social media information flows has been identified as a key potential area of developing CY-OPS practice. However, the value of the projects examined here seems to be of the foundational type, lying in the way they allow users to understand the information environment and track ideas as they move through the Web rahter than in producing any type of manipulative tool. The military context and knowledge of SOCOM and CENTCOM projects suggests that such knowledge *can* be instrumentalised by military actors, but there is little practical advice in the research itself for these users. However, in allowing

[128] Indeed, it is interesting to note that in the preliminary stages of research for this thesis, I used the *Truthy* tool in an (unsuccessful) attempt to identify potential military-linked astroturf campaigns. At the time, information linking the project to DARPA was not in the public domain. This highlights that the development of military communication practices in the Web 2.0 environment is subtle and complex: the tool I was using in an attempt to identify nefarious "strategic communication" campaigns was in fact funded under a project on that very subject!

military users to visualise and track information flows, break the flow of communication down into discrete, analysable, and potentially manageable chunks of information, the projects offer military users useful tools in adapting communication practices to the online information environment, and it is at this more basic level that these R&D projects fit into the propaganda apparatus.

6.5.4. Communication, Narrative and Identity

While the majority of the R&D projects examined during the research are characterised by an approach to the online information environment which aids military communication through the general development of a Web 2.0 knowledge base, there were a few areas in which projects more directly addressed the question of PSYOPS. These particularly address the issues of identifying malicious communicators, narrative as an element of the content of online communication, and the relationship between communication platforms and personal persuasion. While they are outliers in the R&D programmes examined here, these examples draw on work from other influential areas, and thus represent important aspects of developing CY-OPS practice.

The identification of imposters or deceptive actors within Web 2.0 communities was named as a key area of interest in DARPA's outline of the SMISC program (see DARPA, 2011; Rawnsley, 2011), though it has been addressed infrequently in the projects which were funded. However, an HSCB-linked Navy project (conducted in-house) attempts to develop an automated process to identify – based on semantic content of a user's text – "when individuals attempt to infiltrate a group in order to alter the opinion of other group's members, or simply gain credibility from posing as a member of the group" in order to "assist intelligence analysts [in] identifying those who wish to bring harm against others" (Ellen et al, 2012:223). The authors outline their approach as a first step in developing this area of "Cognitive Information Operations" (Ellen et al, 2012:223). Flipping the CENTCOM approach of "persona management" on its head - this computational analysis of semantic content of online messages in order to ascertain norms and identify abnormal phenomena (i.e. sockpuppets) is found in a number of projects presented here and this example shows how it might be applied to military ends. Working along similar lines, another project examines linguistic "cues to deception in social media" through examining how linguistic tropes affect audiences perceptions of credibility and truthfulness (Briscoe et al, 2013), part of a project to "intelligently utilize social media data as a reliable 'sensor' for detecting and understanding human behaviour" (Briscoe et al, 2013:6) – which has been applied in relation to analysis of the Egyptian revolution (Weiss et al, 2013)[129].

One of the key buzzwords in contemporary military discussion of public communication practices is "narrative". Military-based discussion of narrative has given rise to a variety of approaches: from strategic-level explanation of military operations in public debate (Corman, 2013; Miskimmon et al, 2013), to the guidance of operational planning (Nissen, 2013) or the refinement of distinct messaging strategies (Zalman, 2010, Quinlan, 2013). The key site in the development of "narrative" thinking within the HSCB program is

[129] I also mentioned further requests for information in this area in a recent SOCOM contracting documents on page 138, suggesting it is a continuing area of development.

Arizona State University, where a group of researchers around Professor Steve Corman work on narrative from a communication studies perspective which has been influential in post-GWOT military communication thought (see Corman et al, 2008 Trethewey et al, 2009; Corman, 2013). The work is of dubious moral, academic, and practical value (Revie, 2013), however it has been well funded and influential with relevant military circles.

Arizona State work also features elements which have directly applied the narrative approach to understanding the 'battle of ideas' between the US government and insurgents or terrorists – including an HSCB-sponsored project on "Identifying and Countering Terrorist Narratives" which has produced a "database of archetypes that help spread terrorist ideology" and a "method that helps operational teams to recognize these narratives/fragments in statements of extremists groups" in order to counter them – which has been developed into a software tool in use at AFRICOM (Mitre, 2013:32). This archetype-based assessment of GWOT-based communication has given rise to a number of projects linked to Corman (see ASU News, 2013), including one called *LookingGlass* which assesses the narrative tropes of social media content and groups individuals into categories based on how extremist or "radical" they are (Kim et al, 2013). The ease with which an approach based on identifying textual tropes which supposedly reveal a certain mind-set can be applied to social media texts means that this influential but dubious paradigm for assessing the 'battle of ideas' becomes wound up in Web 2.0 communication all too easily.

This is further exemplified in the work of a colleague of Corman's on an OSD project called "Embedding Story Analysis in Expeditionary Units" (See Bernardi et al, 2012) which saw him deploy as a 'narrative consultant' with the Navy in Southeast Asia (Bernardi et al, 2012:136). Bernardi's account of working with a Navy public affairs team to craft messages in support of US humanitarian operations in Indonesia is fairly benign, he advised on how to dispel unnecessary misunderstandings and overcome cultural barriers (Bernardi, 2012:153-156). However, his conception of narrative operations and their link to Web 2.0 suggests a more controversial future. He writes that the role of an analyst like him is to locate and defuse "Narrative IEDs" – "*ad hoc* devices, constructed of bits and pieces of narrative systems and lying unseen to [the military communicator] until exploding and disrupting expensive and highly sophisticated communication campaigns" (Bernardi et al, 2012:4) – he equates these 'narrative IEDs' with user-generated content in social media which draw on existing memes, stories, jokes and information and may allow "extremists and sympathisers [to] manufacture strategic narratives online" – such that "an emphasis on the virtual dimensions of contemporary insurgencies and counterinsurgency studies is not only appropriate but even necessary" (Bernardi et al, 2013:49).

One of the more bizarre narrative projects carried out by Corman's team is on "Narrative Neurobiology", which brought together the communications studies of narrative with neurobiological experts to produce MRI scans of subjects brains to assess the reaction to different narrative tropes (see Corman-DARPA, 2011; ASU - *Past Projects*, 2013). While this project did not have any link to Web 2.0 communication – indeed it worked at a much more fundamental level – there is evidence elsewhere in the DOD research of emerging interest in the links between neuroscience, Web 2.0 and information operations. This has been the subject of a number of Strategic Multilayer Assessment studies (see Orlina and Dejardins, 2012; Canna and St Clair, 2012:54; Cabayan, 2013; Spitaletta, 2013; Spitaletta,

2014)[130]. The most advanced example of this research, by Spitaletta, discusses the potential for "neuropsychological operations" – which bring together the traditional use of social science in PSYOPS (for target audience analysis, message construction, etc) with "recent advances in neuroscience, cyberpsychology, and captology" for the production of "an advanced set of personalized persuasion tactics" (Spitaletta, 2013:73).

Spitaletta's work is a literature review and speculation about future development pitched at the senior leadership level (the Joint Staff, combatant commanders). He presents a situation in which contemporary developments in the understanding of the neuroscience of persuasion, developing knowledge in social media influence, and the ability to send targeted messages via online communication combine to produce a situation in which advanced forms of PSYOPS are possible. He argues that Web 2.0 offers a range of possibilities to refine messaging focused on adversary key leaders, such as "content analysis of an individual's social media contributions [...to provide] the opportunity to create more refined messaging", and the manipulation of the circumstances of message receipt as well as the content in order to achieve maximum effect (Spitaletta, 2013:76).

In the latter instance, Spitaletta draws on the example of 'captology' or 'persuasive technologies' (Fogg, 2002; Stanford Persuasive Tech Lab, 2014) to argue for the potential of "designing technologies with the explicit intent to change behaviour", particularly online technologies and platforms, in which influence practice takes into account not just messages and conduits, but the process of delivery and interaction with programs and devices (Spitaletta, 2013:76). While this process isn't as ground-breaking as it sounds, and Fogg certainly didn't invent the notion that the design of tools have an impact on peoples reaction to them, a military interest in technology with "user-derived preferences to change opinions, objective reasoning, and ultimately behaviour through this confluence of human-centered design and social influence" (Spitaletta, 2013:76) should certainly draw our attention to the potential of this area of military influence in assessing future developments. Spitaletta also writes of the advanced possibilities for new forms of CY-OPS in relation to the rise of the *Internet of Things* (see Atzori et al, 2010) and constant mobile device monitoring – "this kind of device tracking and monitoring has the potential to reveal motives and patterns of thinking or behaviour" (Spitaletta, 2014:75), making it a key element of target audience analysis. The web allows an enhanced form of target audience analysis which is necessary as "in order to craft effective messages, one has to identify what a person is willing to believe. Therefore, one cannot start by crafting a message; one must incrementally prepare a person or an environment to make the communicated message credible" (Spitaletta, 2014:87).

This form of "personalized persuasion tactics" (Spitaletta, 2013:87) in which vulnerabilities can be "exploited through both the message content as well as the dissemination mechanism" (Spitaletta, 2014:90) seem quite *out there* in relation to most of all the other R&D this chapter has discussed. However, when we understand such PSYOPS practices as based on paying as much attention to the context of communication and its content, and supported by intelligence about audiences, we can see echoes of this in much of the more basic research in this chapter. Furthermore, when we consider the example of the Southeast European Times Facebook page (page 117) - in which an audience was built using the interactive facilities of Facebook, polled regularly to aid

[130] See also Wurzman and Giordano (2014) on *NEURINT* and *neuroweapons*.

understanding by PSYOPS practitioners, incentivised to share content and accept forms of interaction that would embed PSYOPS products into their own news feeds – the application of such advanced forms of CY-OPS practice does not seem quite such an outlier. Indeed, both the use of narrative and enhanced understanding of the *form* of a communication act are deeply embedded in military communication thought, and recognised and supported by many of the more basic research presented earlier in this chapter.

6.5.6. Summary

This tour of the various forms of Web 2.0 influence-focussed R&D projects at the DOD has presented a variety of approaches which address the information environment at different levels, and the issue of influence with varying directness. While the latter examples are those which we might most readily identify with PSYOPS practice, they are outliers, significant but not typical. The much larger projects presented earlier in the chapter which deal with the development of basic knowledge of Web 2.0 interaction, the specifics of influence on particular platforms, and the flow of information through memes, are much more typical and prevalent. They have the key output of *enhanced understanding* of the information environment rather than any particular techniques or tools of engagement with it. Indeed, in the case of the deception-detection tools discussed in the previous section, it seems the project seeks to develop tools which could compromise existing CENTCOM CY-OPS efforts by unmasking sockpuppets. How to understand these developments then, as part of a propaganda apparatus?

Rather than seeing these communication-focussed projects as developing tools or practices for influence, they must be understood in relation to the challenges of the Web 2.0 problem field: characterised by 'flows' of information making military communication difficult, the difficulty of predicting or even *understanding* the drivers of news stories or public debate, and a recognition of the enhanced importance of the proliferation of platforms of communication of potential strategic or operational significance. In this context, rather than *tools* for influence we can see the development of a *platform* for it – of techniques and processes for understanding the information environment, for tracking conversations of relevance, and understanding the impact of military communications. This is the key outcome of "information engagement" in military R&D – the military already has legions of spokesmen, access to the information environment, and a central position in discourse about conflict – what it requires is an understanding of the environment, the foundation of any successful engagement.

6.6. Conclusion: Intelligence, Knowledge, and the Propaganda Apparatus

The description of contemporary US military R&D addressing the problem field of Digital Age conflict in this chapter is based on an analysis of the extensive documentary material produced by a number of major programmes. It covers military activity at a number of sites, from special operations-linked educational establishments to university research. The presentation of this data – following as it does from an analysis of the theoretical and

practical developments in the field of special operations – allows a look at both the intellectual platform supporting these military developments, and insight into potential future areas of activity in the field of Digital Age conflict. It presents an opportunity to build an understanding of less-direct elements of the propaganda apparatus, as well as to discuss the role of knowledge in the field of Web 2.0 in that apparatus.

In terms of understanding the links between knowledge and power in the research situation there are two important areas this chapter highlights: the links between the DOD and the broader knowledge economy of academia; and the role of knowledge as an instrumental element in the propaganda apparatus. In the first area, in section 6.3 and throughout the chapter I drew attention to the deep links between military research programmes and academic research, though analysis of this area requires that our understanding of the links between knowledge and state communication power is nuanced. The R&D projects in question do not generally act as extensions of military power in a linear sense, they are not producing knowledge to be directly and exclusively instrumentalised by military practitioners. Almost all the research projects discussed are based in academia, and lead to the production of research papers and technical reports which are open source, in many cases even producing open source datasets or analytic tools which anyone can use. Yet all are funded under programmes which explicitly seek to build military capability to meet the challenges of Digital Age conflict.

So how do we understand this instrumentality? Firstly, the relationship between the DOD and academia should be understood as the result of the particularities of the age of Web 2.0 itself. I argued in the methodology that the DOD during the research period was an "institution in flux", producing a radical openness in regards to the current intelligence and communication challenges it faces in the age of Web 2.0. The way the problem space is understood is one in which the openness of the information environment and the pace of development of new technologies and forms of sociality are a challenge to existing military practices. This challenge extends to R&D practice. Web 2.0 research is inhospitable to the traditional closed approach. Experts in Web 2.0 are generally young, used to an open research culture where funding is relatively freely available, and developing their expertise in an environment where the military and intelligence organisations are often viewed with suspicion (see e.g. Kopstein, 2014). Furthermore, much of their work, based on large datasets and advanced analytic practices requires openness and collaboration in order to be effective (this is evident, for example, in the large numbers of organisations involved in Web Observatory projects). It seems the DOD has seen the writing on the wall here, and pursued a relative openness in their R&D approach in order to gain a stake in cutting-edge research in the area.

The obvious follow-up is: why doesn't the DOD just keep up to date with this research like everyone else and incorporate what is useful to them without spending all this money? Firstly, the DOD is not the only organisation interested in advanced social media analytics – it is at the foundation of a whole economy which includes online advertising, news, market research, and e-commerce in which much research is proprietary. Many government and military organisations are customers of commercial data mining and analytic companies (e.g. see McGarry, 2013; CCTSO, 2013:16; HootSuite, 2013) yet the DOD has shown a preference for bespoke in-house development and wariness of over-

reliance on the commercial sector (see Lubold and Harris, 2014), or at least a willingness to keep their options open.

Furthermore, the funding of open source research does not mean there is no control over the product of that research. I outlined the key links between DOD research funding and the emerging discipline of social computing – with military figures controlling funding, suggesting conference and research themes, making statements regarding the type of work the DOD will fund, and playing a continuing role in organising, curating, and disseminating research in the area. 6 years after the first social computing conference the military links to the discipline show no sign of waning, and a number of researchers who received military funding in the early days of social computing have emerged as key figures in the field. Here we can see the subtle links between military funding and developing fields of knowledge – which have been demonstrated in relation to other disciplines throughout the last century (Simpson, 1998; Solovey, 2001; Pickering, 1995; Robin, 2001).

As well as allowing an avenue for military influence over the development of a new discipline and construction of a knowledge base useful for military activity, we can look at the example of CASOS to see further instrumental utility. The development of the ORA tool and various military-funded SNA projects has led to an abundance of research linked to CASOS which has pushed the cutting-edge of network analysis in a manner deeply marked by military and security priorities (see Carley, 2014; CASOS – *Networks and Terrorism,* 2014). It has also led to a number of direct applications of ORA to military problems, collaborations between academics and military practitioners (including direct application during the Afghan war), and has given the military a vocal advocate of SNA-based approaches to counter-terrorism and other areas of contemporary conflict. Thus, though there is not a direct relationship between open source research funded by the DOD and specific military utility, it can be seen as building a practitioner network of potential great value to military R&D, an element which the HSCB and SMA programmes have been keen to nurture and promote in their regular newsletters and conferences.

This addresses the implications of one link between knowledge and power in the propaganda apparatus – but it must also be addressed regarding the utility of the R&D output itself to the apparatus. In the examples of intelligence practice discussed in section 6.4 – the role of knowledge as an instrumental element in emerging military approaches is clear. In the development of Web 2.0 intelligence practices I described tools (Lighthouse, DTNA, ORA, TweetTracker) which allow the collection and analysis of large amounts of data relevant to contemporary approaches to the GWOT: understanding social networks, cultural dynamics, and the spread of information online. These tools are of great potential utility to COIN and UW practices in any Web 2.0-saturated operating environment. Furthermore, under the emerging paradigm of "social radar", these tools can be seen as responding to the strategic urgencies identified as 'phase 0' conflict and under the 'indirect approach'.

However, when we examine these developments along with the more communication-focussed projects of SMISC, we see their utility not only as intelligence tools, but as part of a propaganda apparatus. That is, the population-centric intelligence which they produce is a vital element in target audience analysis and understanding the potential communicative environment in which any military communication must take place. In the context of

"information engagement", communication activities such as PSYOPS are based fundamentally on understanding the information environment, information flows, the audience one is communicating with, and potential outcomes of a communicative act. In such circumstances, the communicative act itself is a vital but relatively minor element – being the outcome of long process of intelligence and assessment. Thus in the SMISC programme we see much more research on understanding the nature of influence on particular platforms, monitoring social networks, the flows of communication represented by memes, than we do relating to the act of communication itself. This is not only foundational research into Web 2.0 in that it is premised on understanding the basics of communication, but also in the sense that understanding these elements *forms the foundation of any CY-OPS engagement* and is thus a key element of the Digital Age propaganda apparatus.

7. Conclusion: Understanding a Military Propaganda Apparatus and the Digital Age

The scope of R&D in the areas of intelligence and communication which address Web 2.0 and the range of emerging CY-OPS practices which seek to engage with publics online, demonstrate the importance of examining the military response to Digital Age conflict. Taken together, the range of intelligence practices and paradigms, CY-OPS activities, and strategic developments which incorporate communicative and social elements as a key area of GWOT-era conflict are best understood as forming a *propaganda apparatus* which address the Web 2.0 information environment. In the theoretical introduction to this thesis I described such an apparatus as forming the *problem field* of Digital Age conflict and approaching that field in a way deeply influenced by powerful actors' conception of it *as a problem.* The developments in military discourse, intelligence, communication, and R&D described here demonstrate this thoroughly – showing a coherence from new strategic approaches and paradigms to particular tools and practices – all of which are articulated in a thoroughly Digital Age register. The outcome of this insight is that we must move beyond thinking about military activity as menaced by Web 2.0 or inhibited by new ICTs. Rather, we must understand the US military to be dynamically adapting to the challenges and *the opportunities* presented by Web 2.0.

Understanding of this process is best served by an analysis of the propaganda apparatus as the collection of technologies, practices, paradigms, and processes through which the DOD adapts to address Digital Age conflict. In doing so the apparatus model moves beyond traditional understandings of military communication which study specific practices or communicative acts. Instead, it acknowledges that such discrete elements are simply one point in a long and complex process of engagement with the information environment to achieve specific goals. Thus the analysis has incorporated an understanding of the strategic, organisational, and discursive underpinnings of contemporary PSYOPS practice; an investigation of the range of ways intelligence and military information engage, such that intelligence practices have adapted to support the propaganda apparatus; an understanding of the technological, practical and epistemic requirements and examination of developing approaches in the field; and the study of the range of CY-OPS practices in SOCOM and CENTCOM with particular focus on *how* they function *within* the propaganda apparatus. This holistic analysis has been demonstrated to be key in understanding contemporary developments. For example: the value of the TRWI cannot be understood without the importance of cultivating relationships and audiences made explicit in other programmes; and the range of R&D developments require an understanding of contemporary military intelligence thought and the emerging paradigm of 'information engagement' for their significance to be grasped.

This holistic approach to the subject allows methodological as well as theoretical innovation. The success of the prolonged, in-depth, and all-source approach to the examination of this area demonstrates the possibility of social scientific analysis of the complex and difficult-to-access area of military and intelligence activity. Rather than accept the restrictions of access to relevant individuals and data, this thesis demonstrates that the concerted collection, cataloging and analysis of open source information can yield significant insight into forms of activity usually considered too secretive or inaccessible to base a research strategy on. In focusing on military discourse and documentary material

primarily as an insight into military *activity,* the thesis also demonstrates an approach to contemporary military development in which the analytic perspective shifts from what military actors *say* to what they actually do. In both respects, the research undoubtedly benefited from being conducted a time of relative openness in certain areas of military development, and from the length of time the doctoral research format allows. Both of these elements allowed an immersion in the subject which is hospitable to methodological innovation – though this example and the insights it has produced suggest a way forward for critical research of developing military activity, and of propaganda apparatuses in other fields.

What does this understanding of the propaganda apparatus mean, then, for the study of state communication power in the Digital Age? Most importantly, it means an expansion of the areas which it is necessary to study in order to understand the phenomenon. This includes a holistic examination of: the relationship between intelligence and communication practices; the importance of the non-semantic elements of communication such as flow of messages, platform-specificity, and the means of delivery; and understanding of attribution which moves beyond the binary categorisation of propaganda to understand the role online norms of sharing, reproducing and remixing play in message distribution; and, an expansion of the presumed role of propaganda, away from a focus on the direct influence of specific linear messages towards one which incorporates the instrumental construction of audiences.

The analysis presented here suggests that in Digital Age conflict, state communication power is not simply a matter of communicative action; but of integration into social networks, long-term influence over populations, and the construction of relations with both populations and knowledge which can be instrumentalised in a variety of ways depending on strategic or operational imperatives. As well as providing the basis for a research framework capable of coherently examining this complex situation, the Foucauldian concept of governmentality provides key analytical touchstones for this thesis – with the concepts of knowledge, population, and space facilitating discussion of the implications of various findings throughout the work. In this respect the thesis demonstrates the continuing value of the concept of governmentality, and suggests that its application to the analytical challenges of the GWOT provides an avenue for its continued importance.

At the basic level, an understanding of contemporary state communication power needs to take account of how information 'coming in' (in the military context, intelligence) is used by communication practitioners. In the propaganda apparatus we have seen that the needs of communicators have, to a significant extent, shaped an emerging paradigm of intelligence, making not just individual pieces of intelligence instrumental to the communication process (that is, knowledge about particular events or groups), but effectively instrumentalising the entire *process* of intelligence, which becomes the foundation of the propaganda apparatus. This feature is clear in the extent of Web 2.0-relevant military activity examined which deals with intelligence. The research found developments in Web 2.0 social media analysis which are aimed at supporting the range of military engagement, from tracing the source of information about key events to identifying key individuals in both the information and physical environments, to more

general strategic interests based on large-scale sentiment analysis or event-monitoring (under the social radar paradigm).

In studying developments in GWOT intelligence, I emphasised the influence of Michael Flynn who argued that, in special operations practice, intelligence and operations were becoming increasingly indistinguishable. The research found consistent support for and evidence of the repurposing of military intelligence practice to support PSYOPS activity – moving from the traditional focus on examining enemy materiel, supply lines, capabilities, and potential vulnerabilities, to incorporate the population-centric concerns relevant to winning hearts and minds in the operating environment. In Afghanistan Flynn told his intelligence officers to provide information on local culture, tribal allegiances, the state of local government, and important narratives. He compared this type of approach to a political campaign, and while it unquestionably sounds like a softer and less offensive approach to intelligence than his "Death Star" days – there are important implications for the extension of military thought, surveillance, and activity into the political and social realms.

Furthermore, in the example of social radar, we can see the development of a paradigm concerned with the monitoring and exploitation of the vast amounts of data about populations available online to both provide strategic indicators relating to instability or unrest, as well as to support strategic-level communication programmes. This is the population-centric approach to intelligence activity directly applied in response to the perceived challenges events such as the Arab Spring present to US military and foreign policy. In this case, the Web 2.0 information environment and military intelligence and communication practices become deeply intertwined. Indeed, it is impossible to conceive of a paradigm such as social radar *without* Web 2.0 data – there is simply no other source which could meet its requirements in terms of the volume and timeliness of information. This demonstrates military strategy not simply challenged by Web 2.0 – but *made possible* by it.

Much attention was given in outlining the problem field to the non-semantic elements of communication – the 'unruliness' of information flows, the contingency of what is known about an event, and the twin menaces of emergence and convergence. In this area we can see new forms of knowledge being developed which engage with Web 2.0 communication flows to enhance military practice, allowing the propaganda apparatus to operate with a deep understanding of the flows and dynamics of information and communication online. While McNair talks of a "chaotic" information environment in which control of information and interpretation of messages is impossible to predict (page 31), we can see military thinkers discussing modern messaging such as Facebook posts as only the first input in a communication act – and the need to follow the message 'out there' into the information environment to shepherd interpretation (Cunningham, 2010:16).

Chapter 6 highlighted R&D work which produces knowledge to support such strategies – with significant research into understanding memes and virality, dynamics of influence on various social media platforms, and advanced forms of target audience analysis such as sentiment analysis and tracking key conduits and influencers. The range of CY-OPS practices within CENTCOM demonstrates the capability to engage with audiences at all levels to have an effect on interpretation and thus provide some form of control over information. The Web 2.0 information environment is certainly less predictable and more

difficult to influence than the media of old – but this does not mean powerful actors have given up trying. The analysis here suggests there are new forms of influence and control which increase the potential scope of military activity. Here the concept of CY-OPS offers an important area of future analysis: providing a way of thinking about influence in the online world which moves beyond the analysis of rhetoric or persuasion, to take into account the instrumentality of surveillance, communication flows, memes, conduits, online communication norms and protocols in our understanding of psychological operations in the Digital Age.

Chapter 5 demonstrated the PSYOPS and Public Affairs programmes based in CENTCOM through which a permanent staff of web commenters engage in both overt and covert manner on news websites' comment sections, blogs, social media, and online discussion forums to discuss news events relevant to US operations. Between the attributed public affairs commentators and the clandestine ones using 'persona management' software to mask their identity the DOD has the full range of engagement options – with effective communication being supported by whichever form of attribution is most appropriate. Here the increased scope of state communication power is clear. Traditional ways of thinking about military influence such as the examination of military-produced or influenced content or specific practices would suggest that the proliferation of information recording devices and media platforms over which the military has no influence negates their power – but in insinuating CY-OPS communicators within networks and platforms unusually considered social or secondary to mainstream media activity, we can see a potential influence at a much more granular, targeted level.

Much online discussion about current events is centred around specific media – with news stories or blog posts acting as a catalyst for sharing content, discussion and debate. In this case, the exampled the Trans Regional Web Initiative is particularly interesting, and allows us to make sense of it as an instrumental PSYOPS tool within the contemporary propaganda apparatus. The majority of the content of the TRWI websites is innocuous – including football scores, human interest pieces, and re-posting of wire service reports - and cannot be seen as consistently supporting US interests in a manner 'old media' studies of propaganda would recognise. Rather, the news sites can be seen as providing content to catalyse online debate in a context in which PSYOPS practitioners have a privileged position: as publishers of original content, moderators of the comment sections of those websites, and as platforms for using social media such as Facebook to nurture audiences and discussions, with demonstrable PSYOPS utility. This was particularly the case with the successful SETimes Facebook page, which has been held up as an example of best practice in the PSYOPS community, and was co-developed by one of the key figures writing on developing PSYOPS practice in the field of unconventional warfare. This also entails communication approaches that are not so directly instrumental as the 'messaging' and persuasion campaigns associated with military propaganda – the innocuous content on TRWI websites can best be understood as building trust, credibility, and an audience for these platforms. This has been clearly stated as the purpose by practitioners in the area, and in the case of sites with large audiences in certain regions the accumulated and maintained audiences represent a *latent* PSYOPS power, which is maintained and groomed, and can be leveraged when more directly instrumental messaging is deemed necessary.

It is clear from early in the discussion of the problem field that the conception of military communication practices as linear, distinct from other military activity, and a matter of working through the mainstream media are inadequate to understanding the new information environment. Communication is not a matter of 'messaging' or broadcasting – but of a deep *engagement* with audiences based on an understanding of them and a broad understanding of the social, political, and military context of communication. The emerging "information engagement" paradigm of PSYOPS – in taking in the importance of intelligence, non-semantic elements of communication, knowledge of particular platforms, and an understanding of the *limits* as well as the *possibilities* of the information environment – is important in examining CY-OPS practice. It also entails an understanding of the impact of specific communicative acts on the part of the communicator, for example: a key element of the SETimes Facebook page was the analysis and polling of the Facebook audience; and an analysis of the RWIP shows that PSYOPS activity is consistently monitored for its impact on the tone of discussion and sentiment expressed on forums of interest. Thus we can see the research practices which might be used to examine military propaganda practices (sentiment analysis, polling, etc.) are actually *integral* to those practices, they are a key part of the measured and concerted activity of the propaganda apparatus.

A further important role of the TRWI websites lies in their incorporation of military influence into the space of Web 2.0 - allowing PSYOPS-produced content to circulate within regional and global news ecologies. Here we saw an element of the propaganda apparatus which exploits the interconnection and norms of online news (the use of hyperlinks, the reposting of content on blogs and other news sites) to insinuate DOD content within civilian communication flows – even in the case of one newspaper as the consistent and long-term reproduction of PSYOPS content masked as impartial regional news. I also showed how the imbrication of PSYOPS content into these global flows of news have the effect of boosting the legitimacy of the TRWI sites themselves, especially as they are seldom referred to as DOD platforms, drawing on Web 2.0 flows to further 'cloak' their provenance. Without viewing these developments within the context of a propaganda apparatus there would be a contradiction here between stating that the content is mainly innocuous and also that it insinuates PSYOPS influence throughout online news media. However when it is understood in terms of building legitimacy, an audience, and popularity for platforms which are instrumentalised in time of need, this simply enhances our understanding of information engagement, and demonstrates a developing form of state communication power which is attuned to the value, possibilities, and risks of Web 2.0 communication.

In outlining the problem field of Digital Age conflict I have emphasised the dual-nature of the challenge of Web 2.0 *and* the changing military environment of the GWOT. In this context the role of military special operations has been demonstrated to be particularly important due to its importance at the 'sharp end' of military activity (kill or capture raids, drone strikes, etc.) and the growing strategic role as coordinating the GWOT through the 'indirect approach'. This two-levelled approach of broad influence with discrete, more-risky activities below the radar, is mirrored in the developing propaganda apparatus. As a corollary to the strategic element, we can see in the concept of social radar the rise of a global strategic military intelligence capability to monitor global stability; and in the TRWI websites a structure to generally pursue and coordinate PSYOPS activities which act as a

platform for other engagement. Under the radar, we can see activities of the MIS teams in US embassies and the clandestine online engagement programmes as the more direct and precise use of communication to push certain information or pursue more directly instrumental communication strategies. In this we have a propaganda apparatus which must be understood not as coerced into being by the challenges faced by the military, but coherent with emerging military strategy and well positioned to exploit the opportunities presented by new ICTs.

We can see further correlations between the challenges of Web 2.0 and the contemporary military situation. In relation to the contemporary population-centric imperative, in creating an information environment in which the control over what is recorded, broadcast, and spread widely diminishes – Web 2.0 in a sense *necessarily* drives communication and policy together in that thinking about an event and its representation as separate parts of elite practice becomes increasingly untenable. This serves to draw our attention to the importance of attending to the conception of a *population* in particular strategies of communication power. I have drawn attention to the implications of particular practices in addressing populations in specific ways: from the dangers of MIS teams using conduits in dangerous environments, to the sliding scale of population-centric and enemy-centric approaches to SNA-based operations (section 4.4 and 6.4.1), and the *global* conception of a population under the social radar paradigm. In each case, how populations are conceived within that approach has important effects on how individuals come to be addressed by military power, even entailing potentially lethal outcomes in some circumstances.

In traditional studies of state communication power the impact upon populations is generally understood in terms of cognitive or behavioural impact: do the lies of the state make it into the newspaper, do people believe them? Such approaches range from sophisticated analyses based on a deep understanding of how people reason about media content (e.g. Philo and Berry, 2004), to those that infer the impact of communication power from political developments (e.g. Patrick and Thrall, 2007). However, what the analysis of Digital Age propaganda apparatus suggests is that in a situation where information and communication saturate everyday life there is a much deeper range of potential outcomes: does being deemed part of the 'population' referent of a *population-centric* approach mean that your information environment (from regional news websites through to your Facebook page) becomes the site of significant military interference? If you are an avid Facebook user in most Balkan states, you are more than likely regularly exposed to American PSYOPS products through an SETimes Facebook campaign, according to the practitioners own analysis. In Turkey, the online news ecology is one in which one of the most active Facebook pages for a news organisation is run by SOCOM. An increasing focus on information flows and the way networks cohere around particular flows or stories means, furthermore, that populations need not necessarily be geographically defined, but are those interested in and commenting on particular issues. This is an element which, when we consider the range of potential forms of intervention the propaganda apparatus facilitates and the globally-conceived nature of its strategic mandate, is a key area of consideration. In a sense, we can see a deterritorialisation of propaganda, even a breakdown of the domestic/warzone distinction based not on geography but on proximity to a certain discourse – the logical conclusion of a globally-conceived battle of ideas.

At the sharper end of the propaganda apparatus: does being involved the network of certain political or social movements which might be of interest to the US military (either as a potential ally or adversary) mean your information environment is targeted by more direct forms of special operations PSYOPS infiltration, from cyber personas to the use of conduits? Or further, does the intelligence necessary to support such an engagement strategy crossover into supporting potential violent activities against your network, identified based on communication alone? If this latter example seems to stretch credulity we need only look to East Africa, where there is an active SOCOM PSYOPS website in Somalia and Kenya (*Sabahi*), where special operations MIS teams may be operating to influence the civilian population, while their colleagues wage a low intensity war across the Somali border, where the US- and UK-funded Kenyan police have been accused of running death squads against alleged domestic extremists (Jepson, 2014), and where a US-based Somali journalist was identified as running an "extremist" website by SOCOM contractors and reported to the FBI (see Whitlock, 2013). While analysts have been busy covering what Al Shabaab have been up to on Twitter (see ICSR, 2012; Prucha and Fisher, 2013; Alonso, 2012), a potentially dangerous militarisation of public communication in the area is underway without publicity or scrutiny.

This draws our attention to the effects of the propaganda apparatus on the information environment as a *space.* In traditional thinking about state communication power we can imagine a line between military space at one end and social space at the other. At one end, from a communication point of view, what happens in the conflict is military space – they control the images, access of journalists, and can shape events to fit the narrative. The media, in the middle, is contested by military and other actors who attempt to influence it. At the other end is social space, where the military message, filtered through the contested space of the media, is understood and debated in social context amongst social networks, and interpreted by individuals in various ways based on their own experience or beliefs[133]. What we see in Digital Age conflict is the division between military and social space broken down – this has been addressed at the 'military end' in the literature, where a proliferation of 'information doers' has broken the military monopoly on conflict imagery and information. It has also been addressed (though less comprehensively) in the contested middle ground, where forms of influence aimed at the 'mainstream media' wain in the time of Web 2.0 – this space was always contested though, and now the contest is more complicated. What this thesis has identified is that this contest now proliferates into the *social space* into which the propaganda apparatus or mass forms of military influence did not previously reach. The assumed social space of social media must be understood as one in which military communication continue to promote their agenda, influence interpretation, and attempt to shape the bespoke information environments that we create for ourselves through Web 2.0.

This blurring of social and military space can also be seen in the implications of Digital Age military strategy. Horn has written that intelligence is "a kind of knowledge characterized above all by its innate linkage to power and war. Whoever becomes the object of this knowledge is the enemy, by definition" (Horn, 2003:4). In a situation where intelligence

[133] Note: this is not to say that state power has no bearing on this space – more long-term effects of what have variously been studied as hegemony, ideology, received understanding, and here "state communication power" of course influence interpretation.

practices grow to cover entire operating environments, sometimes conceived globally, does this mean we are all "the enemy"? This perhaps overstates the case somewhat, though the underlying truth of the relationship between intelligence and power, and the way it brings its subjects into military consideration is an important one. I discussed the outcomes of SNA-based approaches, from the population-centric which focus on communication programmes or socio-political initiatives, to the enemy-centric which incorporates the targeting of particular individuals. I noted a tendency in developing intelligence practices for these two forms to converge, a phenomenon which has potentially serious consequences for populations which are the subject of these practices.

We can see, for example, how population-centric intelligence practices which surveille social networks with an interest in the sentiments and flows of opinion on a subject of military interest (say, protests against US presence in Benghazi, see Carley et al, 2013 see page 162), when they incorporate potential tools discussed in this chapter which help track message flows and key nodes, could quickly identify potential agitators or influential leaders within a group. In this case, the PSYOPS approach would perhaps advocate steps be taken to undermine the credibility of these individuals or counter the messages they are sending. However, we can also see that within certain paradigms of military thought, in agitating against the US such individuals can be seen as a strategic threat – and, drawing on wider special operations experience, perhaps may be more directly dealt with through violent military action. This would, of course, be a serious escalation of propaganda activity, yet there is precedent in the assassination of the AQAP propagandist Anwar al-Awlaki (Scahill, 2013:398).

This is not to suggest that military communication programmes are being replaced by assassination programmes, but that the incorporation of sentiment, cultural and social factors into intelligence practices, which in turn support PSYOPS practices, place large populations within *a continuum* of potential military activity from the communicative to the violent. Indeed, contemporary information operations doctrine discussed in section 4.5 recognises this continuum from the opposite side – that every military action has a communicative corollary. We can flip this and recognise that being part of a civilian population whose opinions, emotions, and actions are the subject of military intelligence practice embedded in a special operations-approach to conflict entails that communicative relationships also have a military corollary. Even, as we noted in relation to social radar, where the main focus of military interest is the impact on the *information environment,* being included in a military approach which is underwritten by the application of violence makes the Web 2.0 information environment a potentially hostile one.

This continuum of communication and violence will, of course, some as no surprise to those on either side of American counterinsurgency operations over the last decade. Within military thought, there has been recognition at all levels of a breakdown in distinction between war and social life. From Arquilla and Ronfeld's concept of "social netwar" (1997) and the COIN manual's soldiers as "armed social workers" (US Army/Marine Corps – *FM 3-24:*A-7) to the militarisation of anthropology and the calls for intelligence to be repurposed to run military campaigns like political ones (Flynn et al, 2010:11). Owens describes COIN as the "integration of military strategy with political and economic engineering, a self-conscious attempt to rewrite the perceived boundaries between war, politics, economy and anthropology" (Owens, 2012:2). These elements can

be situated within broader analyses of the development of war in relation global political and social life. Martin Shaw has identified a 'new Western way of war' (Shaw, 2005) – a conception which coheres with the implications of COIN, 'the battle of ideas', and communication in conflict more generally. Shaw examines broad trends in conflict and outlines a general shift from an understanding of conflict as 'total warfare' (a whole of society effort, often of existential consequence), to the contemporary situation which he characterises as one of 'global warfare': based on *indirect* mobilization of populations, limited in scope by political, economic and cultural considerations, involving advanced public opinion-control and media management, and a proliferation of non-state actors in conflict (Shaw, 2005). In this context Shaw points to the "different general relationship between warfighting and the political, economic and cultural-ideological domains" (Shaw, 2005:56). In the shift from total war, that is, conflict becomes more integrated with other aspects of social and political life.

Global warfare is generally waged at a lower intensity than total war. Instead of having primacy, war "must nestle in the interstices of politics, economy and culture… warmaking must … *exploit* democratic political forms, and *manage* independent media" (Shaw, 2005:57). This conception allows us to move beyond an understanding based solely in the context of COIN situations – to one in which the relationship of war to other elements of political and social life can be seen as increasingly integrated in military, security and governmental activity. Building on the understanding of global warfare, we can take the insight that the "expansion of the battlefield to include human perception and the 'virtual space'" (Dunn Cavelty and Brunner, 2007:11) is not just a matter of military practice or strategy, but a significant one for our understanding of contemporary social and political experience. The examination of the contemporary propaganda apparatus through which the US military addresses Digital Age conflict demonstrates not just an organisation keeping up with Web 2.0 technology, but one at the cutting age of adapting practices which enhance the scope of state communication power, expanding influence beyond that traditional realm of military activity. This recognition compels us not only to revaluate our understanding of what military propagandist are *doing* in the online information environment, but to adapt our conception of what propaganda *is* – underlining the vital importance of studying the relationship between communication, technology, and warfare in the analysis of contemporary state communication power.

Appendix A: Methodological Note on the Search for CY-OPS Practice at the DOD

This section briefly outlines the method for researching DOD organisations which identified SOCOM and CENTCOM as key to the research. Engagement with both doctrine and broader military discourse illustrated that, at the cutting edge, formal military structures and processes of development are not necessarily a perfect guide to identifying areas of research interest. As such, in studying military practice the research began by casting a wide net – using doctrine and the other 'problem field' research as a guide while remaining aware of potential outliers or *ad hoc* practical developments not accounted for in the discursive material. Research began by deeply examining *all US military organisations with a relationship to Information Operations, PSYOPS, and "cyber" activities* – in order to ensure no relevant material was overlooked. This investigation involved studying material relating to a number of military commands and units (see list at end of Appendix), including: military-run website material (e.g. 24th Air Force, 2013; 1st IO Command, 2013), social media material, congressional testimony by commanders (see e.g. Hernandez, 2012; Alexander, 2013, Schwartz, 2010:491), job advertisements, PowerPoint presentations aimed at military peers (e.g. Walker, 2013; Information Dominance Corps, 2013), media articles on unit activities (e.g. Donnelly, 2011:16-18; Wilson, 2012; Pellerin, 2013), and other material which allowed an assessment of whether a unit was of potential interest.

I began by seeking to establish if there were any relevant activities which addressed the Internet as a sphere of public communication in a substantive way. Practically, this entailed identifying units with declared "cyber" or "PSYOPS/MISO" capabilities, and focussing on those cases where these activities overlapped – hence, CY-OPS. The focus of "cyber" on the Internet is fairly self-explanatory (though the terms "online", "web", "social media" and "Internet" were also used in searchers of relevant documents), and although in the doctrine it has been found to refer very strongly to the *technical* aspects of cyberspace, it is still a sign of an area worthy of examination. The broad area of "Information Operations" includes such disparate specialities as linguistics, network security, public affairs, and "directed energy systems" (those which use bands of the electromagnetic spectrum to incapacitate people, see Bostick, 2011:19-20), as such searches focussed on "PSYOPS" or "MISO" as the area of interest, but also included searches for the related terms "social", "psychological" and "media" in documents[134].

This approach lead to two main avenues of research. Firstly, into the structures and activities of the units under the relatively new US Cyber Command (CYBERCOM) and a search for cases in which they may be engaging with the content of information relating to public communication (rather than as the technical transmission or storage of data). And secondly, into the structures and activities of the US Special Operations Command (SOCOM) – which is tasked with leading PSYOPS/MISO development in the DOD, and

[134] Secretary of Defense Directive 3600.01 on information operations explicitly states that all PSYOPS/MISO activities must be listed as separate budget items in official documents (Secretary of Defense, 2013:10 – Directive 3600.01), technically meaning every instance would appear in military budget requests (which were examined during the research), however this was only one element of the research process, recognising that research cannot rely on the rigour of the subject organisation.

houses its only full time PSYOPS/MISO units[135] – with a special focus on their attempts to engage publics via Web 2.0. As will be clear, the research found that the later area – of PSYOPS structures and practices engaging in the cyber domain – was much more active than the former. Thus an analysis of SOCOM's PSYOP activity which addresses the challenges and opportunities of Web 2.0 provides the bulk of the key examples in this chapter.

The activity of United States Cyber Command (CYBERCOM) was examined in detail for signs of potential interest. CYBERCOM is a large and high-profile new command organisation created in 2009 in direct response to the increasingly importance of the Internet in conflict. It sits under the US Strategic Command – historically the Command responsible for outer space, global communication, command and control systems, some information operations, and control of the nuclear arsenal (US Strategic Command, 2011). During the research period, CYBERCOM was commanded by General Keith Alexander who also lead the National Security Agency (NSA) – the intelligence agency responsible for mass surveillance and analysis of telecommunication data which has been the subject of significant publicity and controversy since the whistle-blower Edward Snowden leaked documents making information of its activities public in 2013 (Greenwald, 2014)[136]. The two organisations are collocated at Fort Meade, Maryland, an arrangement which "promotes intense and mutually beneficial collaboration" (Alexander, 2013). However, this collaboration appears to be limited to the technical elements of 'cyber' such as network defence and hacking.

All material in the public domain on the training and activities of CYBERCOM forces – including military press material (e.g. Welsh, 2014), internal training or explanatory documents or presentations (e.g. US CYBERCOM – *WARGAME 13*, 2013), statements to lawmakers and peers (Alexander, 2011; Alexander, 2013), and reviews by external experts (e.g. Leed, 2013) – supports the conclusion that CYBERCOM's focus is on the technical aspects of cyberspace. Meaning they focus on securing networks and infrastructure, with some offensive hacking capability, and have no direct interest in the symbolic or social content of communication, it is war as the continuation of system administration by other means. PYSOPS is explicitly outwith the remit of CYBERCOM: the same policy announcement which designates USSTRATCOM (and by extension, CYBERCOM) as the proponent of Computer Network Operations and Joint Electromagnetic Spectrum Operations[137], designates PSYOPS as the responsibility of SOCOM (Secretary of Defense, 2013:10 – Directive 3600.01). Indeed, the only exception to the exclusion of

[135] There is another area of the military which focuses on PSYOPS, the US Army Civil Affairs and Psychological Operations Command, a reserve component which provides general purpose PSYOPS support to ground forces such as the capability to distribute leaflets or produce radio broadcasts, it is basically a logistics branch which has not seen any Web 2.0 development.

[136] This research has not engaged in a major way with the leaked material from the NSA (and its UK equivalent, GCHQ), because although it is undoubtedly of interest it is not a military endeavor. Furthermore, the problems of access to material are significant, the leaked documents are released selectively by a number of gatekeepers in the media and the agencies in question have adopted a "no comment" stance in relation to further information requests. However, work which examines the activities of NSA and GCHQ undoubtedly provides important context for this research (see Greenwald, 2014b; 2014c; GCHQ, 2014)

[137] Further demonstrating this, it is expected that the new Army Cyber Field Manual will be integrated with Electronic Warfare doctrine (Clark, 2013) – placing it firmly in the battlefield of wires and bytes rather than words and images.

PSYOPS within the structures of CYBERCOM is found within the subordinate Navy Fleet Cyber Command, where a 2013 order issued by the Chief of Naval Operations (Chief of Naval Operations, 2013) designates part of the responsibility for PSYOPS integration to Navy Information Operations Command (NIOC) Norfolk, which is the Navy's Centre of Excellence for Information Operations training and planning, collocated with Naval Special Warfare Command (NAVSPECWARCOM) in Virginia (NIOC Norfolk, 2014). NIOC Norfolk is party of CYBERCOM, but in the order it plays a *support role* to NAVSPECWARCOM, which is designated "as the primary conduit for the development of Navy MISO capabilities funded through USSOCOM" (Chief of Naval Operations, 2013:5). NAVSPECWARCOM is a Navy element of SOCOM - and is the organizational home to the special operations SEAL Teams which have played a significant role in the "shadow war" of the GWOT (see, e.g. Scahill, 2013).

That adaptation of Navy MISO doctrine and influence on cyber organization is guided from outside – by SOCOM – offers confirmation that the formal organizational importance of SOCOM in the area of PSYOPS matches its influence in developing PSYOPS and intelligence discourse and doctrine. As such, the research focussed on an examination of SOCOM, where I found that the most important developments in relation to Web 2.0 adaptation are deeply imbedded in special operations theory and practice.

List of DOD Organisations Examined

*This lists (in **bold**) the main elements of the US Department of Defense structure which were examined in the search for areas where Cyber and Psychological Operations merged. Below each main element are the subordinate units to which special interest was paid in the examination as they were found to be most likely to feature activity of interest to the research. Those underlined are sites where significant activity was found and are discussed in the body of the thesis.*

Policy/Executive Level: Secretary of Defense

Defense Information Systems Agency

DOD Information Operations Centre for Research (Naval Postgraduate School)

Office of Director of National Intelligence

Joint Information Operations Warfare Centre (located at 24th Air Force, San Antonio, Texas)

Joint Staff – J-39, Information Operations Coordination

Under Secretary of Defence Policy (Information Operations)

Assistant Secretary for Special Operations/Low Intensity Conflict (MISO)

US Strategic Command

Joint Task Force – Global Network Operations

Joint Task Force – Network Warfare (staff from both moved to Cyber Command)

US Cyber Command

Cyber Mission Forces

Army Cyber Command

Network Enterprise Technology Command

1st IO Command (Land)

1st IO Battalion

2nd IO Battalion

7088th Military Intelligence Brigade

Fleet Cyber Command (Navy)/10th Fleet

Navy Network Warfare Command

Cyber Defense Operations Command

Navy Information Operations Command

CTF 1030 Navy Information Operations Command Norfolk

CTF 1030.2 Navy Information Operations Command San Diego

CTF 1030.1 Navy Information Operations Command Norfolk

CTF 1030.3 Navy Information Operations Command Whidby Island

Air Force Space Command (home of Air Force Cyber component)

24th Air Force

67th Cyberspace Wing

688th Cyberspace Wing

318th Cyberspace Operations Group

38th Cyberspace Engineering Group

Marine Forces Cyber Command

Marine Forces Network Operations and Security Center

Company L

US Special Operations Command

J39 Operations Group

US Army Special Operations Command

JFK Network Warfare Center and School

Military Information Operations Support Command

4th Military Information Support Group/Psychological Operations Group

8th Military Information Support Group/Psychological Operations Group

3rd Military Information Support Battalion
Navy Special Warfare Command
Air Force Special Operations Command
193rd Special Operations Wing
Marine Special Operations Command
Joint Special Operations Command
Joint Military Information Support Command (previously Joint PSYOPS Support Element)
Department of Defense Analysis (Naval Postgraduate School)
CORE Lab (Naval Postgraduate School)

US Central Command
Special Operations Command Central
Interactive Internet Activities – Joint Psychological Operations Task Force
Digital Outreach Team
J3 – Information Operations

US Army Reserve Command
US Army Civil Affairs and Psychological Operations Command
2nd PSYOPS Group
7th PSYOPS Group

Appendix B: TRWI Content Analysis Notes and Table

Notes on Trans-Regional Web Initiative Website Analysis

The analysis undertaken of the TRWI websites was an immersive analysis based on visiting those websites every day for a one month period, covering November 2013. This also included checking the social media profiles of the websites to build an understanding of the interactive elements.

The analysis of Alexa analytics was carried out in April 2014. The process of link analysis was to look at the list of all sites linked to the TRWI site listed by Alexa, which are arranged according to popularity of the page on which the hyperlink originates. I searched through the list of in-links for the URL's for major news sites, blogs, etc. which were familiar to me as popular or influential. This is a manual process intended to show the potential of links to other sites rather than a quantitative analysis of the phenomenon.

Magharebia

"Headlines"

Between 6 and 10 stories a day, of which on average 2-3 stories are related to sports – mostly to North African football. These stories are all short (2 sentence) pieces reporting on results, transfers, etc. which are drawn from other sources "X beat Y at this place in this competition, AFP reported".

Most other stories are regional news – local cultural, political or security events. These are also mostly 2-3 sentences which are based on press releases or stories reported elsewhere (the BBC, Libya Herald, El Watan, Shems FM, Tunisie Numerique, Le Matin, AFP). Some are longer (4-10 sentences) with some original reporting in the form of quotes from regional officials.

Mauritania stories notable during research period: for example a story on the elections is headlined "Mauritanian elections end in calm", it is 4 sentences long and says only that "the head of the African Union (AU) observer mission, Algerian former Prime Minister Ahmed Ouyahia, confirmed that no irregularities had been seen" and lists the number of candidates and seats (Magharebia, 25/11/2013a). Another story on 05/22/2013 says "election campaign starts in Mauritania" and notes "The government brought in foreign observers to guarantee transparency" (Magharebia, 05/11/2013).

Overall headline coverage is minimalist. There is rarely much of an editorial line taken because there is not enough space. Just reporting things that have happened: conferences, statements made, etc. However, as the Mauritania coverage suggests, the very choice of facts and events presented give a very sanitised and bland view of the issues.

"Features"

There are 70 "feature" articles in November 2013, in categories of Security (20), Terrorism (15), Sport (7), Analysis (1), Media (1), Politics (3), Energy (4), Culture (4), Crime & Justice (3), Diplomacy (2), Protests (1), Human Rights (2), Economy (4), Arts & Entertainment (1), and Youth (1) – 1 was uncategorised.

These are longer pieces of original journalism, with named journalists in the region reporting on statements at summits, interviews with local politicians or civil society, and interviews with other journalists on regional security developments, etc.

They produce little activity on social media, with between 0-15 shares on Facebook and Twitter. Some popular articles produce a substantial amount of comments – one on the killing of a terrorist has over 150 people voting in a like/dislike pole and 25 comments (Magharebia, 25/11/2013b). Another article on the rise of terrorism in Tunisia (Magharebia, 22/11/2013) has 200 like/dislike and 22 comments, comments are most very critical of the tone of the piece, calling it scaremongering and accusing it of equating Islam with terrorism. Another (Magharebia, 20/11/2013) is based on reporting the opinions posted by Libyan blogger, which shows some integration into the blogosphere through links, thought the (20) comments are mostly partisan and not very constructive. Comments are moderated by the site, though ones critical of American allies and policy are allowed, though they are mostly just "God's curse on France and its supporters!", etc.

Interactive forum Zawaya

This is a Magharebia-hosted forum which has threats which begin with posted video clips and then had comment threats. They are not really very popular: Started January 2013 - 35 threads. 8 have no comments, 14 have 1-5 comments, 5 had 6-10 comments, 5 have 10-20 comments, and 1 has 121. It is not very active

Link Analysis:

- Linked to by CNN (06/01/2014) for its coverage of Mali – no acknowledgement of the sites source just a hyperlink, the story is on Moroccan training of Malian imams as part of the peace process (Magharebia, 23/09/2013)

- Linked to in the Wall Street Journal, (13/12/2013) amongst a number of international sources in a round up of global media, the link says "Morocco continues its fight against terrorist financing. (Maghrebia)". The story is Magharebia (12/12/2013) and is a good-news story about AML laws in Morocco.

- L'Express (10/02/2011) (France) references a Magharebia article as a "very emotional plea from Libyan bloggers" on censorship of the Internet there, this is a Magharebia (02/02/2010) article which recycles Libyan bloggers comments on YouTube censorship.

- Al Jazeera (05/01/2011) uses a link to Magharebia (03/01/2011) to demonstrate criticism by Tunisian politicians of AJ's coverage of the post-Bouzizzi protests – the report is based on statements of many politicians and journalists which are predominantly negative to AJ.

- Magharebia (07/02/2013) on the rift between AQIM and Mokhtar Belmokhtar is referenced in part of a channel 4 report (Hilsum, 2013) on Mali which says that some Islamists were drug smuggling "while claiming all their activities for religiously sanctioned" [sic]. The Magharebia story is based on an interview with a Sahel expert talking about Belmokhtar.

- An Amnesty International, (2013) report on the detention of youth activist Tahar Belabes in Algeria links to an interview with him by Magharebia (17/06/2011). Demonstrating it is not all pro-US regime propaganda and that it a complex dynamic.

<u>Sabahi Online</u>

"Headlines"

These articles are a bit longer than the ones on Magharebia, with 2-10 sentence articles on various security incidents, statements by policy makers, political developments in the

region, etc. Mostly draws on other media (Garowe Online, AFP, Hiiraan Online, Radio Bar-Kulan) and press releases (MSF, the Somali government, Open Society Justice Initiative)

Includes stories critical of regional allies including: "Kenyan anti-terrorism police accused of human rights violations" (Sabahi, 21/11/2013a) which mentions US and UK funding of said CT police; and, "Somali police arrest alleged rape victim as UN calls for inquiry" (Sabahi, 21/11/2013b), though there is a spin in the headline "Somali government welcomes critical report on rape investigation" (Sabahi, 12/11/2013) which discusses a report critical of the government.

Few of the stories have any likes, shares, or comments.

"Features"

There are around 30-35 in a month, and they are not categorised as they are on Magharebia. They cover a variety of issues such as: social issues in Kenya (access to justice, police corruption, press freedom), security policy in Somalia (a ban on tinted windows), and the fight against Al Shabaab.

They tend to have none or just a handful of FB shares or tweets, and less than 10 comments, though sometimes up to 40-50 like/dislike votes. The comment feature on this site is not very active – the three most popular have 20, 34 and 200 comments. This outlier is an article on Quail farming (05/11/2013), with most comments asking how to get hold of quails and various details on quail husbandry.

Link Analysis

- Yahoo! News (15/11/2013) links to and quotes extensively a Sabahi article on Al Shabaab banning smart phones – basically the whole content is drawn from a Sabahi (14/11/2013) article

- Ironically, referenced in a CNN (02/08/2013) called "Why we should keep out of Somalia's affairs" as a link about a reconstruction conference taking part which Sabahi (25/06/2013) reported on.

- Is referenced in the Daily Beast (12/01/2014) in an article on Al Qaeda's evolution for the claim that "al-Qaeda may in fact have taken on unacknowledged affiliates during the Arab Spring", linking to a Sabahi (05/10/2012) interview with a Moroccan terrorism research called Abdellah Rami about Ansar al-Sharia.

- Is described in the Canada Star (02/10/2013) as "a news website that covers the horn of Africa", and referenced in relation to the quotes given in the article by Somaliland officials supporting the jailing of convicted (Canadian-Somali) rapists Sabahi (06/08/2013)

- Referenced in Foreign Policy (04/11/2013) in relation to an interview Sabahi (08/10/2013) did with an ex-pirate who was later arrested in a sting operation, lured to Belgium expecting to consult on a movie about his life.

<u>Southeast European Times</u>

Content

This is a different format from the AFRICOM websites – it doesn't have the daily "headlines" and "features. Instead it publishes only features, which aren't listed by date but by subject – politics, extremism, justice and law enforcement, foreign relations,

peacekeeping, economic development, integration, society. They are also listed by country. There are 20-30 articles published a month.

The stories are predominantly fairly banal news fare reporting on government statements, new policies, and regional governance. Most notable thing about the stories is that coverage heavily emphasises regional cooperation and good relations – e.g. "Attacks on Roma spark calls for action in Southeast Europe" (SETimes, 11/11/2013), "On Tolerance Day, Macedonia organises a national discussion on hate speech" (SETimes, 21/11/2013), "Education ministries working to prevent bullying in schools" (SETimes, 19/11/2013).

The comments section at the bottom of each story often features quite coherent and engaged discussion between commenters (and automatically translates comments into English on the English version of the site). In terms of relevant comments and the frequency with which posters engage in debate and dialogue with one another it is the most vibrant and useful website.

Link Analysis

- In Huffington Post (19/08/11) article it is quoted just as a reference of a statement Turkey made to Mubarak, the SETimes (02/02/2011) just reported Turkey's statement at the time.

- Business Insider (29/10/2012) quotes at length from an SETimes (29/10/2012) article on the rise of Golden Dawn in Greece.

- Again (like other TRWI sites) linked to in the Wall Street Journal (02/07/2013) "Risk and Compliance" blog – this time as "Turkey's wealth amnesty might blaze a train for Balkan nations", SETimes (01/07/2013)

- Referenced in Bloomberg (28/02/2012) embedded in a link that says "But a much larger increase in tax rates could help to both narrow the fiscal gap and further **reduce smoking rates**." in Greece. SETimes, 05/01/2012.

- Referenced in the Atlantic (14/12/2012) in relation to a "bizarre speech" by Erdogan in Turkey on a historical TV drama that he critiqued for misrepresenting ottoman history. This just quotes an SETimes report (03/12/2012) of a speech – demonstrating that being an accessible English-language source for this type of news it gets links.

- The Economist lists it (31/09/2010) in an article on "news from the east" – saying it "overs 12 countries in nine languages other than English, boasts a solid reference section and news archive, but is perhaps not as slick or thoroughly updated as one would expect from an outlet sponsored by the US Military's European Command".

SES Türkiye

Has around 50-60 medium-long articles per month, written by a small group of Turkish writers. They are of medium length and cover issues such as Turkish-Armenian relations, Turkish media, Turkish regional cooperation, cultural issues like gender and heritage, and developing issues within Turkish media and culture. Tend to be bigger-picture features articles which discuss emerging trends or debates rather than hard news (e.g. "Security experts debate change in military service time" (SES Türkiye, 11/11/2013; "Bride-swapping practice facing criticism from youngsters" (SES Türkiye, 18/11/2013)), likely because these type of articles catalyse more discussion on social media and don't have the time constraints of breaking news. Again, focus is on regional and communal cooperation, e.g.: "Football Unites on Cyprus" (SES Türkiye, 19/11/2013); "Christian-Islamic dictionary

promotes peaceful co-existence" (SES Türkiye, 08/11/2013a); "Turkish army contributes to reconciliation, stability in BiH" (SES Türkiye, 08/11/2013b).

Most articles have less than 10 shares, but around half also have comment threads between 10 and 50 comments with users debating in a constructive way.

No link analysis was possible as the site is a sub-domain of SETimes and thus not searchable as a separate entity.

Al-Shorfa

"Latest news" Headlines

In the research period there were 200 'headline' stories (6-7 a day) of between 2 and 8 sentences based on regional newspapers (Jordan Times, Okaz Daily, AFP, Oman Daily, Al-Watan Kuwait) or press releases (a lot from Iraqi police and Army spokespeople, Yemeni MOD). Almost all Iraq stories are about security issues – bombings, arrests, attacks, raids – and all are based entirely on statements of Iraqi Army, Police or government officials who give quotes which make up the bulk of the piece. They have this format: Sentence describing the news (attack, new policy, etc). Quote from Iraqi official saying "x told Al-Shorfa". Another sentence of context, sometimes with another quote from the same official. (e.g. see Al-Shorfa, 27/11/2013a; 27/11/2013b, 26/11/2013)

"Features"

From across the region, written by local reporters, usually about 10 paragraphs. Cover mostly positive stores: infrastructure construction, policies to fight social problems, regional cooperation, and cultural events. Also covers anti-AQ stories and reports on gains against terrorists (i.e. arrests). Also a fair amount of Syria coverage relating to AQ linked groups, including "Al-Qaeda recruiting children, orphans in Syria" (14/11/2013), "Al-Qaeda affiliate struggles to re-establish control in Syria" (19/11/2013), etc. The former of which received over 100 like/dislike votes, 59 tweets and 29 FB recommends, and 115 comments (most of which are just like "O God protect Syria!"). This type of engagement is found only in a very few popular stories and the comments do not give the impression of a vibrant engagement by users (few responses or discourses).

Apps

USCENTCOM listed as developer in Google Play and iTunes app stores – has 6 Arabic apps. They are all "brought to you by the Open Dialogue Form, a U.S. Central Command sponsored discussion community". All require the following permissions: It requires the following permissions: full network access, storage, disable lock screen, test access to protected storage, prevent from sleeping. Download numbers refer to Google Play store only (iTunes does not list number of downloads)

Khatta - for Arabic calligraphy, it has 50-100k downloads, and 1,026 reviews with 4 star average.

Kutob - a "regularly updated collection of key books that embody the fruits of Arab enlightenment". It has 50-100k downloads and 583 reviews with 4 star average.

Aghani – A gramophone app with classic "golden age" Arabic music. 10-50k downloads, 111 reviews with 4 star average.

Towards Mecca – An app which uses the compass to point to Mecca, prayer time reminders "with countdown", verses from the Quran and Hadith, "clickable prayer beads" and

calendar. 5-10k downloads, 65 reviews with 4 star average. This app requires extra permissions: access to 'precise location" through GPS and network-based means, Camera access, and permission to run at startup.

Shakhsiyat – An "interactive educational Arabic-language tool that highlights key figures in Islamic history, showcasing their life, work, influence, and contributions to Islam and humanity". 500-1000 downloads, 8 reviews with 3.4 stars average.

Sharqiyat – "lead your animated band into music with this innovative Arabic-language app!". 100-500 downloads with 4 star average.

Link Analysis

Not linked-to as often as the other websites. I suspect due to more reputable media in this area offering better sources to work from.

- Notably, is referred to in a (BBC, 07/09/2013) article (from BBC Monitoring) on the problems with tourism in Lebanon as "The US state-backed Al-Shorfa news site" which is ones of the only times I saw a TRWI website identified as such.

Mawtani Al-Shorfa

Shares Al-Shorfa's short stories, and in the research period had 26 extra feature stories covering Iraq. These are in line with the state aim of "highlights movement toward greater regional stability both through bilateral and multilateral cooperative arrangements and steps governments take toward stability in Iraq", and also focus on developments that hinder both terrorist activity and support for terrorism in the region" (Mawtani Al-Shorfa – *About Us,* 2014). Stories cover positive developments in social issues (events hosted, education achievements, new policies, "Iraqi Ashura commemoration reflects national unity" (15/11/2013), "Baghdad hosts special festival for orphans" (26/11/2013)), arts (new theatre, gallery shows, 'Baghdad day' (07/11/2013a)), security (successes of Iraqi security forces), and terrorism ("Jabhat al-Nusra steals formula destined for Syrian babies" (01/11/2013), "Anbar residents close ranks against al-Qaeda" (04/11/2013), "Al-Qaeda's mafia-like actions in Syria underline its fragmentation" (07/11/2013b).

The stories are written by local reporters, include sources in government and the police, and small local NGOs. Around 10-20% of popular stories have between 50-100 comments.

As with SES Türkiye there is no link analysis available as the site is a sub-domain of Al Shorfa.

Khabar South Asia

"News Briefs"

These are articles 5-10 sentences long. Based on reports from global and local media (AFP, Times of India, Dhaka Tribune) as well as press conference statements by officials (though these are mostly drawn from other reports in the media). They cover incidents of violence (mostly Maoists rebels and Islamists), political developments (elections, campaigns, new policies), and crime (arrests for notable crimes, trials). Very few of these stories have any likes, shares, or comments at all.

"Features"

Longer (6-10 paragraph) articles on a variety of topics: Bollywood, cricket, infrastructure projects, social issues (underage marriage (20/11/2013), inter-community cooperation (16/11/2013), prison), politics (elections, summits, new policies). Also focuses on regional security issues such as Maoist groups in northern India (23/11/2013) and the Tehreek-e Taliban in Pakistan (27/11/2013). Around a quarter of these have 5-20 shares or tweets, and 1-5 comments – though not hugely popular.

Link Analysis

- A whole article from Khabar is reposted with link on a blog called Bangladeshwatchdog (15/08/2013) which also reposts articles from the Economist, Forbes, Open Democracy and other news websites.

- Again in the Wall Street Journal (26/07/2013) in the "Risk & Compliance Journal" section, Khabar (26/07/2013) is linked to on a story on Nepalese anti-money laundering policy

- The Bangladeshi news site Natunbarta.com has, throughout 2013, been publishing articles based entirely on stories from Khabar South Asia – including hyperlinks to Khabar, statements like "x told Khabar…", "report obtained by Khabar", "X happened reports Khabar South Asia". This was the format of 419 stories on the site, often with links to multiple Khabar stories within a single Natunbarta story. It is never attributed as a PACOM website. Nutunbarta is the 4th most popular news website in Bangladesh, and the 14th most popular website overall, with 277,000 unique monthly visitors.

- Similarly, the Bangladesh Chronicle has been publishing wholesale full stories from Khabar, just putting a link at the bottom that says "Source: Khabar South Asia". There are 16 stories like this on the site, and 1 other on the topic of Khabar which is critical of PACOM's sponsorship, saying that "Regionalism in Southasia should […not be] something to be promoted or manipulated by the geo-strategic agenda of a world power" and says it "is inappropriate for a military behemoth to run a news-and-analysis portal aimed at the Southasian public, for it can only be a masquerade. The state-sponsorship makes the endeavor suspect, an attempt to tilt public opinion in the direction favoured by US strategists" (Bangladesh Chronicle, 03/04/2012).

- Another 13 stories are also posted in full on TheMuslimTimes.org with "Source: Khabar South Asia" before them.

<u>Khabar Southeast Asia</u>

"News briefs"

Around 50 shorter articles posted per month. Subjects include national and regional security (especially in Malaysia in Philippines), inter-regional cooperation, and national political events. They are mostly 5-10 sentences long and draw on regional and international reports (Jakarta Post, AFP, The Jakarta Globe, Tempo). They have very few shares or comments.

"Features"

These are longer articles with a strong focus on regional and inter-cultural cooperation – this is the prevailing theme. For example: "Indonesia's U-19 football team displays athletic excellence, tolerance" (19/11/2013); "In Central Java, NU to open dialogue with Ahmadiyah followers" (27/11/2013); "Thailand to launch 24-hour Malay TV channel"

(22/11/2013); "Doing their part to help storm victims" (21/11/2013); and "Truth and Reconciliation Commission discussions held in Aceh" (06/11/2014).

Most feature articles have between 1-5 comments, with a small amount of popular ones receiving up to 50.

Links Analysis

- Is linked to by Foxnews.com (01/09/2013) as the sole source on a story about virginity testing at a school in Indonesia

- Is linked to 4 times by the wholesale posting of stories on Themuslimtimes.org

InfosurHoy

"Headlines"

89 in November 2013. Stories cover drug war stories (which make up the bulk of the news), national politics, and some issues of international politics that touch on south America. They are mostly 3-6 sentences and based on international and local news sources. They list all their news sources at the bottom (AFP, El Pais (Uruguay), El Universal (Mexico), Milenio (Mexico), Reuters, EFE (Guatemala), Clarin (Argentina), El Tiempo (Colombia)). No shares or comments on almost all the articles.

"Features"

Mostly cover national issues through local reporters – again a heavy focus on the drug war (arrests, operations against gangs, drug problems) as well as some on social issues (education, environment) and some on football. Focus seems to be on central America and the Colombia, focusing more on allies than rivals (i.e. there is very little coverage of Venezeula).

Most articles have 1-15 comments, though many (the majority) of them seem to be by bots and do not really engage with the subject matter or other comments: e.g. "very good article…I liked it a lot" (Infosurhoy, 08/11/2014)

Link analysis

- Linked to in the "Around the web" section of a Huffington Post (22/02/2013) on favelas, listed in line with links from the LSE, NYT, FT, etc. Gives credibility

- Is linked to as a source for the claim in a Business Insider (09/12/2011) article that Evo Morales is the source of "a lack of proactive efforts" to cut cocaine production, the story is InfoSur Hoy (22/12/2008) which notes that Morales has stopped allowing the US DEA to operate in the country. Again in Business Insider (26/03/2013) for a source of stats on tourism in Colombia

- Linked to in the Daily Beast (25/06/2013) as a source for the stats on car deaths in Brazil, similarly in Al Jazeera (11/08/2013) as a source of a claim that land and human rights activists had been murdered in Honduras

- 59 stories from InfoSurHoy have been reposted in English on HondurasWeekly.com, with the note "This article was originally published by Infosurhoy" at the bottom – no disclaimer as to the military backers..

Central Asia Online

"Latest news"

All short articles between 2 and 6 sentences covering reports of attacks, arrests, new policies announced, etc. Quotes local media, state media, and sometimes RFE/RL. For Afghan stories uses statements from local officials. This has the dual role of giving them an audience for their statements and building up their media training, while allowing CAO to show engagement with Afghans.

Features

Mostly on regional cooperation (14/11/2013a, 14/11/2013b) and problems of extremism in society (e.g. 27/11/2013; 25/11/2013). There is one notable article with lots of comments and engagement which relates accusations that Tehran is meddling in Afghanistan (07/11/2013). Apart from that however there is not much evidence of audience engagement with the articles (only 0-5 comments on most).

Link Analysis

- Embedded link in the "Around the Web" section at the bottom a Huffington Post article (10/02/2013) on Pakistan to a CAO story about the Pakistani bomb squad being 'unsung heroes" (19/08/2013) based entirely on interviews with said bomb squad. The link it in a list with BBC, Reuters and Times of India links which confer credibility upon it.

- Embedded link in a CNN article on the use of "little girls" as suicide bombers by the Taliban (CNN, 07/01/2014) to "media reports" about Afghan police stopping a 12-year old girl from being a suicide bomber. "media reports" links to a CAO story (21/11/2013) based on the statements of Afghan officials.

- A link in the Wall Street Journal (17/06/2013) on the passage of an AML bill in Tajikistan reference Central Asia Online (13/06/2013)

- The International Business Times (14/09/2013) gives Central Asia Online (with link) as the source of a quote from a Pakistani military official on militancy in Balochistan, the (Central Asia Online, 10/09/2013).

- In an article in Dawn (19/12/2012) called "Drones aren't the only killing machines" about the violence from Taliban in Pakistan it references a CAO story on militants carrying out attacks on schools with a hyperlink (25/10/2012) to a story carrying mainly quotes from Pakistani officials on the evils of Taliban targeting children.

- An article in the Independent (17/05/2012) on misogyny and the link to wearing of bikinis and niqab links to a Central Asia Online (10/03/2011) which is very critical of the role of the hijab in Tajik society – blaming it for women's exclusion from education (without discussing the role of anti-hijab laws in excluding women).

COCOM - Program Name	CENTCOM - Earnest Voice	
Regional News Websites	Mawtani	Al-Shorfa
URL	www.mawtani..al-shorfa.com	www.al-shorfa.com
Languages	Arabic, Farsi, English	Arabic, Farsi, English
Region	Iraq	Middle East, Iran
Attribution	"Sponsored by USCENTCOM" - in "About Us" section	"Sponsored by USCENTCOM" in "About Us" section
Dates (from Archives)	05/2008-present	05/2008-present
Contractors	General Dynamics IT	General Dynamics IT
Alexa Ranking - Country as % of Traffic/Populatrity of site in that country	sub-domain of Al-Shorfa	Egypt: 24.6%:3,181; Iraq: 14.2%:**1,118**; Yemen 10.6%:**988**
Volume of stories	26 features per month - shares news 'headlines' stories with parent domain - Al-Shorfa.	120 short headlines and 58 features articles in a month
Content of stories - Short Notes	Stories by local reporters - lots of quotes from government, police, and local NGOs. Stories fit in with the stated aim to "highlight movement toward greater regional stability both through bilateral and multilateral cooperative arrangements and steps governments take toward stability in Iraq. Mawtani.com also focuses on developments that hinder both terrorist activity and support for terrorism in the region" (From the About Us page). Stories cover positive social issues (events hosted, new policies, shows of national unity, et,c) - "Iraqi Ashura commemoration reflects national unity", "Baghdad hosts special festival for orphans". Also successes of the security forces, and the crimes of Islamists (especially in Syria).	Headlines: 2-8 sentence stories based on regional newspapers (Jordan Times, Okaz Daily, AFP, Oman Daily, Al-Watan Kuwait) or press releases from alies (a lot from Iraqi police and Army spokespeople, Yemeni MOD). All Iraq stories are security events (bombings, attacks, new policy, etc.) with a quote from an Iraqi official. Features: Written by stringers accross the region, about 10 paragraphs. Mostly good news stories about infrastrucuture being built, policies tackling social problems, and cultural events, or stories about AQ crimes or setbacks. Notably most Syria coverage are negative stories about AQ-linked groups.
Other features	A 'featured video' section which contains links to and conversation on YouTube videos discussed in Al-Shorfa's "YouTube" section. There are only two videos, one of which has over 3000 like/dislike votes and 300 comments.	A section on "The Bin Laden Documents", a'leaks' style series discussing the documents released by the Counter Terrorism Centre, probably linked to a SOCOM PSYOPS project called "Project Redbeard" which is based on exploiting captured AQ material for PSYOPS purposes. Also has 6 apps on Google Play and iTunes, dowload stats from Google Play: Khatta - Arabic Caligraphy (50-100k); Kutob - "collection of key books of that embody the fruits of the Arab enlightenemnt" (50-100k); Aghani - "golden age" Arabic music (10-50k); Towards Mecca - uses geolocation to point to Mecca, has prayer timer and "clickable prayer beads" (5-10k); Shakysiyat - educational tool about "key figures in Islamic history" (500-1000); Shaqiyat - "lead your own animated band" (100-500).
Interactive elements in news stories	Internal comments, a few popular articles have up to 50-100 comments though the majority of these are basic statements like "God bless you/them/Iraq" or "God, give us victory/have mercy on us". Has a like/dislike function which can get over 1000 votes on the ~10% of articles which are popular.	Internal comments, very few have any on the short "latest news" articles, though some have up to 10. Has a like/dislike vorting system with up to 100-200 votes on the few popular articles.
Social Media links	Links to tweet this or recommend on Facebook but not used more than 10 times on most.	Very low uptake on Twitter and Facebook sharing or articles. Some longer features have up to 10 of each, and there a few outliers with up to 60.

Measurements of Popularity		
Facebook - All social media analysis done 11-13/02/2014	Yes, has 48,000 likes (arabic), 1,401 (Farsi). Says it is "Sponsored by US Central Command" in about us. Most popular in Baghdad amongst 18-24 year olds. Justs posts the articles from Mawtani, most have between 1-10 likes and no comments, about 1 in 10 posts has between 1-10 comments, not very active.	Yes, in Arabic. Has 36,533 likes (Arabic), 858 likes (Farsi),. "Sponsered by US Central Command" in about section. Posts links to all stories, most have none or a few likes, some (around 1 in 20) have 0 to 10 likes or comments. Very low level of use compared to EUCOM sites.
Twitter	@mawtani, (arabic) 94 followers,@mawtani_fa (farsi) - 0 followers, no interaction	@al_shorfa (arabic) 784 followers, @al_shorfa_fa (Farsi) - 14 followers, just tweets links to stories, no interaction
YouTube	Shares page with Al-shorfa	116 subscribers, 6 videos with between 11000 and 177000 views. These videos are all slickly-produced anti-suicide bombing videos - they do not bear any branding or notice of who made them. I think this is a separate project that Al-Shorfa links to - they are also posted in the 'featured videos' section on Mawtani

COCOM - Program Name		AFRICOM - Ob
Regional News Websites	Central Asia Online	Magharebia
URL	www.centralasiaonline.com	www.magharebia.com
Languages	Urdu, Russian, Farsi, English	English, French, Arabic
Region	Tajikistan, Uzbekistan, Kazakhstan, Afghanistan, Kyrgystan, Turkmenistan, Iran, Pakistan	North Africa (Mauritania to Tunisia)
Attribution	"Sponsored by USCENTCOM" in "About Us" section	"Sponsored by United States Africa Command" in "About Us" section
Dates (from Archives)	05/2008-present	12/2004-Present
Contractors	General Dynamics IT	General Dynamics IT
Alexa Ranking - Country as % of Traffic/Populatrity of site in that country	Pakistan: 47.6%:4,121; US: 10%:207,831; Iran: 8.1%:23,084	Algeria: 23.3%: **1,136**; Libya: 22.7%: **395**; Morocco: 15.9%: **1,008**; Tunisia: 12%: **831**; US: 6.6%; 151,543; Mauritania: 4.6%: **150**
Volume of stories	271 short stories and 39 features articles in a month.	216 short article and 67 features articles in a month
Content of stories - Short Notes	"Latest News" stories: between 2-6 sentences, reporting attacks, arrests, new policies of regional govenrments - based on quotes from local media stories, and sometimes from Radio Free Europe/Radio Liberty. Afghan stories focus heavily on quotes from local officals. "Features" are 6-10 paragraphs long and focus on regional cooperation and the problems of extremism in society. Notably, in all stories which mention Iran it is portrayed as an aggressor - supplying weapons, training terrorists, collaborating with the Taliban, etc.	"Headlines" are mostly 2-3 sentence stories covering issues of general interest, about 30% football, local cultural events, local security or political incidents. Based on stories from other media (BBC, Libya Herald, El Watan, Shems FM, Tunisie Numerique, Le Matin, AFP). Some longer stories 4-10 sentences add to these reports with staements from regional officials. At the time of analysis, headline coverage of Mauritanian elections noticible for not mentioning controversy. "Features" are longer by local journalists reporting on statements at summits, interviews with local policians or civil society or other journalists as area experts.
Other features	Featutes the YouTube video from Al-Shorfa's page - the slick ones against suicide bombing.	A discussion site called Zawaya - short vidoes to catalyse discussion with comments threads. Started January 2013 - 35 threads. 8 have no comments, 14 have 1-5 comments, 5 had 6-10 comments, 5 have 10-20 comments, and 1 has 121
Interactive elements in news stories	Internal comments are quite active, 1-10 on most articles, and the like/dislike function has over 100 votes on about 30% of articles, suggesting stories can consistently get a modest amount of engagement.	Internal comments can reach 20-80 on popular articles, the like/dislike voting function gets up to 100-200 votes on popular articles.
Social Media links	Longer features have 10-20 shares through Facebook and Twitter, though short ones are mostly not shared at all.	Low uptake on Twitter and Facebook sharing, most have less than 10.

Measurements of Popularity		
Facebook - All social media analysis done 11-13/02/2014	Yes - 14,846 Likes (Russian), 1,932 (Farsi), 45,932 (urdu). "sponsored by US Central Command" in about section. All posts links to stories - standard of about 1-10 likes per story, with around 1 in 25 stories receiving a hundreds likes and hundreds of comments - suggesting a potential significant latent audience of lurkers.	Yes. 504,619 Likes (arabic only). Shares every feature article published on Magharebia - a significant amount of which have hundreds of likes and comments (mostly in arabic), it is a very active page. The Facebook page is attributed to AFRICOM in the "about" section of the profile.
Twitter	@ctrlasiaonline (russian), 207; @CAO_ru (russian), 58 followers;@CAO_fa (Farsi) - 14 followers; @CAO_ur (Urdu) - followers, no interaction, just posts links to stories (1000s of tweets each so not low followers due to new accounts)+E19	@magharebia, 2,145 followers, tweet every article, no interaction.
YouTube	no	250 subscribers, 36 videos over 5 years, between 100 and 20,000 views

COCOM - Program Name	jective Voice	EUCOM - Assure
Regional News Websites	Sabahi	South European Times
URL	www.sabahionline	www.setimes.com
Languages	Somali, Arabic, English, Kiswahili	Bosnian, Croatian, Serbian, Greek, Macedonian, Albanian, and English
Region	Somalia, Kenya, Tanzania, Djibouti	Albanian, Boznia and Herzegovina, Bulgaria, Croatia, Greece, Kosovo, Macedonia, Moldova, Montenegro, Romania, Serbia, Turkey
Attribution	"Sponsored by United States Africa Command" in "About Us" section	"Sponsored by the US European Command" in "About us" section
Dates (from Archives)	01/2012-Present	Created 1999 (as Balkan Times), Changed to SETimes in 2002 - Present
Contractors	General Dynamics IT	General Dynamics IT, Started by Rendon Group
Alexa Ranking - Country as % of Traffic/Populatrity of site in that country	Kenya: 47.7%**: 952**	Turkey: 28.5%: 18,119; U.S.: 27%: 176,569; Greece: 10.1%: 16,423; Serbia: 4.9%: 12,276; Bosnia and Herz: 4.8%: 4,106; Albania: 3.4%: 3,250; Macedonia: 3.0%: 3,794
Volume of stories	144 short articles 36 features articles a month	Hard to say as not archived by date - around 6-7 longer articles every week. No 'headlines' or short news items.
Content of stories - Short Notes	"Headlines" are 2-10 sentences long on various security incidents, statements on policy, and regional political/security developments. All based on regional media (Garowe Online, AFP, Hiiraan Online, Radio Bar-Kulan) or press releases (MSF, the Somali government, Open Society Justice Initative). Notably, has stories critical of Kenyan CT police which mentions US funding, and of the Somali govenrment's arrest of an alleged rape victim. "Features" cover social issues in Kenya (justice, corruption), security in Somalia, and the fight against Al Shabaa, also include interviews with Somali officials and other personalities.	Does not publish any short articles or 'headlines' - focussing on "Features" only. Stories are listed by subject rather than date, and these cover: politics, extremism, justice and law enforcement, foreign relations, peacekeeping, economic development, integration, society. However, most of them are fairly conservative news fare reporting on government statements, new policies, and non-contrversial social issues. Coverage heavily emphasises regional cooperation and good inter-communal relations.
Other features	Has a "resources" page hosting "Somailia's Roadmap Documents" establishing the current Western-backed government	An "info centre" with country info, political system timelines, and "who's who". A weekly podcast "highlighting the best of the weeks articles"- this is a 3 minute bad recording of a non-native english speaker reading some articles - it is not compelling listening. Not available in other languages. Also has "Special Reports" which are linked series of articles on issues like "The Hague's Most Wanted", "Eurovision 2010" and the EU 2009 elections.
Interactive elements in news stories	Internal comments (usually less than 10), like/dislike voting with around 40-50 votes per feature article. One outlier has 200 comments - an article on quail farming in Kenya which has many comments facilitating the trade in quails.	Internal comments but you need to register and there are very few articles with any comments - those that do often have lots "under review" as they must be vetted. Has like/dislike voting with rarely more than 10 responses.
Social Media links	Low sharing rate on Twitter and Facebook - mostly no shares.	Facebook 'recommend' link - some of which have been used 100s of times

Measurements of Popularity		
Facebook - All social media analysis done 11-13/02/2014	Yes. 20,575 likes (English), 16,848 (Somali) 6,188 (Arabic), . Most popular in Nairobi (Eng), Mogadishu (Somali),and Hargeisa (Somaliland, arabic) with 18-24 year olds. Posts are stories from the site. Most have less than 5 likes or comments, though the Somali page is fairly consistent with this small amount of engagement.	Yes, 580,582 likes (English only). Most popular city is Tirana and age group is 18-24. States in "about" section it is sponsored by EUCOM. It has gone from 100,000 fans in 2011 to 500,000 now. Posts are almost all articles, some of which get 100s of likes and and up to 100 comments. It is an active community but small enough that comments are worthwhile
Twitter	@sabahionline (eng), 1,298 followers; @sabahisomali (somali) -101 followers, @sabahiarabic (arabic) - 42 followers, no interaction, just tweets short snippets of news, sometimes without links.	@setimes, 2,186 followers. Justs tweets articles with no replies
YouTube	no	42 Subscribers, 61 videos, very few with more than 500 views.

COCOM - Program Name	ed Voice	NORTHCOM - Clear Voice
Regional News Websites	SES Turkey	Agora Revista
URL	www.turkey.setimes.com	www.agorarevista.com
Languages	Turkish, English	Spannish (NO english)
Region	Turkey	Mexico and other spannish-seaking South American countries though they are outside NORTHCOM
Attribution	"sponsored by the US European Command" in "About this site" section	"Sponsored by NORTHCOM" in the "About Us" section
Dates (from Archives)	08/2011-present	2009-present
Contractors	General Dynamics IT	General Dyanmics IT
Alexa Ranking - Country as % of Traffic/Populatrity of site in that country	sub-domain of SETimes (hence large Turkish audience for that)	n/a
Volume of stories	50-60 news stories a month, these are longer stories rather than short headlines	Is a website which supports a regional magazine "For defence and security professionals". 2-5 stories a month from the magzine focussing on military cooperationa and regional security/counter-narcotics
Content of stories - Short Notes	Publishes only medium-length features, all written by Turkish authors. They cover Turkish-Armenian relations, Turkish media, Turkish regional cooperation, gender, cultural and herritage issues. Tends to be 'big picture' analysis which discuss emerging trends or debates rather than hard news - likely because these types of articles catalyse discussion more than straight-up news stories.	n/a
Other features	no	Download all past editions of the magazine
Interactive elements in news stories	Has internal comments but like the SETimes you need to register, which have usually less than 5, also has a like/dislike voting system on the articles which rarely has more than 10 reponses	Internal comments, though very rarely any actvity.
Social Media links	Tweet and recommend on Facebook buttons which generally only have between 0 and 10.	A "like" button which is used very infrequently

Measurements of Popularity		
Facebook - All social media analysis done 11-13/02/2014	Yes, 413,191 likes (Turkish). Most popular in Istanbul and amongst 18-24 year olds. Says it is part EUCOM in about section. Very active page - 50-100 likes within hours of posting links to articles, some with 100s more. Healthy comments threads with most less than 50.	no
Twitter	@SesTurkiye, 548 followers. Just tweets articles, no replies	no
YouTube	no	no

COCOM - Program Name	PACCOM - Reliant Voice	
Regional News Websites	Khabar South Asia	Khabar South East Asia
URL	www.khabarsouthasia.com	www.khabarsoutheastasia.com
Languages	English, Urdu, Bengali	English, Bahasa Indonesian
Region	India, Sri Lanka, Bangladesh, Pakistan, Maldives, Nepal, Bhutan,	Indonesia, Brunei, Malaysia, Phillipines, Myanmar, Thailand, Cambodia
Attribution	"Sponsored by US Pacific Command" in "About Us" section	"Sponsored by US Pacific Command" in "About Us" section
Dates (from Archives)	12/2011-present	12/2011-present
Contractors	General Dynamics IT	General Dynamics IT
Alexa Ranking - Country as % of Traffic/Populatrity of site in that country	Bangladesh: 69.9%: **1,414;** India: 17.4%: 118,278	Indonesia: 83.3%: 8,788
Volume of stories	58 short "news briefs" and with 20 longer features articles a month	40 short "news briefs" with 18 longer features articles a month
Content of stories - Short Notes	"News Briefs" are 5-10 sentences long, based on reports from local and global media (AFP, Times of India, Dhaka Tribune) and press releases by officials (though these are probably secondary from other media too). Cover incidents of violence (Maoists and Islamists), poltical developments (policies, elections, etc.), and crime (notable trials, arrest). "Features" are longer and cover a variety of general interest topics: Bollywood, cricket, infrastructure projects, social issues (underage marriage, criminal justice), and more in depth politics.	"News Briefs" are 5-10 sentneces long and are based on reports from local and global media (Jakarta Post, AFP, The Jakarta Globe, Tempo). Cover the security situation in Indonesia and Philippines, inter-regional cooperation and national politics. "Features" are longer, by local journalists with a strong focus on regional and inter-cultural cooperation, such as the religious harmony of the Indonesian football team.
Other features	no	no
Interactive elements in news stories	Internal comments, the very few articles which have any rarely more than 5.	Internal comments. A few popular features articles have up to 20 comments. A like/dislike voting system which sometimes shows up to 50 or even 250 people voting on very popular articles.
Social Media links	Around 20% have 5-10 shares via Twitter or Facebook but most have less than 3.	Few news briefs have any likes or shares - those that do only 1-10 in total. Some more popilar features articles have 10-20 shares/likes.

Measurements of Popularity		
Facebook - All social media analysis done 11-13/02/2014	Yes, 37,177 likes (english only) and 427 "talking about this". "Sponsored by US Pacific Command" in "about" section. Posts every article on the site in link, most have between 0-5 likes and no comments, however some (1 in 20) have 100s of likes which suggests a latent audience of lurkers, as even these well-liked posts have few comments (usually less than 5).	Yes, 46,598 likes (english only). Says "sponsored by US Pacific Command". All articles posted in English. All posts are links to stories. Most have 0-5 likes and no comments, the most popular one I saw in the space of 8 months had 75 likes and 10 comments, which doesn't show a great degree of user involvement.
Twitter	@KhabarSouthAsia, 123 followers, no interaction	@khabarsoutheastasia (Bhasa), 149 followers, no interaction
YouTube	no	no

COCOM - Program Name		SOUTHC
Regional News Websites	Asia-Pacific Defence Forum	InfoSurHoy
URL	www.apdforum.com	www.infosurhoy.com
Languages	English, Bahasa Indonesia, Thai and Standard Chinese (Zhongwen)	English, Spannish, Portugese
Region	Covers pacific region military coperation	All of Central and South America
Attribution	"is the online version of Asia Pacific Defence Forum magazine and is sponsored by U.S Pacific Command" in "About Us" section.	"Sponsored by the US Southern Command" in "About this site".
Dates (from Archives)	Began online in 01/2009 - though this was Volume 34 Issue 3 of the magazine so obviously long-running	11/2008-present
Contractors	General Dynamics IT	General Dynamics IT
Alexa Ranking - Country as % of Traffic/Populatrity of site in that country	n/a	Costa Rica: 32.1%: **1,002**; United States: 13.8%: 309,916
Volume of stories	Features magazine articles on various regional defence issues - training excercises, procurement, etc. Also links to various AP and AFP articles on regional news.	89 "headlines" and 36 features articles in a month.
Content of stories - Short Notes	n/a	"Headlines" are 3-6 sentence articles which draw on a variety of regional news sources (AFP, El Pais (Uruguay), El Universal (Mexico), Milenio (Mexico), Reuters, EFE (Guatemala), Clarin (Argentina), El Tiempo (Colombia)). The vast majority of stories relate to the drug war, while others discuss national politics or internaitonal issues that touch on South America. "Features" cover national issues through local reproters, again there is a heavy focus on the drug war (arrests, operations against gangs, drug problems, etc), as well as stories on football, education and the environment. Focus predominatly on Central America and Colombia.
Other features	download past editions going back to 2009	no
Interactive elements in news stories	internal comments but used very rarely	internal comments not used at all on short articles. Some comments only on very occasional popular articles.
Social Media links	"Like" button used on a handful of times each article, and sometimes up to 100-200 times on very popular articles.	"Like" button used very rarely

Measurements of Popularity		
Facebook - All social media analysis done 11-13/02/2014	Yes, 11,241 likes. Posts links to articles - nothing but 1 or 2 'likes' in response to any post. Not very active	Yes, 44,095 likes (Spanish only). Says it is run by SOUTHCOM. Most of the links posted to the stories have less than 5 likes and less than 2 comments, though some do have a little more activity (up to 70 likes and 30 comments).
Twitter	@APDForum (engish), 26 followers; APDForum_th (thai) - 13; APDforum_zh (chinese) - 4 followers, no interaction.	@infosurhoy (spannish only), 352 followers, just tweets articles no interaction
YouTube	no	Yes, 18 subscribers, 30 videos, most of which have less than 1000 views, most are just to illustrate news items.

Bibliography

1st IO Command (2013), *1st Information Operations Command Homepage,* https://www.1stiocmd.army.mil (accessed 11/08/2013)

24th Air Force (2013), *24th Air Force Homepage*, http://www.24af.af.mil/index.asp (accessed 09/12/2013)

Abbasi, M., Kumar, S., Filho, J. and Liu, H. (2012), 'Lessons Learned in Using Social Media for Disaster Relief – ASU Crisis Response Game', presentation at International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction, April 2012, College Park, MD

Abdul-Ahad, G. (2013), 'How to Start a Battalion (in Five Easy Lessons)', *London Review of Books,* 35(4), pp 13-14, http://www.lrb.co.uk/v35/n04/ghaith-abdul-ahad/how-to-start-a-battalion-in-five-easy-lessons (accessed 04/09/2014)

Abdulhad, A. (2014), CV Posted on Skillpages.com, http://www.skillpages.com/administrative-assistant/balqa-jordan/abeer.abdulhade (accessed 15/09/2014)

Abraxas (2011), Job posting number 21 on K-Bar List, http://kbarlist.blogspot.co.uk/2011/01/k-bar-list-jobs-8-jan-2011.html (accessed 15/09/2014)

AbuKhalil, A. (2011), 'How to Start a Revolution: Or the Delusions of Gene Sharp', *Al Akhbar English,* 02/12/2011, http://english.al-akhbar.com/node/2169 (accessed 13/09/2014)

Ackerman. S. (2012), 'Military Intelligence Gadfly Will Lead All Military Intelligence' , *Wired – Danger Room,* 07/17/2012, http://www.wired.com/2012/04/michael-flynn-dia/ (accessed 11/09/2014)

Ackerman, S. and Ambinder, M. (2012), 'How the Pentagon's Top Killers Became (Unaccountable) Spies' , *Wired – Danger Room,* 02/13/2012, http://www.wired.com/2012/02/jsoc-ambinder/ (accessed 02/13/2012)

Aday, S., Farrell, H., Lynch, M., Sides, J. and Freelon, D. (2012), *Blogs and Bullets II: New Media and Conflict After the Arab Spring,* Washington, DC: United States Institute of Peace

Agamben, G. (2009), *What is an Apparatus?,* Stanford: Stanford University Press

Agarwal, N., Liu, H., Salrno, J. and Sundarajan, S. (2008), 'Understanding group Interaction in Blogosphere: A Case Study', paper presented at ICCCD, 2nd converence, http://www.aaai.org/Papers/ICCCD/2008/ICCCD08-002.pdf (accessed 15/09/2014)

Agarwal, N. (2009), *Social Computing in Blogosphere,* PhD Thesis at Arizona State University

Ahn, Y., Bagrow, J. and Lehmann, S. (2011), 'Link communities reveal multiscale complexity in networks', *Nature,* 1038, pp 1-5

Albro, R. (2008), 'Minerva and Critical Public Engagement', *Social Science Research Council – The Minerva Controversy,* http://essays.ssrc.org/minerva/2008/11/14/albro/ (accessed 15/09/2014)

Alexander, K. (2011), 'Building a New Command in Cyberspace', *Strategic Studies Quarterly,* Summer 2011, http://www.au.af.mil/au/ssq/2011/summer/alexander.pdf (accessed 12/09/2014)

Alexander, K. (2013), Statement of General Keith B. Alexander, Commander, United States Cyber Command before the House Committee on Armed Services, Intelligence, Emerging Threats and Capabilities Subcommittee, 13/03/2013

Al Jazeera (2011), 'Pakistanis protest against US drone strikes', *Al Jazeera English,* 22/05/2011, http://www.aljazeera.com/news/asia/2011/05/201152262955326528.html (accessed 25/09/2012)

Al Jazeera (05/02/2011), 'Tunisian protester dies of burns', http://www.aljazeera.com/news/africa/2011/01/201115101926215588.html (accessed 13/09/2014)

Al Jazeera (11/08/2013), 'How to reduce crime in the world's most violent country', http://www.aljazeera.com/indepth/opinion/2013/08/2013810135741207607.html (accessed 25/09/2014)

Alonso, P. (2012), 'Twitter: The New Frontline in Global Cyber-Jihad', *Owni.eu,* 10/01/2012, http://owni.eu/2012/01/10/twitter-the-new-frontline-in-global-cyber-jihad-al-qaeda-somalia/ (accessed 25/09/2012)

Al-Shorfa (30/11/2010), 'US military hands over Imam Ali Airbase', http://mawtani.al-shorfa.com/en_GB/articles/iii/features/iraqtoday/2010/12/01/feature-01 (accessed 13/09/2014)

Al-Shorfa (04/11/2013a), 'Kurdish figher rout jihadists across Syria's northeast', http://al-shorfa.com/en_GB/articles/meii/newsbriefs/2013/11/04/newsbrief-03 (accessed 13/09/2014)

Al-Shorfa (04/11/2013b), "Jabhat al-Nusra steals formula destined for Syrian babies', http://al-shorfa.com/en_GB/articles/meii/features/2013/11/04/feature-02 (accessed 13/09/2014)

Al-Shorfa (08/11/2013), 'Al-Qaeda affiliate execute nurse in Syria's al-Raqa', http://al-shorfa.com/en_GB/articles/meii/newsbriefs/2013/11/08/newsbrief-05 (accessed 13/09/2014)

Al-Shorfa (14/11/2013), 'Al-Qaeda recruiting children, orphans in Syria', http://al-shorfa.com/en_GB/articles/meii/features/2013/11/14/feature-01 (accessed 25/09/2014)

Al-Shorfa (19/11/2013), 'Al-Qaeda affiliate struggles to re-establish control in Syria: analysis', http://al-shorfa.com/en_GB/articles/meii/features/2013/11/19/feature-02 (accessed 13/09/2014)

Al-Shorfa (21/11/2013), 'Syria extremists impose dress code at schools', http://al-shorfa.com/en_GB/articles/meii/newsbriefs/2013/11/21/newsbrief-02 (accessed 21/11/2013)

Al-Shorfa (26/11/2013), 'Iraqi forces destroy 2 al-Qaeda camps near Syria', http://al-shorfa.com/en_GB/articles/meii/newsbriefs/2013/11/26/newsbrief-05 (accessed 25/09/2014)

Al-Shorfa (27/11/2013a), 'Iraqi forces arrest 2 al-Qaeda suspects in Mosul', http://al-shorfa.com/en_GB/articles/meii/newsbriefs/2013/11/27/newsbrief-08 (accessed 25/09/2014)

Al-Shorfa (27/11/2013b), 'Iraqi forces stop gunmen infiltrating from Syria', http://al-shorfa.com/en_GB/articles/meii/newsbriefs/2013/11/27/newsbrief-02 (accessed 25/09/2014)

Altman, A. (2013), 'Socom web initiative on Senate chopping block, *The Tampa Tribune,* 08/12/2013, http://tbo.com/list/military-news/socom-web-initiative-on-senate-chopping-block-20131208/ (accessed 13/09/2014)

Ambinder, M. (2010), 'Original Document: Making PYSYOPS Less Sinister', *The Atlantic,* 30/06/2010, http://www.theatlantic.com/politics/archive/2010/06/original-document-making-psyops-less-sinister/58947/ (accessed 11/09/2014)

Ambinder, M. and Grady (2012), *The Command: Deep Inside the President's Secret Army,* Hoboken, NJ: John Wiley & Sons

Amnesty International (2013), 'Latest detention underlines Algeria's ongoing harassment of activists', *Amnesty International News,* 04/01/2013, http://amnesty.org/en/news/latest-detention-reveals-algerias-ongoing-repression-2013-01-04

Amr, T. (2011), 'Egypt: Gene Sharp Taught Us How To Revolt!", *Global Voices,* 15/04/2011, http://globalvoicesonline.org/2011/04/15/egypt-gene-sharp-taught-us-how-to-revolt/ (accessed 13/09/2014)

al-Zawahiri, A. (2005), Letter to Abu Musab al-Zarqawi, October 2005, http://fas.org/irp/news/2005/10/letter_in_english.pdf (accessed 04/09/2014)

Anand, S. (2011), 'From Abbottabad, Live-Tweeting the Bin Laden Attack', *The Wall Street Journal,* 13/08/2012, http://blogs.wsj.com/indiarealtime/2011/05/02/from-abbottabad-live-tweeting-the-bin-laden-attack/ (accessed 25/09/2012)

Armistead, L. (ed.) (2004), *Information Operations: Warfare and the Hard Reality of Soft Power,* Dulles: Brassey's Inc

Armistead, L. (ed.) (2007), *Information Warfare: Separating Hype from Reality,* Washington, DC: Potomac Books

Army Human Terrain System (2014), 'Welcome to the Human Terrain System', Homepage, http://humanterrainsystem.army.mil/ (accessed 15/09/2014)

Arquilla, J. and Ronfeldt, D. (1997), *In Athena's Camp: Preparing for Conflict in the Information Age,* Santa Monica: RAND Corporation

Arquilla, J. and Ronfeldt, D. (2001), *Networks and Netwars,* Santa Monica, California: RAND Corporation

Arquilla, J. (2013), 'How to Protect Yourself from the Online Axis of Evil: What has happened to the notion of cyberdefense?', *Foreign Policy,* June 2013, http://www.foreignpolicy.com/articles/2013/06/10/how_to_protect_yourself_from_the_online_axis_of_evil (accessed 04/09/2014)

ARSOF 2022 (2013), ARSOF 2022, 'US Army Special Operations Command', *Special Warfare,* 26(2), special insert

Asher, T. (2008), 'Making Sense of Minerva Controversy and the NSCC', *Social Science Research Council – The Minerva Controversy,* http://essays.ssrc.org/minerva/files/2008/10/asher.pdf (accessed 15/09/2014)

ASU News (2013), 'Faculty Achievement Service Award, Honoree: Steven R Corman', *Arizona State University News,* 21/02/2013, http://alumni.asu.edu/events/founders-day/honorees/faculty-achievement-service-award (accessed 15/09/2014)

ASU – *Past Projects* (2014), Projects: "Towards narrative Disruptors and Indicators: Mapping the Narrative Comprehension Network and its Persuasive Effects', *Arizona State University Website,* http://csc.asu.edu/projects/ (accessed 15/09/2014)

Atlantic (14/12/2012), 'Why Turkey's Prime Minister Can't Stand His Country's Top Soap Opera', *The Atlantic Monthly,* http://www.theatlantic.com/international/archive/2012/12/why-turkeys-prime-minister-cant-stand-his-countrys-top-soap-opera/266274/ (accessed 25/09/2014)

Atzori, L., Iera, A., and Morabito, G. (2010), 'The Internet of Things: A Survey', *Computer Networks,* 54, pp 2787-2805

Auer, M. (2011), 'The Policy Science of Social Media', *Policy Studies Journal,* 39(4), pp 709-736

Axe, D. (2012), 'Clinton Goes Commando, Sells Diplomats as Shadow Warriors', *Wired – Danger Room,* 24/05/2012, http://www.wired.com/dangerroom/2012/05/clinton-goes-commando/ (accessed 15/09/2014)

Bakir, V. (2010), *Sousveillance, Media and Strategic Political Communication: Iraq, USA, UK,* London: Continuum

Bamford, J. (2005), 'The Man Who Sold the War: Meet John Rendon, Bush's general in the propaganda war', *Rolling Stone,* 18/11/2005

Bangladesh Chronicle (03/04/2012), 'The Pentagon's Southasia', http://www.bangladeshchronicle.net/index.php/2012/04/the-pentagons-southasia/ (accessed 13/09/2014)

Bangladesh Watchdog (15/08/2013), 'Religion and after: Bangladeshi identity since 1971', http://bangladeshwatchdog.blogspot.de/2013_08_01_archive.html (accessed 13/09/2014)

Barbier, G. and Liu, H. (2011), 'Information Provenance in Social Media', Salerno, J., Jay Yang, S., Nau, D., Chai, S. (eds), *Social Computing, Behavioural-Cultural Modeling and Prediction,* 4th International Conference, March 2011, Proceedings, SPB 2011 Lecture Notes in Computer Science 6589, London: Springer

Barnard-Wills, D. and Ashenden, D. (2012), 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk', *Space and Culture,* 15(2) pp110-12

Barnes, T. (2008), 'Geography's underworld: The military-industrial complex, mathematical modeling and the quantitative revolution', *Geoforum,* 39, pp 3-16

Baudrillard, J. (1995), *The Gulf War Did Not Take Place,* Indiana: Indiana University Place

BBC (07/08/2013), 'Lebanon: Syrian conflict 'causes slump', http://www.bbc.co.uk/news/blogs-news-from-elsewhere-23602890 (accessed 13/09/2014)

BBC (23/11/2013), 'Mauritania holds elections despite opposition boycott', http://www.bbc.co.uk/news/world-africa-25065023 (accessed 13/09/2014)

Beaumont, C. (2008), 'Mumbai attacks: Twitter and Flickr used to break news', *The Telegraph,* 27/11/2008, http://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html (accessed 25/09/2012)

Béen, D. (2013), 'Guest Speakers – Brig Gen David Béen', in Canna, S. and Popp, G. (eds.), *Over a Decade into the 21st Century…What Now? What Next?, Strategic Multilayer Assessment, 7th Annual Conference Proceedings,* Washington, DC: NSI

Belfiore, M. (2010), *The Department of Mad Scientists: How DARPA Is Remaking Our World, from the Internet to Artificial Limbs,* New York: Harper-Collins

Belk, R. and Noyes, M. (2012), *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy,* Washington, DC: Office of Naval Research

Belknap, M. (2002), 'The CNN Effect: Strategic Enabler or Operational Risk', *Parameters,* Autumn, 2002

Belov, N., Patti, J., Wilzoz, S. , Almanzar, R., Kim, J., Kellogg, J. and Dang, S. (2010), 'Exploring the Human Fabric through an Analyst's Eyes', in Chai, S., Salerno, J. and Maybry, P. (eds.), *Advances in Social Computing, Proceedings of Third International Conference on Social Computing, Behavioural Modeling, and Prediction,* SBP 2010, Lecture Notes in Computing Science 6007, London: Springer

Ben Gharbia, S. (2010), 'The Internet Freedom Fallacy and the Arab Digital activism', *Sami Ben Gharbia's Blog,* 17/09/10, http://samibengharbia.com/2010/09/17/the-internet-freedom-fallacy-and-the-arab-digital-activism/ (accessed 27/09/11)

Bennett, D. (2013), 'Exploring the impact of an evolving war and terror blogosphere on traditional media coverage of conflict', *Media, War & Conflict,* 6(1), pp 37-53

Bennett, W. L., Paletz, D. L. (Eds.). (1994). *Taken by storm: The media, public opinion, and U.S. foreign policy in the Gulf war.* Chicago: University of Chicago Press

Bensaada, Ahmed (2011), *Arabesque Americaine,* Montreal: Michel Brule

Benson, J. (2010), *The Use of Information Operations (IO) in Immersive Virtual Environments (IVE),* Thesis at the Naval Postgraduate School, http://edocs.nps.edu/npspubs/scholarly/theses/2010/Jun/10Jun_Benson.pdf (accessed 04/09/2014)

Bernardi, D.L., Cheong, P.H., Lundry, C., and Ruston, S.W., (2012), *Narrative Landmines: Rumors, Islamist Extremism, And The Struggle For Strategic Influence,* Rutgers UP: New Jersey

Betz, D. and Stevens, T. (2011), *Cyberspace and the State: Towards a strategy for cyber-power,* Aelphi Series 424, International Institute for Strategic Studies

Betz, D. (2008), 'The Virtual Dimension of Contemporary Insurgency and Counterinsurgency', *Small Wars & Insurgencies,* 19(4), pp 510-540, page references from extended draft version available at http://www.windsofchange.net/virtual-dimension-of-contemporary-insurgency-and-counterinsurgency.pdf (accessed 09/09/2014)

Betz, D. (2012), 'Cyberspace and Insurgency', in Rich, P. and Duyvesteyn, I. (eds.), *The Routledge Handbook of Insurgency and Counterinsurgency,* Oxon: Routledge

Beyerchen, A. (1992), 'Clausewitz, Nonlinearity and the Unpredictability of War', *International Security,* 17(3), pp 59-90

Biernatzki, W. E. (2002), 'War and Media', *Communication Research Trends,* 22(3)

Bigge, M. (2009), 'SOUTHCOM: Encouraging Social Media Experimentation', *GoverningPeople.com,* 06/05/2009, http://governingpeople.com/strategicsocial/12982/southcom-encouraging-social-media-experimentation (accessed 11/09/2014)

Biggs, R. and Feve, S. (2013), *Review of Programs to Counter Narratives of Violent Extremism: What Works and What are the Implications for Government,* London: Institute for Strategic Dialogue

BlogTracker (2014), 'BlockTrackers: Analyzing Social media for Cultural Modeling', http://www.public.asu.edu/~huanliu/projects/BlogTrackers/ (accessed 15/09/2014)

Bloomberg (28/02/2012), 'Cigarette Taxes Can Help Cure Two of Greece's Ills: Peter Orszag', *Bloomberg View,* http://www.bloombergview.com/articles/2012-02-28/cigarette-taxes-can-help-cure-two-of-greece-s-ills-peter-orszag (accessed 25/09/2014)

Boehnert, J. and Nasi, J. (2013), 'Military Information Support Operations in the Trans-Sahel', *Special Warfare,* 26(1), pp 10-13

Boguchwal, L. (2012), 'Network Science Centre at West Point: Social Network Analysis Programme', http://www.usma.edu/nsc/siteassets/sitepages/publications/lse_snap%20-%20final.pdf (accessed 15/09/2014)

Bohannon, J. (2009), 'Counterterrorism's New Tool: 'Metanetwork' Analysis', *Science,* Vol 325, 24/07/2009

Bohannon, L. (2008), *Cyberspace and the New Age of Influence,* Thesis presented at School of Advanced Air and Space Studies, Air University, Alabama

Bollier, D. (2003), *The Rise of Netpolitik: How the Internet is Changing International Politics and Diplomacy,* Washington, DC: Aspen Institute

Borg, L. (2008), *Communicating With Intent: The Department of Defense and Strategic Communication,* Incidental Paper for Harvard Center for information Policy Research, http://pirp.harvard.edu/pubs_pdf/borg/borg-i08-1.pdf (accessed 11/09/2014)

Borth, D., Ji, R., Chen, T., Breuel, T. and Chang, S. (2013a), 'Large-scale Visual Sentiment Ontology and Detectors Using Adjective Noun Pairs', http://www.ee.columbia.edu/ln/dvmm/vso/download/visual_sentiment_ontology_FINAL.pdf (accessed 15/09/2014)

Borth, D., Chen, T., Ji, R., and Chang, S. (2013b), 'SentiBank: Large-Scale Ontology and Classifiers for Detecting Sentiment and Emotions in Visual Content', http://www.ee.columbia.edu/ln/dvmm/vso/download/demo.pdf (accessed 15/09/2014)

Bostick, R. (2011), *Initiating a Cognitive Revolution: An Examination of Special Operations Military Information Support Operations,* Paper at US Army War College: Pennsylvania

Bowcott, O. (2011), 'Tzipi Livni spared war crime arrest threat', *Guardian.co.uk,* 06/10/2011, http://www.guardian.co.uk/world/2011/oct/06/tzipi-livni-war-crime-arrest-threat (accessed 25/09/2012)

Boyer, D. (2011), 'Biopower: Biopower and Cyberpower in Online News', in Mascia-Lees, F. (ed.), *A Companion to the Anthropology of the Body and Embodiment,* Chicherster: Wiley-Blackwell

Brafman, O. and Becksrom, R. (2006), *The Spider and the Starfish: The Unstoppable Power of Leaderless Organizations,* London: Penguin Books

Braman, S. (2006), *Change of State: Information, Policy, and Power,* Cambridge, MA: MIT Press

Bratich, J. (2011), 'Kyber-Revolts: Egypt, State-friended Media, and Secret Sovereign Networks', *The Media commons Project,* April 2011, http://mediacommons.futureofthebook.org/tne/pieces/kyber-revolts-egypt-state-friended-media-and-secret-sovereign-networks (accessed 04/09/2014)

Brecher, B, (2007), *Torture and the Ticking Bomb,* Oxford: Blackwell

Breiger, R., Ackerman, G., Asal, V., Melamed, D., Milward, H., Rethemeyer, R., and Schoon E. (2011), 'Application of a Profile Similarity Methodology for Identifying Terrorist Groups That Use or Pursue CBRN Weapons', in Salerno, J., Jay Yang, S., Nau, D., Chai, S. (eds.), *Social Computing, Behavioural-Cultural Modeling and Prediction,* 4th International Conference, March 2011, Proceedings, SPB 2011 Lecture Notes in Computer Science 6589, London: Springer

Bright, J. (2010), 'Security, Technology and Control: Repositioning Securitisation Theory for the Information Society', paper presented at SGIR 7th Pan-European Conference, Stockholm, 2010

Bright, P (2011), 'Anonymous speaks: the inside story of the HBGary hack', *ArsTechnica,* 16/02/2011, http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/ (accessed 04/09/2014)

Briscoe, E., Appling, S., Mappus IV, R., Hayes, H. (2013), 'Determining Credibility from Social Structure', https://dl.dropboxusercontent.com/u/39515687/Briscoe_Credibility_ASONAM.pdf (accessed 15/09/2014)

Bronner, R. and Richards, A. (2008), 'Integrating Multi-Agent Technology with Cognitive Modeling to Develop an Insurgency Information Framework', in Liu, H., Salerno, J. and Young, M. (eds), *Social Computing, Behavioral Modeling, and Prediction,* Proceedings of 1st Conference, London: Springer

Brooke, H. (2006), *Your Right to Know: A Citizens Guide to the Freedom of Information Act,* London: Pluto

Brooks, R. (2011), 'Ten Years On: The Evolution of Strategic Communication and Information Operations since 9/11', prepared statement of testimony before the House Armed Services Sub-Committee on Evolving Threats and Capabilities, 12/07/2011, http://armedservices.house.gov/index.cfm/files/serve?File_id=467e4788-5b39-4c86-98d1-34bc6f43610b (accessed 11/09/2014)

Brown, J (2012), *Improving Nonlethal Targeting: A Social Network Analysis Method for Military Planners,* Thesis at Naval Postgraduate School, http://www.dtic.mil/dtic/tr/fulltext/u2/a573815.pdf (accessed 15/09/2014)

Brown, R. (2003) 'Spinning the War: Political Communications, Information Operations and Public Diplomacy in the War on Terrorism', in Miller, D. (ed.) (2003), *Tell Me Lies: Propaganda and Media Distortion in the Attack on Iraq,* London: Pluto

Brown, W. (2006), 'Power After Foucualt', in Dryzek, J., Honig, B. and Philips, A. (eds.), *The Oxford Handbook of Political Theory,* Oxford: Oxford University Press

Brunner, E. and Dunn Cavelty, M. (2009), 'The formation of in-formation by the US military: articulation and enactment of infomanic threat imaginaries on the immaterial battlefield of perception', *Cambridge Review of International Affairs,* 22(4), pp 629-646

Bureau of Investigative Journalism (2014), 'Somalia: reported US covert actions 2001-2014', http://www.thebureauinvestigates.com/2012/02/22/get-the-data-somalias-hidden-war/ (accessed 09/09/2014)

Burgstein, A. (2014), 'You Can't Win If You Don't Play: Communication – Engage Early, Engage Often', *Air & Space Power Journal,* Jan-Feb 2014, pp 45-67

Burke, J (2011), *The 9/11 Wars,* London: Penguin

Burrell, R. (2013), 'Joint Doctrine for Unconventional Warfare', *Air Land Sea Bulletin,* 2013(1), pp 4-8

Business Insider (09/12/2011), Following the cocaine trail: How the white powder gets into American hands', http://www.businessinsider.com/cocaine-facts-2011-12?op=1 (accessed 25/09/2014)

Business Insider (29/10/2012), 'The Extremist Golden Down Party Is Stoking a Religious Frenzy in Greece', http://www.businessinsider.com/golden-dawn-and-the-greek-orthodox-church-2012-10 (accessed 25/09/2014)

Business Insider (26/03/2013), 'See Why Cartagena Is the Hottest New Getaway in South America', http://www.businessinsider.in/See-Why-Cartagena-Is-The-Hottest-New-Getaway-In-South-America/articleshow/21031911.cms (accessed 25/09/2014)

Butkevics, J., and Hannaford, L. (2013), 'Social Media in UW', *Special Warfare,* 26(1), pp 8-9

Buttigieg, J. (1995), "Gramsci on Civil Society", *Boundary 2* Vol 22. No.3. pp 1-32

Byman, D. (2012), *Breaking the Bonds Between Al-Qa'ida and Its Affiliate Organizations,* Washington, DC: Saban Center at Brookings, http://www.brookings.edu/~/media/research/files/papers/2012/7/alqaida%20terrorism%20byman/alqaida%20terrorism%20byman.pdf (accessed 04/09/2014)

Cabayan, H. (2013), 'Workshop Introduction – SMA Overview', in Canna, S. and St. Clair, C. (eds.), *A World in Transformation: Challenges and Opportunities, Strategic Multilayer Assessment, 6th Annual Conference Papers,* Washington, DC: NSI

Cabayan, H., Casebeer, W., DiEuliis, D., Giordano, J. and Wright, N. (eds.) (2014), *White paper on Leveraging Neuroscientific and Neurotechnological (NeuroS&T) Developments with Focus on Influence and Deterrence in a Networked World,* Washington, DC: Joint Chiefs of Staff

Caldwell IV, W. B. (2009), 'Lieutenant General William B. Caldwell IV on New Media in Military Operations: An Interview with Commander of the US Army's Combined Arms Center and Fort Leavenworth Kansas', *IOSphere,* Summer 2009, pp 24-27

Caldwell IV, W. B., Murphy, D. M., and Menning, A. (2009), 'Learning to Leverage New Media: Israeli Defence Forces in Recent Conflicts', *Military Review,* May-June 2009, pp2-10

Canada Star (02/10/2013), 'Canadian brothers jailed in Somaliland maintain innocence', http://www.thestar.com/news/canada/2013/10/02/canadian_brothers_jailed_in_somaliland_maintain_innocence.html (accessed 13/09/2014)

Canna, S. (ed.) (2013), *Operational Relevance of Behavioral & Social Science to DOD Missions,* Washington, DC: NSI

Canna, S. and St. Clair, C. (eds.) (2012), *A World in Transformation: Challenges and Opportunities, Strategic Multilayer Assessment, 6th Annual Conference Papers,* Washington, DC: NSI

Carley, K. (2005), 'Dynamic Network Analysis for Counter-Terrorism', http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.137.9475 (accessed 15/09/2014)

Carley, K. (2008), 'Advances and Challenges in Dynamic Network Analysis', http://www.mors.org/UserFiles/file/meetings/08es/carley.pdf (accessed 15/09/2014)

Carley, K. (2014), CV, http://www.casos.cs.cmu.edu/bios/carley/KCvita2014_v6.pdf (accessed 15/09/2014)

Carley, K., Pfeffer, J., Liu, H., Morstatter, F., and Goolsby, R. (2013), 'Near Real Time Assessment of Social media using Geo-Temporal Network Analytics', http://www.public.asu.edu/~fmorstat/paperpdfs/asonam2013.pdf (accessed 15/09/2014)

Carpenter, M. and Stajkovic, A., (2006), 'Social network theory and methods as tools for helping business confront global terrorism: capturing the case and contingencies presented by dark social networks', in Suder, G. (ed.) *Corporate strategies under international terrorism and adversity*, Cheltenham: Edward Elgar

Carr, M. (2013), 'Internet freedom, human rights and power', *Australian Journal of International Affairs,* 67(5), pp 621-637

CASOS (2013), Kenya Election Analysis – Key Entity Report, http://www.casos.cs.cmu.edu/projects/kenya/reports/Key_Entities_2013/index.html (accessed 15/09/2014)

Castells, M. (1996, second edition, 2000),*The Rise of the Network Society, The Information Age: Economy, Society and Culture Vol. I*. Oxford: Blackwell

Castells, M. (2009), *Communication Power,* Oxford University Press: Oxford

Central Asia Online (10/03/2011), 'Tajik women pressured to wear hijab', http://centralasiaonline.com/en_GB/articles/caii/features/main/2011/03/10/feature-01 (accessed 26/09/2014)

Central Asia Online (25/10/2012), 'Taliban's attacks on children jeopardise Pakistan's future', http://centralasiaonline.com/en_GB/articles/caii/features/pakistan/main/2012/10/25/feature-01 (accessed 26/09/2014)

Central Asia Online (13/06/2013), 'Tajiks pass anti-money-laundering bill', http://centralasiaonline.com/en_GB/articles/caii/newsbriefs/2013/06/13/newsbrief-11 (accessed 26/09/2014)

Central Asia Online (19/08/2013), 'Bomb Disposal Squad moulds 'unsung heroes' in fight against terrorism', http://centralasiaonline.com/en_GB/articles/caii/features/pakistan/main/2013/08/19/feature-01 (accessed 26/09/2014)

Central Asia Online (10/09/2013), 'Balochistan militants targeted in Pakistani operations', http://centralasiaonline.com/en_GB/articles/caii/features/pakistan/main/2013/09/10/feature-01 (accessed 26/09/2014)

Central Asia Online (07/11/2013), 'Iranian influence in Afghanistan alarms analysts', http://centralasiaonline.com/en_GB/articles/caii/features/pakistan/main/2013/11/07/feature-01 (accessed 26/09/2014)

Central Asia Online (14/11/2013a), 'Islamic writers strive to disseminate peaceful message', http://centralasiaonline.com/en_GB/articles/caii/features/pakistan/main/2013/11/14/feature-01 (accessed 25/09/2014)

Central Asia Online (14/11/2013b), 'Kyrgyzstan improves inter-ethnic relations', http://centralasiaonline.com/en_GB/articles/caii/features/main/2013/11/14/feature-01 (accessed 25/09/2014)

Central Asia Online (21/11/2013), 'Taliban deceive boys into becoming suicide bombers', http://centralasiaonline.com/en_GB/articles/caii/features/pakistan/main/2013/11/21/feature-01 (accessed 13/09/2014)

Central Asia Online (25/11/2013), 'Kyrgyzstan calls on youth to resist extremist incitement', http://centralasiaonline.com/en_GB/articles/caii/features/main/2013/11/25/feature-01 (accessed 25/09/2014)

Central Asia Online (27/11/2013), 'Pakistani ex-radicalised youths turn back on extremism', http://centralasiaonline.com/en_GB/articles/caii/features/pakistan/main/2013/11/27/feature-01 (accessed 25/09/2014)

Chai, S., Salerno, J. and Mabry, P. (eds.), (2010), *Advances in Social Computing, Proceedings of Third International Conference on Social Computing, Behavioural Modeling, and Prediction,* SBP 2010, Lecture Notes in Computing Science 6007, London: Springer

Chang, S., Kumar, V., Gilbert, E. and Terveen, L. (2014), 'Specialization, Homophily, and Gender in a Social Curation Site: Findings from Pinterest', http://www-users.cs.umn.edu/~schang/papers/cscw14.pdf (accessed 15/09/2014)

Chen, J., Cypher, A., Drews, C. and Nichols, J. (2013), 'CrowdE: Filtering Tweets for Direct Customer Engagements', http://www.jeffreynichols.com/papers/crowde_icwsm2013.pdf (accessed 15/09/2014)

Chief of Naval Operations – *OPNAV Instruction 3434.1A* (2013), *Military Information Support Operations,* 01/03/2013

Christensen, C. (2008), 'Uploading dissonance: *YouTube* and the US occupation of Iraq', *Media, War & Conflict,* 1(2), pp 155-175

Choudhury, M., Sundaram, H., John, A. and seligmann, D.D. (2010), 'Anlaysing the Dynamics of Communication in Online Social Networks', in Furht, B., *Handbood of Social Network Technologies and Applications,* New York: Springer

Ciolek, M. (2010), 'Understanding Social Media's Contribution to Public Diplomacy: How Embassy Jakarta's Facebook Outreach Illuminates the Limitations and Potential for the State Department's Use of Social Media', *Mountainrunner.us, http://mountainrunner.us/2010/06/ciolek.html#.UGFbZs0rtWM* (accessed 12/10/10)

CJCS (Chairman of the Joint Chiefs of Staff) (2011), *Military Information Support Operations Supplement To the Joint Strategic Capabilities Plan,* 30/09/2011, Washington, DC: Office of the Joint Chiefs of Staff

Clark, C. (2013), 'Army Cyber Chief Meets Buyers In Pursuit of Faster Acquisition', *Breaking Defense,* 22/10/2013, http://breakingdefense.com/2013/10/army-cyber-chief-meets-buyers-in-pursuit-of-faster-acquisition/ (accessed 12/09/2014)

Clayton, M. (2012), 'Is State Dept. hacking Al Qaeda? Not quite, but propaganda war is fierce', *The Christian Science Monitor,* 24/05/2012, http://www.csmonitor.com/USA/Foreign-Policy/2012/0524/Is-State-Dept.-hacking-Al-Qaeda-Not-quite-but-propaganda-war-is-fierce (accessed 15/09/2012)

Clifton Moore, R. (1998), 'Hegemony, Agency, and Dialectical Tension in Ellul's Technological Society', *Journal of Communication,* Summer 1998

CNN (02/08/2013), 'Why we should keep out of Somalia's affairs', *Global Public Square Blog, CNN,* http://globalpublicsquare.blogs.cnn.com/2013/08/02/why-we-should-keep-out-of-somalias-affairs/ (accessed 13/09/2014)

CNN (06/01/2014), 'Time for U.S. to focus on Western Sahara', *Global Public Square Blog, CNN,* http://globalpublicsquare.blogs.cnn.com/2014/01/06/time-for-u-s-to-focus-on-western-sahara/ (accessed 13/09/2014)

CNN (07/01/2014), 'New terror weapon: Little girls?', http://www.cnn.com/2014/01/07/opinion/bloom-horgan-afghanistan-girl (accessed 13/09/2014)

Cole, D. (2014), 'We Kill People Based on Metadata', *New York Review of Books Blog,* 10/05/2014, http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/ (accessed 15/09/2014)

Coleman, G. (2012), 'Our Weirdnes is Free', *Triple Canoply,* http://canopycanopycanopy.com/15/our_weirdness_is_free# (accessed 25/09/2012)

Collier, S. (2009), 'Topologies of Power: Foucault's Analysis of Political Government beyond 'Governmentality'', *Theory, Culture, Society,* 26(6), pp 78-108

Collings, D. and Rohozinski, R. (2009), *Blogs & Bullets: New Media and the Warfighter,* Center for Strategic Leadership, US Army War College: The SecDev Group, http://www.carlisle.army.mil/DIME/documents/Bullets__Blogs_new_Media__warfighter-Web(20%20Oct%2009).pdf (accessed 27/09/11)

Comer, R. (2010), 'Fighting Global War on Terror Indirectly', *Defense Media Network,* 21/10/2010, http://www.defensemedianetwork.com/stories/fighting-global-war-%E2%80%93-indirectly/ (accessed 09/09/2014)

Committee on Armed Forces (2010), *DOD Appropriations Hearing for FY2011, Second Session on S.3454,* Washington, DC: US Government Printing Office

Committee on Armed Forces (2013), *Hearing on National Defense Authorisation Act for FY 2014,* March 6, 2013, Washington, DC: US Government Printing Office

Comor, E. and Bean, H. (2012), 'America's 'engagement' delusion: Critiquing a public diplomacy consensus', *International Communication Gazette,* 74(3), pp 203-220

Condit, C. M. (1994), 'Hegemony in a mass-mediated society: Concordance about reproductive technologies', *Critical Studies in Mass Communication,* 11, pp 205–230

Conover, M., Ferrara, E., Menczer, F. and Flammini A. (2013a), 'The Digital Evolution of Occupy Wall Street', *PLoS One,* 8(5)

Conover, M., Davis, C., Ferrara, E., McKelvey, K., Menczer, F. and Flammini, A. (2013b), 'The Geospatial Characteristics of a Social Movement Communication Network', *PLoS One,* 8(3)

ConStrat (2010), Archived version: 'ConStrate Awarded U.S. Central Command (US CENTCOM) Contract to Support Communication Integration and Planning', https://web.archive.org/web/20120906023432/http://constrat.net/blog/constrat-awarded-us-central-command-us-centcom-contract-to-support-communication-integration-and-planning (accessed 15/09/2010)

ConStrat (2014), LinkedIn page of ConStrat, http://www.linkedin.com/company/constrat (accessed 13/09/2014)

Conway, M. (2012), 'From Al-Zarqawi to Al-Awlaki: The Emergence and Development of an Online Radical Milieu', *CTX,* 4(2), https://globalecco.org/from-al-zarqawi-to-al-awlaki-the-emergence-and-development-of-an-online-radical-milieu (accessed 18/07/2014)

Corbett, G. (2012), 'Making the Case for PR Pros Editing Wikipedia', *Techdirt.com,* 02/02/2012, http://www.techdirt.com/articles/20120124/12113517528/making-case-pr-pros-editing-wikipedia.shtml (accessed 15/09/2014)

CORE Lab – *Facebook Post* (18/04/2014), 'CORE Lab Co-Director, LTC Glenn Johnson, providing instruction to the Uzbekistan National Military Academy, Tashkent, Uzbekistan', https://www.facebook.com/257980287583444/photos/a.257993520915454.56764.257980287583444/653339171380885/?type=1&theater (accessed 13/09/2014)

CORE Lab – *LinkedIn* (2012), Job Advertisement of Senior Lecturer, CORE Lab, http://www.linkedin.com/jobs2/view/6898693 (accessed 15/09/2014)

CORE Lab – *The Lab* (2014), Common Operational Research Environment – The Lab, http://www.npscorelab.com/the-lab/ (accessed 15/09/2014)

Corman, S. R., Trethewey, A., & Goodall, H. L., Jr. (Eds.) (2008), *Weapons of Mass Persuasion: Strategic Communication in the Struggle Against Violent Extremism,* New York: Peter Lang.

Corman, S. (ed.) (2013), *Narrating the Exit From Afghanistan,* Arizona: Center for Strategic Communication

Corman – DARPA (2011), Contract for Narrative Analysis and Narrative Neurobiology Project, DARPA-BAA-12-03

Corner, J. (2007), 'Mediated politics, promotional culture and the idea of 'propaganda'', *Media, Culture and Society,* 29, p 669

Costa, B. (2013), 'Past, Present, and Future Irregular Warfare Challenges: Private Sector Perspectives', presentation before House Armed Services Committee, Subcommittee on Intelligence, Emerging Threats and Capabilities, 28/06/2013

Costa, B. and Boiney, J. (2011), 'Social Radar', http://ftp.rta.nato.int/public//PubFullText/RTO/MP/RTO-MP-HFM-201///MP-HFM-201-03.doc (accessed 25/09/2012)

Cottle, S. (2011), 'Media and the Arab uprisings of 2011: Research Notes', *Journalism,* 12(5), pp 647-659

Cox, R. (1993), 'Gramsci, Hegemony, and Internation Relations: An Essay in Method', in Gill, S., *Gramsci, Historical Materialism and International Relations,* Cambridge: Cambridge University Press

Croser, C. (2011), *The New Spatiality of Security: Operational uncertainty and the US military in Iraq,* London: Routledge

CTTSO (Combating Terrorism Technical Support Office) (2013), *2013 Review Book,* Washington, DC: CCTSO

Cunningham, T. C. (2010), *Marching Towards the Metaverse: Strategic Communication Through New Media,* Thesis at School of Advanced Military Studies, US Army Command and General Staff College, Fort Leavenworth, 2010

Cunningham, T. C. (2010), 'Strategic Communication in the New Media Sphere, *Joint Force Quarterly* (49)

Cunningham, D., Everton, S., Wilson, G., Padilla, C. and Zimmerman, D. (2013), 'Brokers and Key Plaeyrs in the Internationalization of the FARC', *Studies in Conflict & Terrorism,* 36(6), pp 477-502

Current Events Inquiry (2011), 'From Abraxas to Ntrepid: Tracking the Pentagon's "sock puppet" operation contractor', *Current Events Inquiry,* 17/03/2011, http://ceinquiry.wordpress.com/2011/03/17/abraxas-ntrepid-corp-sock-puppet/ (accessed 15/09/2011)

Curry Jansen, Sue (1988), *Censorship: The Knot That Binds Power and Knowledge,* Oxford: Oxford University Press

Curry Jansen, S, (2008), 'Walter Lippann, Straw Man of Communication Research', in Park, D. and Pulley, J. (eds.), *The History of Media and Communication Research: Contested Memories,* New York: Peter Lang

Daily Beast (25/06/2013), 'The Brutal Fall of Brazilian Billionaire Eike Batista', http://www.thedailybeast.com/articles/2013/06/25/the-brutal-fall-of-brazilian-billionaire-eike-batista.html (accessed 25/09/2014)

Daily Beast (22/01/2014), 'Obama's Kobe Bryant-Al Qaeda Flap', http://www.thedailybeast.com/articles/2014/01/22/obama-s-kobe-bryant-al-qaeda-flap.html (accessed 13/09/2014)

Daniels, J. (2009), 'Cloaked websites: propaganda, cyber-racism and epistemology in the digital era', *New Media & Society,* 11(5), pp 659-983

DARPA (2011), Broad Agency Announcement: Social Media in Strategic Communication, DAPRA-BAA-11-64, http://www.odwyerpr.com/site_images/072011darpa-sm.pdf (accessed 15/09/2014)

DARPA – *RDT&E FY2013* (2012), DARPA FY 2013 Budget Submission, Research, Development, Test & Evaluation, Defense-Wide, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2013/budget_justification/pdfs/03_RDT_and_E/Defense_Advanced_Research_Projects_Agency_PB_2013_1%20Final.pdf (accessed 15/09/2014)

DARPA – *SMISC* (2014), Social Media in Strategic Communication, http://www.darpa.mil/Our_Work/I2O/Programs/Social_Media_in_Strategic_Communication_(SMISC).aspx (accessed 15/09/2014)

DARPA – *SMISC Factsheet* (2014), Fact Sheet: DARPA's Social Media in Strategic Communication (SMISC) Program, https://timedotcom.files.wordpress.com/2014/07/fact-sheet-7-9-14.pdf (accessed 15/09/2014)

DARPA – *SMISC List* (2014), DARPA Open Catalog – Social Media in Strategic Communication, http://www.darpa.mil/OpenCatalog/SMISC.html (accessed 15/09/2014)

DARPA – *STTR 2012.b Topics* (2012) – DARPA Small Business Technology Transfer Program Proposal Submission Instructions, http://www.acq.osd.mil/osbp/sbir/solicitations/sttr2012B/darpa12B.htm (accessed 15/09/2014)

Dartnell, M. (2006), *Insurgency Online: Web Activism and Global Conflict,* London: University of Toronto Press

Dawn (19/12/2012), 'Drones aren't the only killing machines', http://www.dawn.com/news/772474/drones-arent-the-only-killing-machines (accessed 13/09/2014)

Davies, P. (2011), 'Spies as Informants: Triangulation and Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services', *Politics,* 21(1), pp73-80

Davies, N. (2008), *Flat Earth News,* London: Chatto & Windus

Davis, K. (2012), 'Can the US military fight a war with Twitter?', *IDG News Service,* 09/11/2012, http://www.pcworld.idg.com.au/article/441549/can_us_military_fight_war_twitter_/ (accessed 15/09/2012)

Dean, M. (2010), *Governmentality: Power and Rule in Modern Society,* London: Sage

De Benedetti, C. (2012), 'Fremont man says ethnic discrimination to blame for loss of government job', *Contra Costa Times,* 16/10/2012, http://www.contracostatimes.com/ci_21778046/fremont-man-says-ethnic-discrimination-blame-loss-government (accessed 15/09/2014)

DeCanio, S. (2000), 'Beyond marxist state theory: State autonomy in democratic societies', *Critical Review: A Journal of Politics and Society*, 14(2-3), pp 215-236

Deibert, R. (2008). 'Black Code Redux: Censorship, Surveillance, and the Militarization of Cyberspace' in Boler, M. (2008), *Digital Media and Democracy: Tactics in Hard Times,* MIT Press: Cambridge, MA

De Landa, M. (1991), *War in the Age of Intelligence Machines,* Cambridge, MA: Zone

Delezue, G. (1992), 'What is a Dispostif?', in Armstrong, T.J. (ed.), *Michel Foucault Philosopher*. Hemel Hempstead: Harvester Wheatsheaf

Denzin, N. and Lincoln, Y. (1994). 'Introduction: Entering the field of qualitative research' In Denzin, N. and Lincoln, Y. (eds.), *Handbook of qualitative research*. Thousand Oaks: Sage

Der Derian, J. (2009), *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network,* London: Routledge

Der Derian, J. (2013), 'From War 2.0 to quantum war: the superpositionality of global violence', *Australian Journal of International Affairs,* 67(5), pp 570-585

Dillon, M. (2007), 'Governing Terror: The State of Emergency of Biopolitical Emergence', *International Political Sociology,* 2007(1), pp 7-28

Dillon, M. and Lobo-Guerrero, L. (2008), 'Biopolitics of security in the 21st century: an introduction', *Review of International Studies,* 34(02), pp 265-292

DOD – *Current DOD Issuances* (2014), Current DOD Issuances Search, http://www.dtic.mil/whs/directives/index.html (accessed 12/09/2014)

DOD – *Defense Strategic Guidance* (2012), *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense,* Washington, DC: DOD

DOD – *Directive 3600.1* (2013), *Information Operations,* 02/05/2013, Washington, DC: DOD, http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf (accessed 11/09/2013)

DOD – *Information Operations Roadmap* (2003), Washington, DC: DOD

DOD – *JP 2-01.3* (2009), *Joint Intelligence Preparation of the Operational Environment,* Washington, DC: Joint Chiefs of Staff

DOD - *JP 3-0* (2011), *Operations,* Washington, DC: Joint Chiefs of Staff

DOD – *JP 3-05* (2014), *Special Operations,* Washington, DC: Joint Chiefs of Staff

DOD – *JP 3-07* (2011), *Stability Operations,* Washington, DC: Joint Chiefs of Staff

DOD - *JP 3-13,* (2012), *Information Operations,* Washington, DC: Joint Chiefs of Staff

DOD – *JP 3-13.1* (2012), *Electronic Warfare,* Washington, DC: Joint Chiefs of Staff

DOD – *JP 3-13.2* (2011), *Military Information Support Operation,* Washington, DC: Joint Chiefs of Staff

DOD – *JP 3-13.4* (2012), *Military Deception,* Washington, DC: Joint Chiefs of Staff

DOD - *JP 3-16* (2010), *Public Affairs,* Washington, DC: Joint Chiefs of Staff

DOD – *JP 3-60* (2013), *Joint Targeting,* Washington, DC: Joint Chiefs of Staff

DOD – *JP 3-61* (2010), *Public Affairs,* Washington, DC: Joint Chiefs of Staff

DOD - *JP 5-0* (2011), *Joint Operation Planning,* Washington, DC: Joint Chiefs of Staff

DOD – *Joint Terminology for Cyberspace Operations* (2010), Washington, DC: Joint Chiefs of Staff

DOD – *National Military Strategy for Cyberspace Operations* (2006), Washington, DC: Chairman of the Joint Chiefs of Staff, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf (accessed 11/09/2014)

DOD – *SBIR FY12.1* (2012), *DOD SBIR FY12.1 Solicitation Selections,* http://www.dodsbir.net/selections/abs2012-1/dodabs121.htm (accessed 15/09/2014)

DOD – *Strategic Communication Joint Integrating Concept* (2009), 07/10/2009, Washington, DC: DOD

DOD – *Strategy For Operating in Cyberspace* (2011), Washington, DC: DOD

DOD – *STTR FY12.A* (2012), *DOD STTR Program Phase I Selections for FY12.A,* http://www.dodsbir.net/selections/sttr/sttr_2012A.htm (accessed 15/09/2014)

DOD – *STTR FY12.B* (2012), *DOD STTR Program Phase 1 Selections for FY12.B,* http://www.dodsbir.net/selections/sttr/sttr_2012B.htm (accessed 15/09/2014)

DOD – *QDR 2001* (2001), *Quadrennial Defense Review Report,* Washington, DC: DOD

DOD – *QDR 2010* (2010), *Quadrennial Defense Review Report,* Washington, DC: DOD

Donnelly, H. (2011), 'Social Networking for Software Development', *Military Information Technology,* 15(3), pp 10-12

Downey, J. and Murdock, G. (2003), 'The counter-revolution in military affairs: the globalizations of guerilla warfare', in Thussu, D. and Freedman, D. (eds.), *War and the Media: Reporting Conflict,* London: Sage

Drame, M. (2014), CV posted on ResumeBucket.com, http://www.resumebucket.com/dramemb (accessed 15/09/2014)

DSB (Defense Science Board) (2008), *Challenges to Military Operations in Support of U.S. Interests, Volume II, Main Report,* Washington, DC: Office for the Under Secretary of Defense for Acquisition, Technology, and Logistics

DSB (Defense Science Board) (2009), *Report of the Defense Science Board Task Force on Understanding Human Dynamics,* Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics

Dudas, P. (2012), 'Cooperative, Dynamic Twitter Parsing and Visualization for Dark Network Analysis', https://www.ideals.illinois.edu/bitstream/handle/2142/39982/295.pdf?sequence=2 (accessed 15/09/2014)

Duffield, M. (2011), 'Environmental Terror: Uncertainty, Resilience and the Bunker', *School of Sociology, Politics and International Studies: Working Paper No. 06-11*

Duncan, K. (2013), *Assessing the Use of Social Media in a Revolutionary Environment,* Thesis at the Defense Analysis Department of the Naval Postgraduate School, Monterrey, June 2013

Dunn Cavelty, M. and Brunner, E. (2007), 'Introduction: Information, Power, and Security – An Outline of Debates and Implications', in Dunn Cavelty, M., Mauer, V., and Krishna-Hensel, S.F. (2007), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace,* Aldershot: Ashgate

DVIDS (2011), 'News: COL Reginald Bostick takes command of 4th Military Information Support Group (A)', *Defense Video & Imagery Distribution System,* 08/03/2011, http://www.dvidshub.net/news/98921/col-reginald-bostick-takes-command-4th-military-information-support-group#.UwSslRZrFjE (accessed 13/09/2014)

DVIDS (2012), 'Images: MISOC (Airborne)(Provisional) soldiers attend JRTC', *Defense Video & Imagery Distribution System,* 21/10/2012, http://www.dvidshub.net/image/764845/misoc-airborneprovisional-soldiers-attend-jrtc#.UwstaBZrFjE (accessed 09/09/2014)

DVIDS (2013), 'News: Kazahstani officers visit the 4th MISG (A)', *Defense Video & Imagery Distribution System,* 09/05/2013, http://www.dvidshub.net/news/106660/kazakhstani-officers-visit-4th-misg#.UwSgcBZrFjE (accessed 13/09/2014)

Dyer-Whitheford, N. (2004), 'Autonomist Marxism and the Information Society', *Multitudes*, http://multitudes.samizdat.net/Autonomist-Marxism-and-the.html (accessed 25/09/2012)

Echevaria II, A. J. (2008), *Wars of Ideas and The War of Ideas,* California: Strategic Studies Institute

Economist (31/09/2010), 'News from the east', *Eastern Approaches – Ex-Communist Europe,* http://www.economist.com/blogs/easternapproaches/2010/08/eastern_european_english-language_news_sources (accessed 25/09/2014)

Edwards, M. (2014), 'Polio resurgence in Pakistan following backlash from CIA vaccination ruse in hunt for Osama bin Laden', *ABC News,* 27/05/2014, http://www.abc.net.au/news/2014-05-27/polio-resurges-as-health-emergency-in-pakistan/5478144 (accessed 13/09/2014)

Efaw, J. (2009), 'Social networking Services: The New Influence Frontier', *IOSphere,* Winter 2009, pp 4-7

Efaw, J. and Heidger, C. (2012), 'Another Tool in the Influencers Toolbox: A Case Study', *CTX,* 2(4), https://globalecco.org/97 (accessed 13/09/2014)

EFF (Electronic Frontier Foundation) (2014), FOIA: Legal Guide for Bloggers, https://www.eff.org/issues/bloggers/legal/journalists/foia (accessed 04/09/2014)

Egan, M. and Hardenberg, M. (2012), *National Security Challenges: Insights from Social, Neurobiological, and Complexity Sciences,* Strategic Multi-Layer Assessment (SMA) and U.S. Army ERDC

Ehlschlaeger, C. (ed.) (2014), *Understanding Megacities with the Reconnaissance, Surveillance, and Intelligence Paradigm,* SMA White Volume, April 2014

Elegant, R. (1981), *How to Lose a War: The Pres and Vietnam,* New York: Rowmn & Littlefield

Ellen, J., Kaina, J. and Parameswaran, S. (2012), 'Implicit Group Membership Detection in Online Text: Analysis and Applications', in Yang, S., Greenberg, A. and Endsley, M., *Social Computing, Behavioral-Cultural Modeling and Prediction*, Proceedings of 5th Conference, London: Springer

Ellul, J. (1973), *Propaganda: The Formation of Men's Attitudes*, New York: Vintage Books

Everton, S. (2012a), 'State of the Art: Contemplating the Future of Social Media, Dark Networks, and Counterinsurgency', *CTX,* 2(4), pp 66-73

Everton, S. (2012b), *Disrupting Dark Networks,* Cambridge: Cambridge UP

Ewen, S. (1996), *PR!: A Social History of Spin,* New York: Basic Books

Executive Office of the President (2013), 'Statement of Administration Policy: S.1197 National Defense Authorization Act for FY 2014', 18/11/2013

FBO – CENTCOM (2008), Information Operations & Public Affairs, Solicitation number: 03062008, https://www.fbo.gov/index?s=opportunity&mode=form&id=b87e7d8631c4cca2a902a2b2d72c0321&tab=core&_cview=0 (accessed 15/09/2014)

FBO – CENTCOM (2010), Persona Management Software, Solicitation number: RTB220610, https://www.fbo.gov/index?s=opportunity&mode=form&id=d88e9d660336be91552fe8c1a51bacb2&tab=core&tabmode=list&= (accessed 15/09/2010)

FBO – DARPA (2011), Social Media In Strategic Communication, Solicitation No: DAPRA-BAA-11-64, https://www.fbo.gov/index?s=opportunity&mode=form&id=6ef12558b44258382452fcf02942396a&tab=core&_cview=0 (accessed 15/09/2014)

FBO – IARPA (2011), Open Source Indicators, Solicitation No: IARPA-BAA-11-11, https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=cf2e4528d4cbe25b31855a3aa3e1e7c9 (accessed 15/09/2014)

FBO – SOCOM (2008), Solicitation Document for Trans-Regional Web Initiative, Solicitation No: H92222-09-R-0003, 30/10/2008, https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=1cd60ef2b74519e462e1c4391c43c914 (accessed 13/09/2014)

FBO – SPAWAR (2014), Psychometric Approach to Deception Detection in Social Networks, Solicitation No: N65236_SNOTE_00009330E, https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=d58236ea0d79147c7d4986f8adebe2d4 (accessed 15/09/2014)

FBO – USEUCOM (2014), Request for Information/Industry Comments on Draft PWS: Social Media Data-Mining, Localized Research, Market Audience Analysis, and Narrowcast

Engagement Requirement, Solicitation Number: W564KVSMDLRMAANE, https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=bb6ef0868d7a691af91b4992b4f241b4 (accessed 15/09/2014)

Fearon, J. and Laitin, D. (2000), 'Violence and the Social Construction of Ethnic identity', *International Organization,* 54(04), pp 845-877

Felter, J. and Fishman, B. (2007), *Al-Qa'ida's Foreign Fighters in Iraq: A First Look at the Sinjar Records,* https://www.ctc.usma.edu/v2/wp-content/uploads/2010/06/aqs-foreign-fighters-in-iraq.pdf (accessed 15/09/2014), West Point, New York: Combatting Terrorism Center

Fenton, N. (2012), 'The Internet and Social Networking', in Curran, J., Fenton, N. and Feedman, D. (eds), *Misunderstanding the Internet,* London: Routledge

Fernandez, A. (2012), Statement before the Subcommittee on Terrorism, Nonproliferation, and Trade of the Committee on Foreign Affairs, House of Representatives, Serial No, 112-164, http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg75389/html/CHRG-112hhrg75389.htm (accessed 15/09/2014)

Ferrara, E., Ashbagh, M., Varol, O., Qazvinian, V., Menczer, F. and Falmmini, A. (2013a), 'Clustering Memes in Social Media', http://www.emilio.ferrara.name/wp-content/uploads/2013/08/079_0108.pdf (accessed 15/09/2014)

Ferrara, E., Varol, O., Menczer, F, and Flammini, A. (2013b), 'Traveling Trends: Social Butterflies or Frequent Fliers', http://arxiv.org/pdf/1310.2671v1.pdf (accessed 15/09/2014)

Fielding, N. (2011), 'Operation Earnest Voice, Part III', *Circling the Lions Den Blog,* http://circlingthelionsden.blogspot.com/search/label/Operation%20Earnest%20Voice (accessed 28/11/09)

Fielding, N. and Cobain, I. (2011), 'Revealed: US spy operation that manipulates social media', *The Guardian,* 17/03/2011, http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks (accessed 04/09/2014)

Fingerhut, W. (2013), 'ARSOF Way Forward', *Special Warfare,* 26(2), pp 13-16

Fink, C., Kopecky, J., Bos, N. and Thomas, M. (2012), 'Mapping the Twitterverse in the Developing World: An Analysis of Social Media Use in Nigeria' in Yang, S., Greenberg, A. and Endsley, M., *Social Computing, Behavioral-Cultural Modeling and Prediction*, Proceedings of 5th Conference, London: Springer

Fisher, A. (2003), 'Gramsci and the New Intellectuals', *49th Parallel* (number 12)

Flickr – CCDET (2014), US Central Command Flickr Profile, https://www.flickr.com/photos/ccdet/ (accessed 15/09/2014)

Flintbox – mememe (2014), MemeME Details, http://www.flintbox.com/public/project/25185/ (accessed 15/09/2014)

Flintbox – moodminer (2014), Moodminer Details, http://www.flintbox.com/public/project/25187/ (accessed 15/09/2014)

Flintbox – pinnochio (2014), Deception Detection (Pinocchio), http://www.flintbox.com/public/project/25191/ (accessed 05/09/2014)

Flintbox – sentimedir (2014), Sentimidir Details, http://www.flintbox.com/public/project/25190/ (accessed 15/09/2014)

Flynn, M., Juergens, R. and Cantrell, T. (2008), 'Employing ISR: SOF Best practices', *Joint Force Quarterly,* 50(3), pp 56-61

Flynn, M., Pottinger, M. and Batchelor, P. (2010), *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan,* Washington, DC: Center for New American Security

Flynn, M., Sisco, J. and Ellis, D. (2012), '"Left of Bang" The Value of Sociocultural Analysis in Today's Environment', *Prism,* 3(4), pp 12-21

Flynn, M. (2012), 'Populations in their Environments: Factors Impacting the Fragility of "Peace"", Egan, M. and Hardenberg, M., *National Security Challenges: Insights from Social, Neurobiological, and Complexity Sciences,* Strategic Multi-Layer Assessment (SMA) and U.S. Army ERDC

Flynn, M. (2013), 'Preface', in Canna (ed.), *Operational Relevance of Behavioral & Social Science to DOD Missions,* Washington, DC: NSI

Fogg, B. (2002), *Persuasive Technology: Using Computers to Change What We Think and Do,* San Fransisco: Morgan Kaufmann Publishers

Ford, M. (2012), 'Finding the Target, Fixing the Method: Methodological Tensions in Insurgent Identification', *Studies in Conflict & Terrorism,* 35(2), pp 113-134

Foucault, M. (1980), 'Questions on Geography', in Crampton, J. and Elden, S., *Space, Knowledge and Power: Foucault and Geography,* Aldershot: Ashgate

Foucault, M. (1994), 'The Subject and Power', in Foucault, M., (Rabinow, P. and Rose, N. (eds.)), *The Essential Foucault,* London: The New Press

Foucault, M. (2007), *Security, Territory, Population: Lectures at the College de France 1977-78,* London: Palgrave Macmillan

Foreign Policy (2012), 'The FP Twitterati 100', *Foreign Policy,* 18/06/2012, http://www.foreignpolicy.com/twitterati100 (accessed 25/09/2012)

Foreign Policy (14/11/2013), 'The Rise and Fall of Somalia's Pirate King', http://www.foreignpolicy.com/articles/2013/11/04/the_rise_and_fall_of_somalia_s_pirate_king (accessed 13/09/2014)

Froeling, O. (1997), 'The Cyberspace "War of Ink and Internet" in Chiapas, Mexico', *The Geographical Review,* 87(2), pp 291-307

Fuchs, C. (2008), *Internet and Society: Social Theory in the Information Age,* London: Routledge

Fuchs, C. (2009), 'Some Reflections on Manuel Castlles Book "Communication Power"', *TripleC,* 7(1), pp 94-108

Fusco, V. (2010), 'Social Networking: The Silent Counterinsurgent', *Army Public Affairs & Communications,* 04/05/2010, http://www.army.mil/article/38497/Social_Networking__The_Silent_Counterinsurgent/ (accessed 15/09/2014)

Gabbay, M. (2010), 'Potential Operational uses of Rhetoric-Based Modeling of Insurgent Networks', *HSCB Newsletter No 7,* Fall 2010, pp 6-7

Gabbay, M. and Thirkill-Mackelprang, A. (2010), 'Insurgent Operational Claims and Networks', Paper presented at 2010 American Political Science Association, September 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1644714 (accessed 15/09/2014)

Gallagher, T. (2003), 'My Neighbour, My Enemy: The manipulation of ethnic identity and the origins and conduct of war in Yugoslavia', in Turton, D. (ed.), *War and Ethnicity: Global Connectons and Local Violence,* Suffolk: Boydell and Brewer

Galloway, A. and Thacker, E. (2007), *The Exploit: A Theory of Networks,* London: University of Minneapolis Press

Galula, D. (2006 [1964]), *Counterinsurgency Warfare: Theory and Practice,* Westport: Praeger Security International

Gambino, L. (2014), 'CIA will not use vaccination schemes for spying, says White House official', *The Guardian,* 20/05/2014, http://www.theguardian.com/world/2014/may/20/cia-vaccination-programmes-counterterrorism (accessed 13/09/2014)

GAO (Government Accountability Office) (2011), *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities,* Washington, DC: US Government Accountability Office

GAO (Government Accountability Office) (2013), *Military Information Support Operations: Improved Coordination, Evaluations, and Training and Equipping Are Needed,* Washington, DC: GAO – leaked and published at http://cryptome.org/2013/07/gao-13-426su.pdf (accessed 11/09/2014)

Gardner, H. (2009), 'War and the media paradox', in Karatzogiani, A. (ed.), *Cyber Conflic and Global Politcs*, London: Routledge

Gates, R. (2007), 'Landon Lecture (Kansas State university)', http://www.defense.gov/speeches/speech.aspx?speechid=1199 (accessed 11/09/2014)

Gay Stolberg, S. (2011), 'Shy U.S. Intellectual Created Playbook Used in a Revolution', *New York Times,* 16/02/2011, http://www.nytimes.com/2011/02/17/world/middleeast/17sharp.html (accessed 13/09/2014)

GCHQ (2014), 'The Art of Generation: Training for a new generation of online covert operations', leaked and published at https://firstlook.org/theintercept/document/2014/02/24/art-deception-training-new-generation-online-covert-operations/ (accessed 21/09/2014)

Geltzer, J.A. and Forest, J. (2009), 'Conclusion: Assessing the Conceptual Battlespace', in Forest, J., *Influence Warfare,* London: Preager Security International

Gentile, G. (2009), 'A Strategy of Tactics: Population-Centric COIN and the Army', *Parameters,* Autumn 2009

Gentile, G. (2011), 'Beneficial War', *Harvard International Review,* December 2011, http://hir.harvard.edu/india-in-transition/beneficial-war-0 (accessed 04/09/2014)

Giddens, A. (1990) *The Consequences of Modernity*. Stanford: Stanford University Press

Gilboa, E. (2008), 'Searching for a Theory of Public Diplomacy', *The ANNALS of the American Academy of Political and Social Science,* 2008 616:55

Gilmore, C. and Osial, R. (2011), 'The Fourth Estate is dead, long live the Fourth Estate: A New military mindset for a rapidly evolving communication environment', *Public Relations Review,* 38(2), pp 208-213

Gjelten, T. (2010), 'U.S. 'Connects The Dots' To Catch Roadside Bombers', *NPR,* 03/12/2010, http://www.npr.org/2010/12/03/131755378/u-s-connects-the-dots-to-catch-roadside-bombers (accessed 15/09/2014)

Gladwell, M. (2010), 'Small Change: Why the revolution will not be tweeted', *The New Yorker* (04/10/10), http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell (accessed 27/09/11)

Glassman, J. (2008), 'Opening Statement of James K. Glassman' at Senate Foreign Relations Committee Hearing on Nomination as Under Secretary for Public Diplomacy and Public Affairs, 30/01/2008, http://www.carlisle.army.mil/DIME/documents/Glassman%20Senate%20Confirmation.pdf (accessed 11/09/2014)

Gloria, M., McGuiness, D., Luciano, J. and Zhang, Q. (2013), 'Exploration in Web Science: Instruments for Web Observatories', http://tw.rpi.edu/media/2013/05/15/aeb0/WebSciObsv_ACM_CAMERA.pdf (accessed 15/09/2014)

Gomez-Rodrigues, M., Leskovec, J. and Schölkopf, B. (2013), 'Structure and Dynamics of Information Pathways in Online Meida', http://cs.stanford.edu/people/jure/pubs/infopath-wsdm13.pdf (accessed 15/09/2014)

Goode, E. (2012), 'With Green Beret Tactics, Combating Gang Warfare', *New York Times,* 01/05/2012, http://www.nytimes.com/2012/05/01/us/springfield-mass-fights-crime-using-green-beret-tactics.html?_r=1& (accessed 15/09/2014)

Goode, L. (2009), 'Social news, citizen journalism and democracy', *New Media & Society,* 11(8), pp 1287-1305

Goolsby, R. (2008), 'The DOD Encounters the Blogosphere', in Liu, H., Salerno, J. and Young, M. (eds), *Social Computing, Behavioral Modeling, and Prediction,* Proceedings of 1st Conference, London: Springer

Goolsby, R. (2009), 'Lifting Elephants: Twitter and Blogging in Global Perspective', in Liu, H., Salerno, J. and Young, M. (eds), *Social Computing and Behavioral Modeling,* Proceedings of 2nd Conference, London: Springer

González, R. (2013), 'Cybernetic Crystal Ball: "Forecasting" Insurgency in Iraq and Afghanistan", in Whitehead, N. and Finnström, S. (2013), *Virtual War and Magical Death,* London: Duke University Press

Gowing, Nik (2009). *'Skyful of Lies' and Black Swans: The New Tyranny of Shifting Information Power in Crises,* Oxford: Reuters Institute for the Study of Journalism

Graham, S. (2006), 'Cities and the 'War on Terror'', *International Journal of Urban and Regional Research,* 30(2), pp 255-76

Graham, S. (2010), *Cities Under Siege: The New Military Urbanism,* London: Verso

Graham, S. (2012), 'When Life Itself is War: On the Urbanization of Military and Security Doctrine', *International Journal of Urban and Regional Research,* 36(1), pp 136-155

Gramsci, A. (1998), *Prison Notebooks: Selections,* London: Lawrence and Wishart

Gray, L. (2011), 'Gene Sharp: How to Start a Revolution', *The Telegraph,* 21/10/2011, http://www.telegraph.co.uk/culture/film/filmmakersonfilm/8841546/Gene-Sharp-How-to-Start-a-Revolution.html (accessed 13/09/2014)

Greenberg, A., Kennedy, W., and Bos, N. (eds) (2013), *Social Computing, Behavioral-Cultural Modeling and Prediction,* Proceedings of 6th Conference, London: Springer

Greenwald, G. (2012), 'Correspondence and collusion between the New York Times and the CIA', *Guardian.co.uk,* http://www.guardian.co.uk/commentisfree/2012/aug/29/correspondence-collusion-new-york-times-cia (accessed 25/09/12)

Greenwald, G. (2014a), *No Place to Hide,* ebook, McClelland & Stewart, Signal

Greenwald, G. (2014b), 'How Covert Agents Infiltrate Infiltrate the Internet to Manipulate, Deceive and Destroy Reputations', *The Intercept,* 24/02/2014, https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation/ (accessed 12/09/2014)

Greenwald, G. (2014c), 'Hacking Online Polls and Other Ways British Spies Seek to Control the Internet', *The Intercept,* 14/07/2014, https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/ (accessed 12/09/2014)

Grusin, R. (2010), *Premediation: Affect and Mediality After 9/11,* Basinstoke: Palgrave Macmillan

Guerrini, F. (2014), 'How Researchers Use Social Media to Map The Conflict in Syria', *Forbes,* 15/04/1014, http://www.forbes.com/sites/federicoguerrini/2014/04/15/how-researchers-use-social-media-to-map-armed-forces-in-syria/ (accessed 15/09/2014)

Guoming, Y. (2012), 'Real-name policy clamps down on freedom to speak', *Global Times,* 14/03/2012, http://www.globaltimes.cn/NEWS/tabid/99/ID/700306/Real-name-policy-clamps-down-on-freedom-to-speak.aspx (accessed 25/09/2012)

Gupshup – CENTCOM (2012), 'Centcom Greeting' discussion thread, http://www.paklinks.com/gs/religion-and-scripture/581916-centcom-greeting-print.html (accessed 15/09/2014)

Gurman, H. (ed.) (2013), *Hearts and Minds: A People's Hisotry of Counterinsurgency,* New York: The New Press

Gusterson, H. (2008), 'Unveiling Minerva', *Social Science Research Council – The Minerva Controversy,* http://essays.ssrc.org/minerva/2008/10/09/gusterson/ (accessed 15/09/2014)

Haggerty, K. and Ericson, R. (2000), 'The surveillant assemblage', *British Journal of Sociology,* 51(4), pp 605-622

Haggerty, K. and Ericson, R. (eds.) (2006), *The New Politics of Surveillance and Visibility,* London: University of Toronto Press

Hall, S. (2001), 'Foucault: Power, knowledge and discoruse', in Wetherell, M., Taylor, S. and Yates, S. (eds.), *Discourse Theory and Practice: A Reader,* London: Sage

Halliday, F. (2010), *Shocked and Awed: How the War on Terror and Jihad and Changed the English Language,* New York: I.B. Tauris

Hammes, T. (2006), *The Sling and the Stone: On War in the 21st Century,* Minneapolis: Zenith

Hammes, T. (2009), 'Information Warfare' in David Jr., G. and McKeldin III, T. *Ideas as Weapons: Influence and Perception in Modern Warfare,* Washington, DC: Potomac Books.

Hammond, P. (2007), *Media, War, and Postmodernity,* Routledge: London

Hammond, R. and Rowell, A. (2001), *Trust us: We're the tobacco industry,* Campaign for Tobacco Free Kids/Action on Smoking and Health, http://www.ash.org.uk/files/documents/ASH_135.pdf (accessed 04/09/2014)

Hannaford, L. (2013), *Transitioning From the Out Date: Information Seeking Behavior of Junior Enlisted Army Veterans of Operation Iraqi and Enduring Freedom,* MSc thesis at College of Communication and Information, Florida State University

Hanson, E. (2008), *The Information Revolution and World Politics,* Plymouth: Rowman and Littlefield

Heidger, C. and Efaw, J. (2012), 'Another Tool in the influencer's Toolbox: A Case Study', *CTX,* 2(4), https://globalecco.org/another-tool-in-the-influencers-toolbox-a-case-study (accessed 04/09/2014).

Heffelfinger, J. (2013), 'The Risks Posed by Jihadist Hackers', *CTC Sentinel,* July 2013, https://www.ctc.usma.edu/posts/the-risks-posed-by-jihadist-hackers (accessed 04/09/2014)

Herman, E and Chomsky, N (1988), Manufacturing Consent, New York: Pantheon

Hernandez, R. (2012), *Concerning Digital Warrior: Improving Military Capabilities in the Cyber Domain,* Statement by Lieutenant General Rhett Hernandez, Commanding General, US Army Cyber Command before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, http://defenseinnovationmarketplace.mil/resources/ArmyA9R9A51.pdf (accessed 12/09/2014)

Herrerra, G. (2007), 'Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space', in Dunn Cavelty, M., Mauer, V., and Krishna-Hensel, S.F. (2007), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace,* Aldershot: Ashgate

Hier, S. (2003), 'Probing the Surveillant Assemblage: on the dialects of surveillance pratices as processes of social control', *Surveillance & Society,* 1(3), pp 399-411

Hilsum, L. (2013), 'Has France killed a top al-Qaeda commander in Mali?', *Channel 4 News – Lindsey Hilsum on International Affairs,* 28/02/2013, http://blogs.channel4.com/lindsey-hilsum-on-international-affairs/has-france-killed-top-al-qaeda-commander-in-mali/1786 (accessed 25/09/2014)

Hindman, N (2009), *The Myth of Digital Democracy,* Princeton: Princeton UP

Hirst, P. (2005), *Space and Power: Politics, War and Architecture,* London: Polity

Hjarvard, S. (2008), 'The Mediatization of Society: A Theory of the Media as Agents of Social and Cultural Change', *Nordicom Review,* 29 (2), pp 105-134

Hogg, T. and Lerman, K. (2012), 'Social Dynamics of Digg', *EPJ Data Science,* 1(5)

Hogg, T., Lerman, K., and Smith, L. (2013), 'Stochastic Models Predict User Behavior in Social Media', http://arxiv.org/pdf/1308.2705v1.pdf (accessed 15/0/2014)

Holbrooke, R. (2001), 'Get the Message Out', *Washington Post,* 28/10/2001, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/13/AR2010121305410.html (accessed 04/09/2014)

Holmes, S. (2008), 'Free-Marketeering', *London Review of Books,* 30(9)

HootSuite (2013), 'Joint HootSuite at the Social media Within the Military and Defence Sector conference', *Hootsuite.com,* 12/2013, http://blog.hootsuite.com/social-media-defence-military/ (accessed 15/09/2014)

Horn, E. 'Knowing the Enemy: The Epistemology of Secret Intelligence' (translated by Oger, S.), *Grey Room,* 11, May 2003

Horne, A. (2006), *A Savage War of Peace: Algeria 1954-1962,* London: Macmillan

Hoskins, A. and O'Loughin, B. (2010), *War and Media: The Emergence of Diffused War,* Cambridge: Polity

House Appropriations Committee – *Reprogramming Action Omnibus* (2010), FY 10-13 PA, DD 1415-1

House Committee on Armed Services - *Budget Requests from US CENTCOM, US SOCOM, and US TRANSCOM* (2012), Hearing on National Defense Authorization Act for FY 2013, Ful Committee Hearing, 07/03/2012, http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg73438/pdf/CHRG-112hhrg73438.pdf (accessed 13/09/2014)

HSCB Newsletter, No 2 (2009), *Human Social Culture Behavior Modeling Program,* Summer 2009, http://www.dtic.mil/biosys/files/HSCB-news-summer-2009.pdf (accessed 15/09/2014)

HSCB Newsletter, No 7 (2010), *Human Social Culture Behavior Modeling Program,* Fall 2010, http://www.dtic.mil/biosys/files/HSCB-news-fall-2010.pdf (accessed 15/09/2014)

HSCB Newsletter No 8 (2011), *Human Social Culture Behavior Modeling Program*, Winter 2011, http://www.dtic.mil/biosys/files/HSCB-news-winter-2011.pdf (accessed 15/09/2014)

HSCB Newsletter, No 9 (2012), *Human Social Culture Behavior Modeling Program*, Spring 2012, http://www.dtic.mil/biosys/docs/HSCB-news-spring-2011.pdf (accessed 15/09/2014)

HSCB Newsletter, No 15. (2013), *Human Social Culture Behavior Modeling Program,* Summer 2013, https://www.movesinstitute.org/2013/05/16/human-social-culture-behavior-hscb-modeling-program-may-newsletter/ (accessed 15/09/2014)

HSCB Newsletter List (2014), HSCB Modeling Program Newsletters, http://www.dtic.mil/biosys/newsletter.html (accessed 15/09/2014)

Huffington Post (19/08/2011), 'Turkey and Saudi Arabia: The Buildup to Syria', *The World Post,* http://www.huffingtonpost.com/sultan-sooud-alqassemi/turkey-and-saudi-arabia-t_b_931060.html (accessed 25/09/2014)

Huffington Post (22/01/2013), 'Brazil Favelas Find New Home on Rio De Janeiro Maps', http://www.huffingtonpost.com/2013/01/22/brazil-favelas-rio-de-janeiro_n_2528407.html (accessed 13/09/2014)

Huffington Post (10/02/2013), 'Pakistan's Top Police Bomb Disposal Squad Suffers From Severe Underfunding and Neglect', http://www.huffingtonpost.com/2013/10/02/pakistan-bomb-disposal_n_4032608.html (accessed 13/09/2014)

Hutto, C., Yardi, S. and Gilbert, E. (2014), 'A Longitudinal Study of Follow Predictors on Twitter', http://comp.social.gatech.edu/papers/follow_chi13_final.pdf (accessed 15/09/2014)

IARPA – *OSI Program* (2014) – Open Source Indictors (OSI) Program, http://www.iarpa.gov/Programs/ia/OSI/osi.html (accessed 15/09/2014)

ICCCD 2009 (2009), International Conference on Computational Cultural Dynamics – Program Committee

ICSR (International Centre for the Study of Radicalisation and Political Violence) (2012), *Lights, Camera, Jihad: Al-Shabaab's Western Media Strategy,* London; ICSR

Independent (17/05/2012), 'A bikini is not he same as a niqab', *Independent Blogs – James Bloodworth Notebook,* http://blogs.independent.co.uk/2012/05/17/a-bikini-is-not-the-same-as-a-niqab/ (accessed 25/09/2014)

Information Dominance Corps (2013), *Information Dominance Corps Overview,* http://www.usna.edu/Cyber/_files/documents/idc/IDC_Overview.pdf (accessed 12/09/2014)

InfoSurHoy (22/12/2008), 'Drug production grows in Bolivia', http://dialogo-americas.com/en_GB/articles/saii/features/2008/12/22/feature-03 (accessed 25/09/2014)

InfoSurHoy (08/08/2013), 'Honduras: New death in longstanding land conflict', http://dialogo-americas.com/en_GB/articles/saii/newsbriefs/2013/08/08/newsbrief-02 (accessed 13/09/2014)

InfoSurHoy (08/11/2013), 'Colombia: Indigenous people read, write with digital tablets', http://dialogo-americas.com/en_GB/articles/saii/features/main/2013/11/08/feature-07?change_locale=true (accessed 13/09/2014)

International Business Times (14/09/2013), 'Balochistan: Pakistan's 'Dirty War' In Its Poorest, Most Lawless, But Resource-Rich Province', http://www.ibtimes.com/balochistan-pakistans-dirty-war-its-poorest-most-lawless-resource-rich-province-1405620 (accessed 13/09/2014)

ISAF (International Security Assistance Force), *ISAF Homepage,* http://www.isaf.nato.int/ (accessed 09/11/2014)

ISC (Intelligence in Science) (2013), Social Computing and Crisis in the New Information Age conference Programme, 8-9 October, 2013, Brussels, www.iscintelligence.com/archivos.../social_computing_programme.pdf (accessed 15/09/2014)

Jacobsen, J. K. (2008), 'Why do states both to deceive? Managing trust at home and abroad', *Review of International Studies,* 34, pp 337-361

Jacobs Technology (2014), Jacobs Technology – Current Customers – Other Defense Agencies, https://www.jacobstechnology.com/socom.html#ITSMb (accessed 13/09/2014)

Jain, S. and Hovy, E. (2013), 'Determining Leadership in Contentious Discussions', http://isi.edu/~galstyan/smisc/pubs/Hovy2013.pdf (accessed 15/09/2014)

Jansson, A. (2002), 'The Mediatization of Consumption: Towards an analytical framework of image culture', *Journal of Consumer Culture,* 2(1), pp 5-31

Jefferey, S. (2004), 'New Spanish PM promises Iraq withdrawal', *Guardian.co.uk,* 15/03/2004, http://www.guardian.co.uk/world/2004/mar/15/spain.iraq (accessed 25/09/2012)

Jenkins, Henry (2008), *Convergence Culture: Where Old and New Media Collide,* New York: New York UP

Jenkins, H. (2012), 'Contextualizing #Kony2012: Invisible Children, Spreadable Media, and Transmedia Activism', *The Official Weblog of Henry Jenkins,* 12/03/2012, http://henryjenkins.org/2012/03/contextualizing_kony2012_invis.html (accessed 25/09/2012)

Jepson, K. (2014), 'Kenya's Counter-Terrorism Police Confess to Extrajudicial Killings', *Al Jazeera Investigative Unit,* 12/2014, http://interactive.aljazeera.com/aje/KenyaDeathSquads/ (accessed 11/09/2014)

Joint Force Electronic Library (2014), Joint Force Quarterly Homepage, http://www.dtic.mil/doctrine/jfq/jfq.htm (accessed 09/09/2014)

Jones, N. and Baines, P. (2013), 'Losing Control?' Social Media and Military Influence', *RUSI Journal,* 158(1), pp 72-78

Jones, M. (2014), CV 'Arabic Social Media Specialist' for Marisa Jones posted on indeed.cv, http://www.indeed.com/r/Marisa-Jones/14c3cf5e24f76d10?sp=0 (accessed 15/09/2014)

Jowett, G. and O'Donnel, V. (2006), *Propaganda and Persuasion,* Sage: London

Kalb, M. and Saivetz, C. (2007), 'The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict', *The Harvard International Journal of Press/Politics,* 2007, 12(43)

Kaempf, S. (2013), 'The mediatisation of war in a transforming global media landscape', *Australian Journal of International Affairs,* 67(5), pp 586-604

Kaldor, M. (1999), *New and old Wars: Organised violence in the global era,* Cambridge: Polity

Kang, J. and Lerman, K. (2013), 'Structural and Cognitive Bottlenecks to Information Access in Social Networks', http://arxiv.org/pdf/1303.0861v1.pdf (accessed 15/09/2014)

Kapferer, B. (2010), 'The Aporia of Power: Crisis and Emergence of the Corporate State', *Social Analysis,* 54(1), pp 125-151

Keller, J. (2010a), 'When Campaigns Manipulate Social Media, *The Atlantic,* 10/11/2010, http://www.theatlantic.com/politics/archive/2010/11/when-campaigns-manipulate-social-media/66351/ (accessed 15/09/2014)

Keller, R. (2010b), *Influence Operations and the Internet: A 21st Century Issue,* Thesis at the Air War College, http://www.au.af.mil/au/awc/awcgate/maxwell/mp52.pdf (accessed 04/04/2010)

Kelly, M. (2013), 'US Special Ops Have Become Much, Much Scarier Since 9/11', *Business Insider,* 10/05/2013, http://www.businessinsider.com/the-rise-of-jsoc-in-dirty-wars-2013-4 (accessed 11/09/2014)

Keohane, R. and Nye, J. (1998), 'Power and Interdependence in the Information Age', *Foreign Affairs,* September/October 1998

Kettler, B. (2009), 'Mixed Methods Stability Forecasting and Mitigation for the DARPA ICEWS Program', Abstract of presentation at ICCCD 2009,

http://www.umiacs.umd.edu/conferences/icccd2009/program.html#abstracts (accessed 15/09/2014)

Kezar, A. (2003), 'Transformatioal Elite Interviews: Principles and Problems', *Qualitative Inquiry,* 9 pp 395-414

Khabar South Asia (16/11/2013), 'Diwali strengthens bond between Kashmiri Pandits, Muslims, Sikhs', http://khabarsouthasia.com/en_GB/articles/apwi/articles/features/2013/11/16/feature-01 (accessed 25/09/2014)

Khabar South Asia (20/11/2013), 'Underage marriage still a scourge in India', http://khabarsouthasia.com/en_GB/articles/apwi/articles/features/2013/11/20/feature-01 (accessed 25/09/2014)

Khabar South Asia (23/11/2013), 'Amid Maoist threat, Jharkhand, Bihar become IM hotspots', http://khabarsouthasia.com/en_GB/articles/apwi/articles/features/2013/11/23/feature-03 (accessed 15/09/2014)

Khabar South Asia (27/11/2013), 'Pakistani Taliban blamed for international spread of polio virus', http://khabarsouthasia.com/en_GB/articles/apwi/articles/features/2013/11/27/feature-03 (accessed 25/09/2014)

Khabar Southeast Asia (06/11/2013), 'Truth and Reconciliation Commission discussions held in Aceh', http://khabarsoutheastasia.com/en_GB/articles/apwi/articles/features/2013/11/06/feature-02 (accessed 25/09/2014)

Khabar Southeast Asia (19/11/2013), 'Indonesia's U-19 football team displays athletic excellence, tolerance', http://khabarsoutheastasia.com/en_GB/articles/apwi/articles/features/2013/11/19/feature-04 (accessed 25/09/2014)

Khabar Southest Asia (21/11/2013), 'Doing their part to help storm victims', http://khabarsoutheastasia.com/en_GB/articles/apwi/articles/features/2013/11/21/feature-04 (accessed 25/09/2014)

Khabar Southeast Asia (22/11/2013), 'Thailand to launch 24-hour Malay TV channel', http://khabarsoutheastasia.com/en_GB/articles/apwi/articles/features/2013/11/22/feature-02 (accessed 25/09/2014)

Khabar Southeast Asia (27/11/2014), 'In Central Java, NU to open dialogue with Ahmadiyah Followers', http://khabarsoutheastasia.com/en_GB/articles/apwi/articles/features/2013/11/27/feature-06 (accessed 25/09/2014)

Khalili, L. (2013), 'The tip of the spear: US Special Operations Forces', *Al Jazeera,* 29/03/2013, http://www.aljazeera.com/indepth/opinion/2013/03/201332811912362162.html (accessed 09/09/2014)

Khatib, L., Dutton, W. and Thelwall, M. (2011), 'Public Diplomacy 2.0: An Exploratory Case Study of the US Digital Outreach Team', http://ssrn.com/abstract=1734850 (accessed 15/09/2011)

Kilcullen, D. (2005), 'Countering global insurgency', *Journal of Strategic Studies,* 28(4), pp 597-617

Kilcullen, D. (2006) 'Counterinsurgency *Redux*', http://www.au.af.mil/au/awc/awcgate/uscoin/counterinsurgency_redux.pdf (accessed 25/09/2012)

Kim, N., Gokalp, S., Davulcu, H. and Woodward, M. (2013), 'LookingGlass: A Visual Intelligence Platform for Tracking Online Social Movements', Paper at 2013 IEEE/ACM International Conference on Advances in Social Networks and Analysis and Mining, Niagara, Ontario

King, S. (2010), 'Military Social Influence in the Global Information Environment: A Civilian Primer', *Analyses of Social Issues and Public Policy,* 00(00), pp 1-26

Kinniburgh, J. and Denning, D. (2009), 'Blogs and Military Information Strategy', *IOSphere,* Summer 2006, pp 5-13

Kirby, A. and Zakem, V. (2009), 'Jihad.com 2.0: The New Social media and the Changing Dynamics of Mass Persuasion', in Forest, J. (ed.), *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas,* Connecticut: Praeger Security International

Klaehn, J. and Mullen, A. (2010), 'The Propaganda Model and Sociology: Understanding the Media and Society', *Synaesthesia Journal,* 1(1)

Klein, N. (2007), *The Shock Doctrine: The Rise of Disaster Capitalism,* London: Penguin

Knoke, D. (2012), '"It Takes a Network": The Rise and Fall of Social Network Analysis in U.S. Counterinsurgency Doctrine', *Connections,* 33(1), pp 2-10

Knopf, C. and Ziegelmayer, E. (2012), 'Fourth Generation Warfare and the US Military's Social Media Strategy: Promoting Academic Conversation', *ASPJ Africa & Francophonie, http://www.airpower.maxwell.af.mil/apjinternational/apj-af/2012/2012-4/eng/2012_4_02_Knopf-Ziegelmayer.pdf* (accessed 04/09/2014)

Kogan, B. (2014), LinkedIn.com profile of Boris Kogan, http://www.linkedin.com/pub/boris-kogan/25/461/98b (accessed 15/09/2014)

Kramer, F. and Wentz, L. (2008), 'Cyber Influence and International Security', *Defense Horizons,* January 2008 (no 61), pp 1-12

Krebs, B. (2011), 'Twitter Bots Drown Out Anti-Kremlin Tweets', *KrebsOnSecurity,* 08/12/2011, http://krebsonsecurity.com/2011/12/twitter-bots-drown-out-anti-kremlin-tweets/ (accessed 15/09/2014)

Krebs, R. (2008), 'Minerva: Unclipping the Owl's Wings', *Social Science Research Council – The Minerva Controversy,* http://essays.ssrc.org/minerva/2008/11/19/krebs/ (accessed 15/09/2014)

Krebs, V. (2002), 'Mapping Networks of Terrorist Cells', *Connections,* 24(3), pp 43-52

Kuehl, D. (2008), 'Information Operations, Information Power', presentation at National Defense University, http://www.ndu.edu/jrac/docUploaded/RCNSC-Kuehl-July2008.pdf (accessed 02/04/2014)

Kumar, S., Zafarani, R., Abbasi, M., Barbier, G. and Liu, H. (2010), 'Convergence of Influential Bloggers for Topic Discovery in the Blogosphere', in Chai, S., Salerno, J. and Mabry, P. (eds.), *Advances in Social Computing, Proceedings of Third International Conference on Social Computing, Behavioural Modeling, and Prediction,* SBP 2010, Lecture Notes in Computing Science 6007, London: Springer

Kumar, S., Barbier, G., Abbasi, M. and Liu, H. (2011), 'TweetTracker: An Analysis for Humanitarian Disaster Relief', http://arnetminer.org/publication/tweettracker-an-analysis-tool-for-humanitarian-and-disaster-relief-3294241.html;jsessionid=1CB38D3C2393F581EC80EEAF0C6E5955.tt (accessed 15/09/2014)

Kumar, S., Morstatter, F. and Liu, H. (2013), *Twitter Data Analytics,* London: Springer

Lakkaraju, H., McAuley, J. and Leskovek, J. (2013), 'What's in a name? Understanding the Interplay between Titles, Content, and Communities in Social Media', http://cs.stanford.edu/people/jure/pubs/reddit-icwsm13.pdf (accessed 15/09/2014)

Latar, N.L., Asmolov, G. and Gekkar, A. (2010), *State Cyber Advocacy,* Paper presented at Herzlia Conference, 2010, http://www.herzliyaconference.org/_Uploads/3035Newmediafinal.pdf (accessed 25/09/2012)

Lashmar, P. and Oliver, J. (1998), *Britain's Secret Propaganda War: Foreign Office and the the Cold War, 1948-77,* Stroud: Sutton Publishing

Lasswell, H. (1927), 'The Theory of Propaganda', *The American Political Science Review,* 21(3)

Lawson, S. (2008), *Info@War.Mil: Nonlinear Science and the Emergence of Information Age Warfare in the United Stated Military,* PhD Thesis in Science and Technology Studies at Rensselaer Polytechnic Institute: Troy, New York

Lawson, S. (2009), 'Surfing on the edge of chaos: Nonlinear science and the emergence of a doctrine of reventive war in the US', *Social Studies of Science,* 41(4), pp 563-584

Lawson, S. (2013), 'The US military's social media civil war: technology as antagonism in discourses of information-age conflict', *Cambridge Review of International Affairs,* DOI 10.1080/09557571.2012.734787

LeBaron, R. (2012), 'Public Diplomacy as An Instrument of Counterterrorism: A Progress Report', Remarks by Ambassador (retired) Richard LeBaron, The President's Round Table, 20/06/2012, http://mountainrunner.us/2012/06/public-diplomacy-instrument-counterterrorism/#.T-Q96s0zkV8 (accessed 15/09/2012)

Lee, Raymond (1993), *Doing Research on Sensitive Topics,* Sage: London

Lee, D. (2013), 'A Social Movement Approach to Unconventional Warfare', *Special Warfare,* 26(3), pp 27-32

Leed, M. (2013), *Offensive Cyber Capabilities at the Operational Level: The Way Ahead,*: Washington, DC: Center for Strategic & International Studies

Lehmann, T. and Young, T.R. (1974), 'From Conflict Theory to Conflict Methodology: An Emerging Paradigm for Sociology', *Sociological inquiry,* 44(1): pp 15-28

Legg, S. (2011), 'Assemblage/Apparatus: using Deleuze and Foucault', *Area,* 43(2), pp 128-133

Lerman, K., Ghosh, R., Kang, J. and Kumaraguru, P. (2013), 'Limited Attention and Centrality in Social Networks', http://arxiv.org/pdf/1303.4451v1.pdf (accessed 15/09/2014)

Lessig, L. (1999), *Code And Other Laws of Cyberspace,* New York: Basic Books

Levine, Y. (2014), 'Peeling the onion: Almost everyone involved in developing Tor was (or is) funded by the US government', *Pando Daily,* http://pando.com/2014/07/16/tor-spooks/ (accessed 18/07/2014)

L'Express (10/02/2011), 'Facebook, porte-voix des révoltes arabes', http://www.lexpress.fr/actualite/monde/facebook-porte-voix-des-revoltes-arabes_961024.html (accessed 25/09/2014)

Li, Z. (2004), 'The Potential of America's Army the Video Game as Civilian-Military Public Sphere', Masters thesis for Comparative Media Studies at MIT: Cambridge, MA.

Lianos, M. (2003), 'Social Control after Foucault', *Surveillance & Society,* 1(3) pp 412-430

Lighthouse – *About Lighthouse* (2012), About Lighthouse, http://lhproject.info/about-lighthouse/ (accessed 15/09/2014)

Lighthouse – *Collecting Data* (2011), Collecting Data Using Lighthouse, 18/12/2011, http://lhproject.info/collecting-data-using-the-lighthouse-app/ (accessed 15/09/2014)

Limnéll, J. (2013), 'Attacks in cyberspace are capable of influencing global politics', *The Guardian,* 22/07/2013, http://www.theguardian.com/media-network/media-network-blog/2013/jul/22/cyberspace-attacks-influencing-global-politics (accessed 04/09/2014)

Lind, W., Nighengale, K., Schmitt, J., Sutton, J. and Wilson, G. (1989), 'The Changing Face of War: Into the Fourth Generation', *Marine Corps Gazette,* October 1989, https://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf (accessed 09/09/2014)

Lindsay, J. (2013), 'Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations', *The Journal of Strategic Studies,* 36(3), p 422-453

Lippmann, W. (1922 [2008]), *Public Opinion,* BN Publishing

Lips, M. and Taylor J.A. (2008), 'The Citizen in the Information Polity: Exposing the Limits of the E-government Paradigm', *Information Polity* 13(3–4), pp 139–152.

Liu, H., Salerno, J. and Young, M. (eds) (2008), *Social Computing, Behavioral Modeling, and Prediction,* Proceedings of 1st Conference, London: Springer

Liu, X., Tang, K., Hancock, J., Han, J., Song, M., Xu, R. and Pokorny, B. (2013), 'A Text Cube Approach to Human, Social and Cultural Behavior in the Twitter Stream', in Greenberg, A., Kennedy, W., and Bos, N. (eds), *Social Computing, Behavioral-Cultural Modeling and Prediction,* Proceedings of 6th Conference, London: Springer

Livingston, S. and Eachus, T. (1995), 'Humanitarian crises and U.S. foreign policy: Somalia and the CNN effect reconsidered', *Political Communication,* 12(4), pp 413-429

Lockheed Martin – *ISPAN* (2014), Integrated Strategic Planning and Analysis Network, http://www.lockheedmartin.co.uk/us/products/ispan.html (accessed 15/09/2014)

Lofdahl, C., Pfautz, J., Farry, M. and Stickgold, E. (2014), 'Identifying and Understanding Trust Relationships in Social Media', in Ehlschlaeger, C. (ed.) (2014), *Understanding Megacities with the Reconnaissance, Surveillance, and Intelligence Paradigm,* SMA White Volume, April 2014

Lopacienski, E., Grieshaber, W., Carr, B., and Hoke, C. (2011), *Influence Operations: Redefining the Indirect Approach,* Thesis at Navy Postgraduate School

Lord, Carnes (2006), *Losing Hearts and Minds: Public Diplomacy and Strategic Influence in the Age of Terror,* London: Praeger Security International

Lubold, G. and Harris, S., (2014), 'Exclusive: Pentagon Withholds Internal Report About Flawed $2.7 Billion Intel Program', *Foreign Policy,* 18/03/2014, http://www.foreignpolicy.com/articles/2014/03/18/exclusive_pentagon_withholds_report_2.7_billion_intel_program (accessed 15/09/2014)

Luce, M. (2012), 'Speaker Series: "Confessional Communities in Iran and Current Trends', presentation for *Cultural Knowledge Consortium,* 19/06/2012, https://www.culturalknowledge.org/speaker-series-confessional-communities-in-iran-and-current-trends-dr-mark-luce.aspx (accessed 13/09/2014)

Lucente, S. and Wilson, G. (2013), 'Crossing the Red Line: Social media and Social Network Analysis For Unconventional Campaign Planning', *Special Warfare,* 26(3), pp 21-26

Lujan, F. (2013), *Light Footprints: The Future of American Intervention,* http://www.cnas.org/sites/default/files/publications-pdf/CNAS_LightFootprint_VoicesFromTheField_Lujan.pdf (accessed 11/09/2014), Washington, DC: CNAS,

Lukes, Steven (2005), *Power: A Radical View,* Basingstoke: Palgrave Macmillan

Lynch, M., Freelon, D. and Aday, S. (2014), *Blogs and Bullets III: Syria's Socially Mediated Civil War,* Washington, DC: United States Institute of Peace

Lyon, D. (2003), 'Technolgy vs 'Terrorism': Circuits of City Surveillance since September 11th', *International Journal of Urban and Regional Research,* 27(3), pp 666-78

Lyon, E. and Afergan, B. (2012), 'Social Media Conference Summary', *HSCB Newsletter No 13,* Summer 2012

MacAskill, E. (2010), 'WikiLeaks website pulled by Amazon after US political pressure', *Guardian.co.uk,* 02/12/2010, http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon (accessed 25/09/2012)

MacAskill, E., Pilkington, E. and Graham-Harrison, E. (2012), 'Pentagon urgest controversial Florida pastor to stop Qur'an burning plans', *Guardian.co.uk,* 20/04/2012, http://www.guardian.co.uk/world/2012/apr/20/pentagon-florida-pastor-quran-burning (accessed 25/09/2012)

MacCalman, M., MacCalman, A., and Wilson, G. (2013), 'Visualizing Social Networks to Inform Tactical Engagement Strategies that will Influence the Human Domain', *Small War Journal,* 15/08/2013, http://smallwarsjournal.com/jrnl/art/visualizing-social-networks-to-inform-tactical-engagement-strategies-that-will-influence-th?utm_source=rss&utm_medium=rss&utm_campaign=visualizing-social-networks-to-inform-tactical-engagement-strategies-that-will-influence-the-human-domain (accessed 15/09/2014)

Macdonald, S. (2007), *Propaganda and Information Warfare in the Twenty-First Century,* New York: Routledge

MacGinty, R. (2010), 'Social network analysis and counterinsurgency: a counterproductive strategy', *Critical Studies in Terrorism,* 3(2), pp 209-226

Mackay, A. and Tatham, S. (2009), *From General to Strategic Corporal: Complexity, Adaptation and Influence*, *Shrivenham Paper 9,* Shrivenham: Defence Academy of the United Kingdom

Mackinlay, J. (2009), *The Insurgent Archipelago,* London: Hurst & Co.

MacSkassy, S. (2012a), 'Characterizing Retweting Behaviors in Twitter: On the use of Text vs. Concepts', http://www.research.rutgers.edu/~sofmac/paper/ecml2012-colisd/macskassy-colisd2012-preprint.pdf (accessed 15/09/2014)

MacSkassy, S. (2012b), 'On the Study of Social Interactions in Twitter', http://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/viewFile/4575/4987 (accessed 15/09/2014)

Magharebia (02/02/2010), 'YouTube censorship roils Libyan blogosphere', http://magharebia.com/en_GB/articles/awi/blog/2010/02/02/feature-03 (accessed 13/09/2014)

Magherebia (03/01/2011), 'Tunisians question Al Jazeera protest coverage', http://magharebia.com/en_GB/articles/awi/features/2011/01/03/feature-01 (accessed 13/09/2014)

Magharebia (17/06/2011), 'Tahar Belabes: Algerian youths need motivation', http://magharebia.com/en_GB/articles/awi/features/2011/06/17/feature-02 (accessed 13/09/2014)

Magharebia (14/07/2011), 'Africom chief visits Mauritania', http://magharebia.com/en_GB/articles/awi/features/2011/07/14/feature-01 (accessed 13/09/2014)

Magharebia (07/02/2013), 'In Amenas attack magnificis Belmokhtar, AQIM rift', http://magharebia.com/en_GB/articles/awi/features/2013/02/07/feature-02 (accessed 25/09/2014)

Magharebia (23/09/2013), 'Morocco to train Malian imams', http://magharebia.com/en_GB/articles/awi/features/2013/09/23/feature-02 (accessed 13/09/2014)

Magharebia (05/11/2013), 'Election Campaign Starts in Mauritania', http://magharebia.com/en_GB/articles/awi/newsbriefs/general/2006/11/05/newsbrief-02 (accessed 13/09/2014)

Magharebia (20/11/2011), 'Libyan bloggers talk security solutions', http://magharebia.com/en_GB/articles/awi/features/2013/11/20/feature-2 (accessed 13/09/2014)

Magharebia (22/11/2011), 'Tunisians adjust to terror at home', http://magharebia.com/en_GB/articles/awi/reportage/2013/11/22/reportage-01 (accessed 13/09/2014)

Magharebia (25/11/2013a), 'Mauritanian elections end in calm', http://magharebia.com/en_GB/articles/awi/newsbriefs/general/2013/11/25/newsbrief-03 (accessed 13/09/2014)

Magharebia (25/11/2013b), 'Belmokhtar deputy killed in Mali', http://magharebia.com/en_GB/articles/awi/features/2013/11/25/feature-01 (accessed 13/09/2014)

Magharebia (12/12/2013), 'Morocco battles terror funding', http://magharebia.com/en_GB/articles/awi/features/2013/12/12/feature-01 (accessed 25/09/2014)

Magharebia (2014), About Us, http://magharebia.com/en_GB/pages/about (accessed 13/09/2014)

Maltby, S. (2012), *Military Media Management,* London: Routledge.

Mann, S. and H. Niedzviecki (2001), *Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer*, Toronto: Random House Doubleday

Mannes, A., Michael, M., Ptac, A., Silva, A., Subrahmanian, V. and Wilkenfield, J. (2008), 'Stochastic Opponent Modeling Agents: A Cast Study with Hezbollah', in Liu, H., Salerno, J. and Young, M. (eds), *Social Computing, Behavioral Modeling, and Prediction,* Proceedings of 1st Conference, London: Springer

Marr, J., Cushing, J. Garner, B., and Thompson, R. (2008), 'Human Terrain Mapping: A Critical First Step to Winning the COIN Fight', *Military Review,* March-April 2008, pp 18-24, http://www.au.af.mil/au/awc/awcgate/milreview/marr08marapr.pdf (accessed 04/09/2014)

Marvin, C. (1988), *When Old Technologies Were New: Thinking about Electronic Communication in the Late Nineteenth Century,* Oxford: Oxford University Press

Marwick, A. and Boyd, D. (2010), 'I tweet honestly, I tweet passionately: Twitter users, context collapes, and the imagined audience', *New Media & Society,* 13(1), pp 114-133

Marx, G.T. (2002), 'What's new about the "new surveillance"? Classifying for change and continuity', *Surveillance and Society*, 1(1): pp 9-29.

Marx, K. (2007), *Selected Writings,* Oxford: Oxford University Press

Massumi, B. (2005), 'Fear (The Spectrum Said)', *Positions: East Asia Cultures Critique,* 13(1), pp 31-48

Matheny, J. (2011), Open Source Indicators (OSI) Proposer's Day Briefing – Office of Incisive Analysis – presentation on OSI, http://www.iarpa.gov/Programs/ia/OSI/presentations/OSI_Overview_Briefing.pdf (accessed 15/09/2014)

Mathieu, J. (2011), 'SNARC', in HSCB Newsletter No 8, Winter 2008, http://www.dtic.mil/biosys/files/HSCB-news-winter-2011.pdf (accessed 15/09/2014)

Mattis, J. (2013), 2013 Posture Statement as Commander, US CENTCOM, before the Senate Armed Services Committee on March 5, 2013 about the posture of US Central Command', http://centcom.ahp.us.army.mil/en/about-centcom/posture-statement/ (accessed 13/09/2014)

Mawtani Al-Shorfa (01/22/2013), 'Jabhat al-Nusra steals formula desited for Syrian babies', http://mawtani.al-shorfa.com/en_GB/articles/iii/features/2013/11/01/feature-01 (accessed 25/09/2014)

Mawtani Al-Shorfa (04/11/2013), 'Anbar residents close ranks against al-Qaeda', http://mawtani.al-shorfa.com/en_GB/articles/iii/features/2013/11/04/feature-01 (accessed 25/09/2014)

Mawtani Al-Shorfa (07/11/2013a), 'Baghdadis celebrate their city on 'Baghdad Day'', http://mawtani.al-shorfa.com/en_GB/articles/iii/features/2013/11/07/feature-02 (accessed 25/09/2014)

Mawtani Al-Shorfa (07/11/2013b), 'Al-Qaeda's mafia-like actions in Syria underline its fragmentation: analysts', http://mawtani.al-shorfa.com/en_GB/articles/iii/features/2013/11/07/feature-01 (accessed 25/09/2014)

Mawtani Al-Shorfa (15/11/2013), 'Iraqi Ashura commemoration reflects national unity', http://mawtani.al-shorfa.com/en_GB/articles/iii/features/2013/11/15/feature-02 (accessed 25/09/2014)

Mawtani Al-Shorfa (26/11/2013), 'Baghdad hosts special festival for orphans', http://mawtani.al-shorfa.com/en_GB/articles/iii/features/2013/11/26/feature-02 (accessed 25/09/2014)

Mawtani Al-Shorfa – *About Us* (2014), About Us, http://mawtani.al-shorfa.com/en_GB/pages/about (accessed 13/09/2014)

Maybury, M. (2010), *Social Radar for Smart Power,* The MITRE Corporation

Mayfield III, T. (2011), 'A Commander's Strategy for Social Media', *Joint Force Quarterly,* 1st Quarter 2011, Issue 60

Mayfield III, T. (2013), 'A Commander's Strategy for Social Media', *Joint Force Quarterly,* 60, http://www.ndu.edu/press/commanders-strategy-social-media.html (accessed 09/09/2014)

Mazmanian, A. (2014), 'Army extends General Dynamics IT work on African news websites', *FCW.com,* 07/10/2014, http://fcw.com/articles/2014/10/07/army-extends-general-dynamics-it.aspx (accessed 11/12/2014)

Mazzetti, M. and Daragahi, B. (2005), 'U.S. Military Covertly Pays to Run Stories in Iraqi Press', *LA Times,* 30/11/2005, http://articles.latimes.com/2005/nov/30/world/fg-infowar30 (accessed 09/11/2014)

Mazzoleni, G. and Schultz, W. (1999), ''Mediatization' of Politics: A Challenge for Democracy?', *Political Communication,* 16(3), pp 247-261

McCants, W. (2012), *Science and Technology for Communication and Persuasion Abroad: Gap Analysis and Survey,* Washington DC: US DoD Rapid Reaction Technology Office

McCants W. (2013), 'Cyber Jihadists, State Department Now in Full-Blown Twitter War', *Foreign Policy – The Cable,* 30/07/2013, http://thecable.foreignpolicy.com/posts/2013/07/29/jihadis_ape_state_department#.UfgW1Rss8CI.twitter (accessed 04/09/2014)

McCarthy, D. (2011), 'Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet', *Foreign Policy Analysis*, 2011(7), pp 89-111

McChrystal, S. (2011), 'It Takes a Network: The New Front Line of Modern Warfare', *Foreign Policy,* 22/02/2011, http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network (accessed 09/09/2014)

McCormack, R. and Slater, W. (2010), 'An Application of Epidemiological Modeling to Information Diffusion', in Chai, S., Salerno, J. and Mabry, P. (eds.), *Advances in Social Computing, Proceedings of Third International Conference on Social Computing, Behavioural Modeling, and Prediction,* SBP 2010, Lecture Notes in Computing Science 6007, London: Springer

McEvoy Manjikian, M. (2010), 'From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik', *International Studies Quarterly,* 2010, 54, pp 381-401

McGarry, B. (2013), 'Special Forces, Marines Embrace Palantir Software', *Military.com - DOD Buzz,* 01/07/2013, http://defensetech.org/2013/07/01/special-forces-marines-embrace-palantir-software/ (accessed 15/09/2014)

McKelvey, K. and Menczer, F. (2013), 'Truthy: Enabling the Study of Online Social Networks', paper presented at CSCW'13, February 2013, San Antonio, Texas, http://arxiv.org/pdf/1212.4565.pdf (accessed 15/09/2014)

McNair, B. (2006), *Cultural Chaos: Journalism and Power in a Globalised World,* New York: Routledge

McRaven, W. (2012), 'Posture Statement of Admiral William H. McRaven, USN Commander, United States Special Operations Command, Before the 112th Congres Senate Armed Services Committee', March 6, 2012, http://www.socom.mil/Documents/2012_SOCOM_POSTURE_STATEMENT.pdf (accessed 11/09/2014)

Mearsheimer, J. (2011), *Why Leaders Lie: The Truth About Lying in International Politics,* Oxford: Oxford University Press

Mehta, M. and Darier, E. (1998), 'Virtual Control and Disciplining on the Internet: Electronic Governmentality in the New Wired World', *The Information Society*, 14(2), pp 107-116

Meraz, S. (2009), 'Is there an elite hold? Traditional media to social media agenda setting influence in blog networks', *Journal of Computer-Mediated Communication,* 14(3), pp 682-707

Meyssan, T. (2005), 'Soft and Undercover Coups D'État: The Albert Einstein Institution: Non violence according to the CIA', *VoltaireNet.org,* 04/01/2005, http://www.voltairenet.org/article30032.html (accessed 13/09/2014)

Michaels, J. (2012), 'Pentagon Fighting Taliban on Social Media Front', *Newsfactor,* 02/09/2012), http://www.newsfactor.com/news/Pentagon-Fighting-Taliban-Digitally/story.xhtml?story_id=11200005N8N4 (accessed 25/09/2012)

Miles, D. (2013), 'Centcom Taps Social Media to Promote Engagement, Understanding', *American Forces Press Service,* 24/07/2013, http://www.defense.gov/news/newsarticle.aspx?id=120514 (accessed 13/09/2014)

Miller, D. (ed.) (2003), *Tell Me Lies: Propaganda and Media Distortion in the Attack on Iraq,* London: Pluto

Miller, D. and Dinan, W. (2008), *A Century Of Spin,* London: Pluto

Miller, D. and Mills, T. (2010) 'Counterinsurgency and terror expertise: the integration of social scientists into the war effort', *Cambridge Review of International Affairs,* 23(2)

Miller, D. and Sabir, R. (2012), 'Propaganda and Terrorism', in Freedman, D. and Thussu, D., (eds.) *Media and Terrorism: Global Perspectives*. London: Sage.

Miller, P. and Rose, N. (2008), *Governing The Present,* Cambridge: Polity

Minerva – *Chairs Program* (2014), The Minerva Initiative – Minerva Chairs Program, http://minerva.dtic.mil/chairs.html (accessed 15/09/2014)

Minerva – *Program History* (2014), The Minerva Initiative – Program History & Overview, http://minerva.dtic.mil/overview.html (accessed 15/09/2014)

Ministry of Defence (MOD) (2003), *Operations In Iraq: Lessons for the Future,* London: MOD Directorate General Corporate Communication

Miskimmon, A., O'Loughlin, B. and Roselle, L. (2013), *Strategic Narratives: Communication Power and the New World Order,* Oxon: Routledge

Mitra, T. and Gilbert, E. (2014), 'The Language that Gets People to Give: Phrases that Predict Success on Kickstarter', https://dl.dropboxusercontent.com/u/39515687/cscw2014_crowdfunding.pdf (accessed 15/09/2014)

MITRE (2013), *Research and Promise: Research and Engineering for Human Sociocultural Behavior Capability in the U.S. Department of Defense,* McLean, Virginia: The MITRE Corporation

MITRE – *Author DNA* (2014), Author DNA, http://www.mitre.org/research/technology-transfer/technology-licensing/author-dna-0 (accessed 15/09/2014)

MITRE – *Social Radar Technologies* (2014), Technology Transfer: Social Radar, http://www.mitre.org/research/technology-transfer/technology-licensing/social-radar-technologies (accessed 15/09/2014)

Moe, T. (2011), *Social media and the U.S. Army: Maintaining a Balance,* Thesis at the School of Advanced Military Studies, US Army Command and General Staff College, http://www.dtic.mil/dtic/tr/fulltext/u2/a544887.pdf (accessed 11/09/2014)

Monaghan, J. and Walby, K. (2011), 'Making up 'Terror Identities': security intelligence, Canada's Integrated Threat Assessment Centre and social movement suppression', *Policing and Society: An International Journal of Research and Policy,* 22(2), pp 133-151

Moon, D. (2007), *Cyber-Herding and Cyber Activism: Countering Qutbists on the Internet,* MSc thesis at Naval Postgraduate School, http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA475919 (accessed 04/09/2014)

Morganthaler, J. and Giles-Summers, B. (2011), *Targeting: Social Network Analysis in Counter IED Operations,* Thesis at Naval Postgraduate School, https://www.hsdl.org/?view&did=683402 (accessed 15/09/2014)

Moturu, S. (2009), *Quantifying the Trustworthiness of User-Generated Social Media Content,* PhD thesis at Arizona State University

Morozov, E. (2009), 'Iran: The Downside to the "Twitter Revolution"', *Dissent,* Fall 2009, pp 10-14

Morozov, E. (2011), *The Net Delusion: How Not to Liberate the World,* London: Penguin

Mullen, M. (2009), 'From the Chairman – Strategic Communication: Getting Back to Basics', *Joint Chiefs of Staff Website,* 28/09/09, http://www.jcs.mil/newsarticle.aspx?ID=142 (accessed 27/09/11)

Mulrine, A. (2011), 'Pentagon Papers vs. Wikileaks: Is Bradley Manning the new Ellsberg?', *Christian Science Monitor,* 13/05/2011, http://www.csmonitor.com/USA/Military/2011/0613/Pentagon-Papers-vs.-WikiLeaks-Is-Bradley-Manning-the-new-Ellsberg (accessed 25/09/2012)

Munoz, A. (2012), *U.S. Military Information Operations in Afghanistan: Effectiveness of Psychological Operations 2001-2010,* Santa Monica: RAND Corporation

Murphy, D. (2010), 'Attack or Defend? Leveraging Information and Balancing Risk in Cyberspace', *Military Review,* May-June 2010, pp88-96

Murphy, D. (2012), ' The Future of Influence in Warfare', *Joint Force Quarterly,* 64(1), pp 47-51

Murray, K., Lowrance, J., Sharpe, K., Williams, D., Grembam, K., Speed, C., Tynes, R. (2011), 'Towards Culturally Information Option Awareness for Influence Operatiosn with S-CAT', in Salerno, J., Jay Yang, S., Nau, D., Chai, S. (eds), *Social Computing, Behavioural-Cultural Modeling and Prediction,* 4th International Conference, March 2011, Proceedings, SPB 2011 Lecture Notes in Computer Science 6589, London: Springer

Muqawama, Abu, (AKA Andrew Exum) (2012), 'On Terrorism Experts', *CNAS: Abu Muqawama Blog,* http://www.cnas.org/blogs/abumuqawama/2012/03/terrorism-experts.html (accessed 25/09/2012)

Myers, S. and Leskovec, J. (2012), 'Clash of the Contagions: Cooperation and Competition in Information Diffusion', http://cs.stanford.edu/people/jure/pubs/topicmix-icdm12.pdf (accessed 15/09/2014)

Nader, L. (1972), *Up The Anthropologist: Perspectives gained from studying up,* US Department of Health, Education and Welfare: Washington

Nagl, J. (2005), *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam,* Chicago: University of Chicago Press

Nagl, J. (2009), 'A 'Better War' in Afghanistan', Statement prepared for Senate Committee on Foreign Relations, September 2009, http://www.cnas.org/files/documents/publications/CNASTestimony_Nagl_SFRC_September_16_2009.pdf (accessed 04/09/2014)

National Research Council (2008), *Behavioural Modeling and Simulation: From Individuals to Societies,* Washington, DC: National Academies Press

Naughton, J. (2001), 'Contested space: The Internet and global civil society', in Anheir, H., Marlies, G. and Kaldor, M. (Eds.), *Global civil society*, Oxford: Oxford University Press

Nelson, R. (2009), 'CENTCOM climbs aboard social media train', Press Release, *United States Central Command,* http://www.centcom.mil/press-releases/centcom-climbs-aboard-social-media-train (accessed 15/09/2009)

Network of Concerned Anthropologists (2009), *The Counter-Counterinsurgency Manual,* Chicago: Prickly Paradigm Press

Newman, N. (2009), 'The rise of social media and its impact on mainstream journalism', Working Paper, Oxford: Reuters Institute for the Study of Journalism, http://www.sssup.it/UploadDocs/6635_8_S_The_rise_of_Social_Media_and_its_Impact_on_mainstream_journalism_Newman_07.pdf (accessed 25/09/2012)

New York Times (2004), 'The Times and Iraq', *New York Times,* 26/05/2004, http://www.nytimes.com/2004/05/26/international/middleeast/26FTE_NOTE.html (accessed 25/09/12)

New York Times (2010), 'The War Logs: Reaction to Disclosure of Military Documents on Afghan War', *The New York Times,* 25/07/2010, http://atwar.blogs.nytimes.com/2010/07/25/the-war-logs/ (accessed 25/09/12)

Nichols, M. and Honan, E. (2007), 'Internet is "the new Afghanistan": NY police commissioner', *Reuters,* 15/08/2007, http://www.reuters.com/article/2007/08/15/us-security-newyork-internet-idUSN1524872020070815 (accessed 04/09/2014)

Nichols, J., Zhuo, M., Yang, H., Kang, J. and Sun, X. (2013), 'Analyzing the Quality of Information Solicited from Targeted Strangers on Social Media', http://www.jeffreynichols.com/papers/product-reviews-cscw2013.pdf (accessed 15/09/2014)

Niekerk , B. and Maharaj, M. (2013), 'Social Media and Information Conflict', *International Journal of Communication,* 7, pp 1162-1184

Nissen, T. (2013), 'Narrative Led Operations', *MIlitært Tidsskrift,* 141, 04/01/2013, pp 67-77,

Niva, S. (2013), 'Disappearing violence: JSOC and the Pentagon's new cartography of networked warfare', *Security Dialogue,* 44(3), pp 185-202

NRC (National Research Council) (2008), *Behavioral Modeling and Simulation: From Individuals to Societies,* Washington, D.C: National Academies Press

Null, S. (2011), 'In Search of a New Security Narrative', *The New Security Beat,* http://www.newsecuritybeat.org/2011/04/in-search-of-a-new-security-narrative/ (accessed 25/09/2012)

Nye, J. (2004), *Soft Power: The Means to Success in World Politics,* New York: Public Affairs

O'Brien, S. (2010), 'Crisis Early Warning and Decision Support: Contemporary Approaches and Thoughts on Future Research', *International Studies Review,* 12, pp 87-104

O'Brien, S. (2013), 'A Multi-Method Approach for Near Real Time Conflict and Crisis Early Warning', in Subrahmanian, V. (ed.), *Handbook of Computational Approaches to Counterterrorism,* Springer: London

Office of Inspections, Department of State (2009), *Report of Inspection: Embassy Nouakchott, Mauritania,* http://oig.state.gov/documents/organization/122725.pdf (accessed 13/09/2014)

Office of Inspections, Department of State (2013), *Inspection of Embassy Abuja and Consulate General, Lagos, Nigeria,* http://oig.state.gov/documents/organization/207009.pdf (accessed 13/09/2014)

O'Hagan, J. (2013), 'War 2.0: an analytical framework', *Australian Journal of International Affairs,* 67(5), pp 555-569

Olson, E. (2008), 'Admiral Olson's Keynote Address', *Unrestricted Warfare Symposium Proceedings 2008,* pp 7-26, http://www.jhuapl.edu/urw_symposium/proceedings/2008/Authors/Olson.pdf (accessed 09/09/2014)

Olson, E. (2010), Statement at hearing on Department of Defense Authorisation for Appropriations for Fiscal Year 2011, before the Committee on Armed Services of the US Senate, S. 3454, 16/03/2010

Orlina, E. and Desjardins, A. (2012), 'Cyber on the Brain: The effects of CyberNeurobiology & CyberPsychology on Political Extremism', in Strategic Multilayer Assessment, *Insights from Neurobiology on Influence and Extremism,* Fall 2012, Washington, DC: Office of the Secretary of Defense/NSI

OSD RDT&E – *FY2012* (2012), *Department of Defense FY2012 Budget Estimates: Research, Development, Test & Evaluation, Defense Wide Justification Book,* February 2011, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2012/budget_justification/pdfs/03_RDT_and_E/OSD.pdf (accessed 15/09/2014)

OSD RDT&E – *FY2014* (2013), *Department of Defense FY2014 Budget Estimates: Research, Development, Test & Evaluation, Defense Wide Justification Book,* April 2013, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2014/budget_justification/pdf/03_RDT_and_E/Office_of_the_Secretary_of_Defense_PB_2014.pdf (accessed 15/09/2014)

OSD RDT&E – *FY2015* (2014), *Department of Defense FY2015 Budget Estimates: Research, Development, Test & Evaluation, Defense Wide Justification Book,* March 2014, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/budget_justification/pdfs/03_RDT_and_E/3_RDTE_MasterJustificationBook_Office_of_the_Secretary_of_Defense_PB_2015_Vol_3.pdf (accessed 15/09/2014)

O'Shaughnessy, N. J. (2004), *Politics and Propaganda: Weapons Of Mass Seduction*, Manchester: Manchester University Press

Otwell, R. (2013), 'MISO Integration with Intelligence Efforts', in Souter, J. and Heidger, C., 'The Future of MISO in Unconventional Warfare', *Special Warfare,* 26(1), pp 7-9

Overbey, L., Paribello, C. and Jackson, T. (2013), 'Identifying Influential Twitter Users in the 2011 Egyptian Revolution', in Greenberg, A., Kennedy, W., and Bos, N. (eds), *Social Computing, Behavioral-Cultural Modeling and Prediction,* Proceedings of 6th Conference, London: Springer

Owens, P. (2012), 'From Bismark to Patraeus: the Question of the Social and the Social Question in Counterinsurgency', *European Journal of International Relations,* 0(0), pp1-23

Packer, J. (2010), 'What is an Archive?: An Apparatus Model for Communications and Media History', *The Communication Review*, 13(1), pp 88-104

Pakistan Affairs – US CENTCOM (2012), 'US CENTCOM – Public Affairs – Digital Engagement Team' discussion thread, http://www.pakistanaffairs.pk/threads/1387-US-CENTCOM-Public-Affairs-Digital-Engagement-Team (accessed 15/09/2014)

Pakistan Defence – CENTCOM (2014), '5 Killed as two blasts hit cinema hall in northwest Pakistan' discussion thread, http://defence.pk/threads/5-killed-as-two-blasts-hit-cinema-hall-in-northwest-pakistan.298264/page-2 (accessed 15/09/2014)

Pamment, J. (2012), 'American Strategic Communication in Iraq: The "Rapid Reaction Media Team"', *Online Journal of Communication and Media Technologies,* 2(2), April 2012

Pantucci, R. (2011), 'The UK's Efforts to Disrupt Jihadist Activity Online', *CTC Sentinel,* Summer 2011, 4(9)

Papacharissi, Z. (2009), 'The Virtual Sphere 2.0: The Internet, the Public Sphere and beyond', in Chadwick, A. and Howard, P. (eds.), *Handbook of Internet Politics,* New York: Routledge

Patraeus, D. (2010), Statement of General David H. Patraeus, U.S. Army, Commander, U.S. Central Command, before the Senate Armed Services Committee on the Posture of U.S. Central Command, 16/03/2010, http://armed-services.senate.gov/statemnt/2010/03%20March/Petraeus%2003-16-10.pdf (accessed 13/09/2014).

Patrick, B. and Thrall, T. (2007), 'Beyond Hegemony: Classical Propaganda Theory and Presidential Communication Strategy After the Invasion of Iraq', *Mass Communication and Society,* 10(1), pp 95-118

Payne, K. (2009): 'Winning the Battle of Ideas: Propaganda, Ideology, and Terror', *Studies in Conflict & Terrorism*, 32(2), 109-128

Payne, K. (2011), 'Hearts and Minds? Psychology in classic counterinsurgency writing', ISA Annual Conference, Montreal, 2011

PC Mag (2012), 'Definition of walled garden', http://www.pcmag.com/encyclopedia_term/0,1237,t=walled+garden&i=54187,00.asp (accessed 25/09/2012)

Pellerin, C. (2013), 'Marines Focused at Tactical Edge of Cyber, Commander Says', *American Forces Press Service,* http://www.defense.gov/news/newsarticle.aspx?id=120246 (accessed 12/09/2014)

Peralta, E. and Carvin, A. (2011), ''Gay Girl in Damascus' Turns Out To Be An American Man', *NPR Online,* 12/06/11, http://www.npr.org/blogs/thetwo-way/2011/06/13/137139179/gay-girl-in-damascus-apologizes-reveals-she-was-an-american-man (accessed 30/09/11)

Peter, T. A. (2008). 'U.S. Begins Hunting Iraq's Bombmakers, Not Just Bombs', *The Christian Science Monitor*, 08/09/2008, http://www.csmonitor.com/2008/0908/p04s01-wome.html (accessed 09/09/2014)

Peterson, S. (2002), ''Smarter' bombs still hit civilians', *Christian Science Monitor,* 22/10/2002, http://www.csmonitor.com/2002/1022/p01s01-wosc.html (accessed 25/09/12)

Petit, B. (2011), 'The Fight for the Village, Southern Afghanistan, 2010', *Military Review,* May-June 2011, pp 25-32

Petit, B. (2012), 'Social Media and UW', *Special Warfare,* 25(2), pp 20-29

Pfadenhauer, M. (2009), 'At Eye Level: The Expert Interview – a Talk between Expert and Quasi-Expert', in Bogner, A., Littig, B., and Menz, W. (eds.) (2009), *Interviewing Experts,* London: Palgrave MacMillan

Phillips, R. (1998), 'The Politics of History: some methodological and ethical dilemmas in elite-based research', *British Educational Research Journal,* 24:1, pp 5-19

Philo, G. and Berry, M. (2004), *Bad News from Israel,* Pluto: London

Physics arXiv Blog (2011), 'Undercover researchers expose Chinese Internet Water Army', *Technology Review,* 22/11/2011, http://www.technologyreview.com/view/426174/undercover-researchers-expose-chinese-internet/ (accessed 25/09/2012)

Pickering, A. (1995), 'Cyborg History and the World War II Regime', *Perspectives on Science,* 3(1)

Plaisance, P. L. (2005), 'The Propaganda War on Terrorism: Analysis of the United States' "Shared Values" Public-Diplomacy Campaign After September 11, 2001', *Journal of Mass Media Ethics,* 20(4), pp 250-268

Polese, A. and Ó Beacháin, D., (2011), 'The Color Revolution Virus and Authoritarian Antidotes', *Demokratizatsiya: The Journal of Post-Soviet Democratization,* 19(2), pp 111-127

Pollock, S., Alt, J., and Darken, C. (2011), 'Representing Trust in Cognitive Social Simulations', in Salerno, J., Jay Yang, S., Nau, D., Chai, S. (eds), *Social Computing, Behavioural-Cultural Modeling and Prediction,* 4th International Conference, March 2011, Proceedings, SPB 2011 Lecture Notes in Computer Science 6589, London: Springer

Poole, R (ed.) (2011), *Sociocultural Data to Accomplish Department of Defense Missions: Towards a Unified Social Framework,* Washington, DC: National Research Council

Potter, E. (ed.) (2002), *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century,* London: McGill-Queens UP

Pötzsch, H. (2013), 'The emergence of iWar: Changing practices and perceptions of military engagement in a digital era', *New Media & Society,* published online before print, DOI: 10.1177/1461444813516834, http://nms.sagepub.com/content/early/2013/12/15/1461444813516834 (accessed 04/09/2014)

Price, D. (2013) 'The role of culture in wars waged by robots', in Whitehead, N. and Finnström, S. (2013), *Virtual War and Magical Death,* London: Duke University Press

Price, M. (2012), 'Iran and the Soft War', *International Journal of Communication,* 6, pp 2397-2415

Priest, D. and Arkin, W. (2011), ''Top Secret America': A Look at the Military's Joint Special Operations Command', *Washington Post,* 02/09/2011, http://www.washingtonpost.com/world/national-security/top-secret-america-a-look-at-the-militarys-joint-special-operations-command/2011/08/30/gIQAvYuAxJ_story.html?hpid=z1 (accessed 09/09/2014)

Prucha, N. and Fisher, A. (2013), 'Tweeting for the Caliphate: Twitter as the New Frontier for Jihadist Propaganda', *CTC Sentinel,* June 2013, http://thecable.foreignpolicy.com/posts/2013/07/29/jihadis_ape_state_department#.UfgW1Rss8CI.twitter (accessed 04/09/2014)

Qualter, Terence (1985), *Opinion Control in the Democracies,* London: Macmillan

Quinlan, T. (2013), 'Building a Human Sensor Network', presentation at Information Operations Global 2013, slideshow distributed to conference participants

Quinn, B. (2014), 'Ministry of Defence funding research into online habits', *The Guardian,* 07/01/2014, http://www.theguardian.com/uk-news/2014/jan/07/ministry-defence-fund-research-online (accessed 04/09/2014)

Quinn, B. and Ball, J. (2014), 'US military studied how to influence Twitter users in Darpa-funded research', *The Guardian,* 08/07/2014, http://www.theguardian.com/world/2014/jul/08/darpa-social-networks-research-twitter-influence-studies (accessed 04/09/2014)

Raden Keefe, P. (2013), 'Rocket Man: How an unemployed blogger confirmed that Syria had used chemical weapons', *The New Yorker,* November 25, 2013, http://www.newyorker.com/magazine/2013/11/25/rocket-man-2 (accessed 04/09/2014)

Ragucci, J. (2014), 'New command, big changes', *United States Special Operations Command* press release, July 1, 2014, http://www.soc.mil/UNS/Releases/2014/July/140701-01/140701-01.html (accessed 18/07/2014)

Rahimi, B. (2011), 'The Agonistic Social Media: Cyberspace in the Formation of Dissent and Consolidation of State Power in Postelection Iran', *The Communication Review,* 14(3), pp 158-178

Rampton, S. and Stauber, J. (2003), *Weapons of Mass Deception: The Uses of Propaganda in Bush's War on Iraq,* New York: Tarcher

Rappert, B. (1999), 'Assessing technologies of political control', *Journal of Peace Research,* 36(6), pp 741-750

Ratkiewicz, J. Conover, M., Meiss, M., Goncalves, B., Patil, S., Flammini, A, and Menczer, F. (2010), 'Detecting and Tracking the Spread of Astroturf Memes in Microblog Streams', http://arxiv.org/pdf/1011.3768.pdf (accessed 15/09/2014)

Rawnsley, A. (2011), 'Pentagon Wants a Social Media Propaganda Machine', *Wired – Danger Room,* 15/07/2011, http://www.wired.com/dangerroom/2011/07/darpa-wants-social-media-sensor-for-propaganda-ops/ (accessed 15/09/2014)

Raymond, E, (1999), *The Cathedral and the Bazaar,* http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ (accessed 25/09/2012)

Reed, B. (2007) 'A Social Network Approach to Understanding an Insurgency, *Parameters,* Summer 2007, pp 19-30

Reeder, E. (2013), 'From The Commandant', *Special Warfare,* 26(3), p 04

Ressler, S. (2006), 'Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research', *Homeland Security Affairs,* II(2), July 2006

Reuters (01/12/2013), 'Syrian helicopters drop 'barrel bombs' on rebel town, killing 20', http://www.reuters.com/article/2013/12/01/us-syria-crisis-aleppo-idUSBRE9B009C20131201 (accessed 13/09/2014)

Revie, R. (2010), 'Wikileaks and 21st Century Statecraft, *Pulse Media.org,* 8/12/2010, http://pulsemedia.org/2010/12/08/wikileaks-and-21st-century-statecraft/ (accessed 27/09/11)

Revie, R. (2011), 'New Media, New Battlefields', paper presented at *A Decade Of Terrorism and Counterterrorism* Conference, Glasgow, 2011

Revie, R. (2012a), 'How NATO and the US State Department endanger internet freedom', *Pulse Media,* http://pulsemedia.org/2012/04/30/how-nato-and-the-us-state-department-endanger-internet-freedom/ (accessed 25/09/2012)

Revie, R. (2012b), 'The Tangled Web of 'Internet Freedom'', *World Policy Journal Blog,* 11/07/2012, http://www.worldpolicy.org/blog/2012/07/11/tangled-web-internet-freedom (accessed 04/09/2014)

Revie, R. (2013), 'NATO Strategic Communication and a Narrative of Bullshit', *FORWARD!Slash,* http://4ward5lash.tumblr.com/post/52664330225/nato-strategic-communications-conference-and-a (accessed 15/09/2014)

Ricks, T. (2009), 'The COINdinistas', *Foreign Policy,* 30/11/2009, http://www.foreignpolicy.com/articles/2009/11/30/the_coindinistas (accessed 09/11/2014)

Rid, T. (2007), *War and Media Operations: The US military an the press from Vietnam to Iraq,* New York: Routledge

Rid, T. and Hecker, M. (2009), *War 2.0: Irregular Warfare in the Information Age,* London: Praeger Security International

Rid, T. (2011), 'Cyber War Will Not Take Place', *Journal of Strategic Studies,* 1-28

Ritzer, G. and Jurgenson, N. (2010), 'Production, Consumption, Prosumtion: The nature of capitalism in the age of the digital 'prosumer'', *Journal of Consumer Culture,* 10(13)

Rizwan, S. (2000), 'Revolution in Military Affairs', *Defence Journal,* 3(9)

Robin, R. (2001), *The Making of the Cold War Enemy: Culture and Politics in the Military-Industrial Complex,* Princeton, NJ: Princeton University Press

Robins, K. and Webster, F. (1983), 'The mis-information society', *Universities Quarterly,* Autumn 1983

Robins, K., and Webster, F., and Pickering, M. *(*1987), 'Propaganda, Information and Social Control', in Hawthorn, J. (ed*.), Propaganda, Persuasion and Polemic*, London: Edward Arnold

Robins, K. and Webster, F. (1988), 'Cybernetic Captialism: Information, Technology, Everyday Life', in Mosko, V. and Wask, J. (eds.), *The Political Economy of Information,* Madison: University of Wisconsin Press

Robins, K, and Webster, F. (1999), *Times of the Technoculture: From the Information Society to the Virtual Life,* Oxford: Routledge

Robinson, P. (2002), *The CNN Effect: The Myth of News, Foreign Policy and Intervention,* London: Routledge

Rockefeller, H. (2011), 'UPDATED: The HB Gary Email That Should Concern Us All', *Daily Kos,* 16/02/2011, http://www.dailykos.com/story/2011/02/16/945768/-UPDATED:-The-HB-Gary-Email-That-Should-Concern-Us-All (accessed 15/09/2011)

Roennfeldt, C. (2011), 'Productive War: A Re- Conceptualisation of War, Journal of Strategic Studies', 34:1, pp 39-62

Rohde, D. (2012), 'The Obama Doctrine', *Foreign Policy,* March/April 2012, http://www.foreignpolicy.com/articles/2012/02/27/the_obama_doctrine?print=yes&hidecomments=yes&page=full (accessed 25/09/2012)

Romero, D., Tan, C. and Ugander, J. (2013), 'On the Interplay between Social and Topical Structure', http://www.cs.cornell.edu/~chenhao/pub/social-topical-structure.pdf (accessed 15/09/2014)

Roston, A. (2012), 'Unwitting Sensors: How DoD is Exploiting Social Media', *Defense News,* 13/11/2012, http://www.defensenews.com/article/20121113/DEFREG02/311130003/Unwitting-Sensors-How-DoD-Exploiting-Social-Media (accessed 15/09/2014)

Rumbaugh, R. and Leatherman, M. (2012), *The Pentagon as Pitchman: Perception and Reality of Public Diplomacy,* Washington, DC: Stimpson

Sabahi (05/10/2012), 'As al-Qaeda falls, Ansar al-Sharia rises', http://sabahionline.com/en_GB/articles/hoa/articles/features/2012/10/05/feature-01 (accessed 13/09/2014)

Sabahi (25/06/2013), 'Somali president praises New Deal plans', http://sabahionline.com/en_GB/articles/hoa/articles/newsbriefs/2013/07/25/newsbrief-01 (accessed 13/09/2014)

Sabahi (06/08/2013), 'Somaliland court sentences 21 men in a gang rape case', http://sabahionline.com/en_GB/articles/hoa/articles/newsbriefs/2013/08/06/newsbrief-06 (accessed 25/09/2014)

Sabahi (08/10/2013), 'Somali ex-pirate kingpin now leads anti-piracy fight', http://sabahionline.com/en_GB/articles/hoa/articles/features/2013/10/08/feature-02 (accessed 25/09/2014)

Sabahi (05/11/2013), 'Quail farming a hot investment trend in Kenya', http://sabahionline.com/en_GB/articles/hoa/articles/features/2013/11/05/feature-02 (accessed 13/09/2014)

Sabahi (12/11/2013), 'Somali government welcomes critical report on rape investigation', http://sabahionline.com/en_GB/articles/hoa/articles/newsbriefs/2013/11/12/newsbrief-04 (accessed 13/09/2014)

Sabahi (14/11/2013), 'Al-Shabaab says smartphones used 'to spy on Muslim people', http://sabahionline.com/en_GB/articles/hoa/articles/features/2013/11/14/feature-01 (accessed 13/09/2014)

Sabahi (21/11/2013a), 'Kenyan anti-terrorism police accused of human rights violations', http://sabahionline.com/en_GB/articles/hoa/articles/newsbriefs/2013/11/21/newsbrief-05 (accessed 13/09/2014)

Sabahi (21/11/2013b), 'Somali police arrest alleged rape victim as UN calls for inquiry', http://sabahionline.com/en_GB/articles/hoa/articles/newsbriefs/2013/11/21/newsbrief-01 (accessed 13/09/2014)

Sabir, R. (2014), *Understanding Counter-Terrorist Policy and Practice in the UK since 9/11,* PhD thesis at Department of Social and Policy Sciences, University of Bath: Bath

Saco, D. (2002), *Cybering Democracy: Public Space and the Internet,* Minneapolis: University of Minnesota Press

Sageman, M. (2004), *Understanding Terror Networks,* Philadelphia: University of Pennsylvania Press

Salerno, J., Jay Yang, S., Nau, D., Chai, S. (eds) (2011), *Social Computing, Behavioural-Cultural Modeling and Prediction,* 4th International Conference, March 2011, Proceedings, SPB 2011 Lecture Notes in Computer Science 6589, London: Springer

Samuels, D. (2002), 'On message: A theater of war at the Pentagon', *Harper's Magazine, 304*(1820), pp 53-62

Sandberg, A. (2012), 'The censor and the eaversdropper: the linkb between censorship and surveillance', *Practical Ethics blog,* http://blog.practicalethics.ox.ac.uk/2012/03/the-censor-and-the-eavesdropper-the-link-between-censorship-and-surveillance/ (accessed 25/09/2012)

Sandell, N., Luettgen, M., Cybenko, G. (2012), 'Two-stage classification for tracking memes in microblogs', http://www.stresearch.com/Documents/deception_spie_final.pdf (accessed 15/09/2014)

SBP 2015 (2014), 2015 International Conference on Social Computing, Behavioural-Cultural Modeling & Prediction (SBP15) - "About the Conference", http://sbp-conference.org/about/ (accessed 15/09/2014)

Scahill, J. (2013), *Dirty Wars: The World is a Battlefield,* New York: Nation Books

Scales, R. (2006), 'Clausewitz and World War IV', *Armed Forces Journal,* http://www.armedforcesjournal.com/2006/07/1866019 (accessed 15/09/2014)

Schmidle, N. (2011), 'Getting Bin Laden: What happened that night in Abbottabad', *The New Yorker,* 08/08/2011, http://www.newyorker.com/magazine/2011/08/08/getting-bin-laden (accessed 11/09/2014)

Schmitt, E. and Shanker, T. (2011), *Counterstrike: The Untold Story of America's Secret Campaign Against Al Qaeda,* New York: Times Books

Schmorrow, D. (2009a), 'Q&A With CDR Dylan Schmorrow', *HSCB Newsletter No 2,* Summer 2009, p 5

Schmorrow, D. (2009b), 'Reasoning About Diverse Cultures Using Multi-Disciplinary Teams and Computer Technology in the Human Social Culture Behavior (HSCB) Modeling Program', Abstract from resentation at ICCCD 2009, http://www.umiacs.umd.edu/conferences/icccd2009/program.html#abstracts (accessed 15/09/2014)

Schmorrow, D. (2011a), *Sociocultural Behavior Research and Engineering in the Department of Defense Context,* Office of the Secretary of Defense: Washington, DC

Schmorrow, D. (2011b), 'Welcome to Focus 2011', presentation on HSCB Program, https://wss.apan.org/746/team_docs/Focus2011_Dylan_State%20of%20Union_slides_Final.pptx (accessed 15/09/2014)

Schmorrow, D. (2013), 'Sociocultural Behavior Analysis and Modeling Technologies for a Phase 0 World', presentation at PACOM, 06/03/2013

Schmorrow, D and Nicholson, D. (eds.) (2010), *Advances in Design for Cross-Cultural Activities,* Boca Raton, FL: CRC Press

Schroeder, R., Everton, S., and Shepherd, R. (2012), 'Mining Twitter Data from the Arab Spring', *CTX,* 2(4), pp 56-64

Schwarz, J. (2008), 'The U.N. Deception: What Exactly Colin Powell Knew Five Yeara Ago, and What He Told The World', *Mother Jones,* 05/02/2008, http://www.motherjones.com/mojo/2008/02/un-deception-what-exactly-colin-powell-knew-five-years-ago-and-what-he-told-world (accessed 25/09/2012)

Schwartz, N. (2010), Statement on hearings for DOD Authorization for Appropriations for Fiscal Year 2011, Hearing before the Committee on Armed Services United States Senate, S.3454, 04/03/2010

Sec.gov (2010), Agreement and Plan of Merger among Cubic Corporation, Abrx Acquisition Corp, and Abraxas Corporation, *Securities and Exchange Commission,* 15/11/2010, http://www.sec.gov/Archives/edgar/data/26076/000110465911004605/a11-5082_1ex10d6.htm (accessed 15/09/2014)

Secretary of Defense – *Policy in DOD IIA* (2007), 'Policy for Department of Defense (DoD) Interactive Internet Activities', 08/06/2007

Secretary of Defense – *Regional Websites* (2007), 'Policy for Combatant Command (COCM) Regional Websites Tailored to Foreign Audiences', 03/08/2007

Seib, P. (2012), *Real-Time Diplomacy: Politics and Power in the Social Media Era,* New York: Palgrave Macmillan

Seffers, G. (2014), 'Open Source Intelligence Offers Crystal Ball Capability', *Signal Online,* 01/01/2014, http://www.afcea.org/content/?q=node/12503 (accessed 15/09/2014)

Senate Armed Services Committee (2010), Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, 10/03/2010,

http://www.gpo.gov/fdsys/pkg/CHRG-111shrg63687/html/CHRG-111shrg63687.htm (accessed 12/09/2014)

Senate Report *113-004* (2014), Committee Reports, 13th Congress (2013-2014), Senate Report 113-044, Nation Defense Authorization Act for FY2014, http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp113DzuqB&r_n=sr044.113&dbname=cp113&&sel=TOC_271971& (accessed 15/09/2014)

SES Türkiye (08/11/2013a), 'Christian-Islamic dictionary promotes peaceful co-existence', http://turkey.setimes.com/en_GB/articles/ses/articles/features/departments/national/2013/11/08/feature-01 (accessed 25/09/2014)

SES Türkiye (08/11/2013b), 'Turkish army contributes to reconciliation, stability in BiH', http://turkey.setimes.com/en_GB/articles/ses/articles/features/departments/world/2013/11/08/feature-01 (accessed 25/09/2014)

SES Türkiye (11/11/2013), 'Security experts debate change in military service time', http://turkey.setimes.com/en_GB/articles/ses/articles/features/departments/national/2013/11/11/feature-02 (accessed 25/09/2014)

SES Türkiye (18/11/2013), 'Bride-swapping practice facing criticism from youngsters', http://turkey.setimes.com/en_GB/articles/ses/articles/features/departments/society/2013/11/18/feature-01 (accessed 25/09/2014)

SES Türkiye (19/11/2013), 'Football unites on Cyprus', http://turkey.setimes.com/en_GB/articles/ses/articles/reportage/2013/11/19/reportage-01 (accessed 25/09/2014)

SETimes (02/02/2011), 'Turkey's Erdogan urges Egypt's Mubarak to step down', http://www.setimes.com/cocoon/setimes/xhtml/en_GB/newsbriefs/setimes/newsbriefs/2011/02/02/nb-02 (accessed 25/09/2014)

SETimes (05/01/2012), 'Price hikes making Greeks put out their cigarettes', http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/features/2012/01/05/feature-02 (accessed 13/09/2014)

SETimes (29/10/2012), 'Greek extremist group's blasphemy protest raises a stir', http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/features/2012/10/29/feature-01 (accessed 25/09/2014)

SETimes (03/12/2012), 'Erdogan takes on 'The Magnificent Century'', http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/features/2012/12/03/feature-05 (accessed 25/11/2014)

SETimes (01/07/2013), 'Turkey's wealth amnesty law potentially blaze trail for region', http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/features/2013/07/01/feature-01 (accessed 25/09/2014)

SETimes (11/11/2013), 'Attacks on Roma spark calls for action in Southeast Europe', http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/articles/2013/11/11/reportage-01 (accessed 13/09/2014)

SETimes (19/11/2013), 'Education ministries working to prevent bullying in schools' http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/features/2013/11/19/feature-02 (accessed 13/09/2014)

SETimes (21/11/2013), 'On Tolerance Day, Macedonia organizes a national discussion on hate speech', http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/features/2013/11/21/feature-02 (accessed 13/09/2014)

Shachtman, N. (2011), 'Pentagon Forecast: Cloudy, 80% Chance of Riots', *Wired – Danger Room,* 07/09/2011, http://www.wired.com/2007/11/lockheed-peers/ (accessed 15/09/2014)

Shachtman, N. (2012), 'Air Force's Top Brain Wants a "Social Radar" to "See into Hearts and Minds"', *Wired – Danger Room* 19/01/2012, http://www.wired.com/dangerroom/2012/01/social-radar-sees-minds/ (accessed 15/09/2014)

ShadowSpear (2014), 'MISOC Units Re-Designate as PSYOP', *ShadowSpear, Special Operations,* http://www.shadowspear.com/2014/08/misoc-units-re-designate-as-psyop/ (accessed 13/09/2014)

Shah, F. and Sukthankar, G. (2011), 'Constructing Social Networks from Unstructured Group Dialog in Virtual Worlds', in Salerno, J., Jay Yang, S., Nau, D., Chai, S. (eds), *Social Computing, Behavioural-Cultural Modeling and Prediction,* 4th International Conference, March 2011, Proceedings, SPB 2011 Lecture Notes in Computer Science 6589, London: Springer

Shakarian, P, Subrahmanian, V. and Sapino, M. (2009), 'SCARE: A Case Study with Baghdad', Presentation at ICCCD 2009, http://www.umiacs.umd.edu/conferences/icccd2009/program.html#abstracts (accessed 15/09/2014)

Shakarian, P., Shakarian, J. and Ruef, A. (2013), *Introduction to Cyber-Warfare: A Multidisciplinary Approach,* Waltham, MA: Syngress

Shakarian, P. (2014), The Homepage of Paulo Shakarian, http://shakarian.net/Paulo (accessed 13/09/2014)

Shalikashvili, J. (2006), *Joint Vision 2010,* Washington DC: Chairman of the Joint Chiefs of Staff

Shanker, T. and Schmitt, E. (2011), 'U.S. Military Goes Online to Rebut Extremists' Messages', *New York Times,* 17/11/2011, http://www.nytimes.com/2011/11/18/world/us-military-goes-online-to-rebut-extremists.html?pagewanted=all (accessed 15/09/2011)

Sharp, G. (1994), *From Dictatorship to Democracy,* Boston: Albert Einstein Institution

Shaw, Martin (2005), *The New Western Way of War,* Cambridge: Polity

Sheridan, G. (2012), 'Newsrooms as intelligence agencies', *Storyful Blog,* 30/07/2012, http://blog.storyful.com/2012/07/30/newsrooms-as-intelligence-agencies/#.UCkC_s2bO9e (accessed 25/09/2012)

Shulz, W. (2004), 'Reconstructing Mediatization as an Analytical Concept', *European Journal of Communication,* 19(1), pp 87-101

Silverman, C. (2011), 'Misinformation Propagation', *Columbia Journalism Review,* 04/10/2011, http://www.cjr.org/behind_the_news/misinformation_propagation.php?page=all (accessed 15/09/2014)

Simpson, C. (1996), *Science of Coercion: Communication Research and Psychological Warfare, 1945-1960,* Oxford: Oxford University Press

Skarda, B., Mills, R., McDonald, T. and Strouble, D. (2008), ''C2 for Complex Endeavors': Operationalising Social Engineering for Offensive Cyber Operations', conference paper at 13th International Command and Control Research and Technology Symposium, http://www.researchgate.net/publication/235081999_Operationalizing_Social_Engineering_for_Offensive_Cyber_Operations (accessed 09/11/2014)

Slaughter, A.M. (2009), 'America's Edge: Power in the Networked Century', *Foreignt Affairs,* January/February 2009

Slaughter, A. M. (2011), 'Preface', in Mr Y. (2011), *A National Strategic Narrative,* Woodrow Wilson International Center for Scholars, http://www.wilsoncenter.org/sites/default/files/A%20National%20Strategic%20Narrative.pdf (accessed 27/09/11)

SMA (Strategic Multilayer Assessment) (2014), Proposal for 2014 SMA Conference, 'A New Information Paradigm? From Genes to 'Big Data' and Instagram to Persistent Surveillance…Implications for National Security'

SMA – *TeleCon Booklet* (2014), *DHS/START and SMA Technical Lecture Series Telecon Booklet, 2011-2014,* distributed through SMA mailing list

Smart, B. (1986), 'The Politics of Truth and the Problem of Hegemony', in Couzens Hoy, D. (ed.), *Foucault: A Critical Reader,* Oxford: Blackwell

Smith, L., Zhu. L., Lerman, K. and Kozareva, Z. (2013), 'The Role of Social Media in the Discussion of Controversial Topics', http://www.isi.edu/integration/people/lerman/papers/Smith13socialcom.pdf (accessed 15/09/2014)

Snow, N. and Taylor, P. (2006), 'The Revival of the Propaganda State: US Propaganda at Home and Abroad since 9/11', *The International Communication Gazette,* 68(5-6), pp 389-407

SOCOM (2008), *United States Special Operations Command: History, 6th Edition,* MacDill AFB, Tampa: USSOCOM History and Research Office

SOCOM – *Budget Justification Book, RTD&E* (2012), *Department of Defense Fiscal Year (FY) 2013 President's Budget Submission: United States Special Operations Command, Justification Book: Research, Development, Test & Evaluation, Defense-Wide,* February 2012, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2013/budget_justification/pdfs/03_RDT_and_E/United_States_Special_Operations_Command_PB_2013-1.pdf (accessed 12/09/2014)

SOCOM – *Factbook* (2012), *U.S. Special Operations Command 2012 Fact Book,* MacDill AFB, Tampa: USSOCOM Public Affairs, https://www.fas.org/irp/agency/dod/socom/factbook-2012.pdf (accessed 13/09/2014)

SOCOM – *TE 14-2* (2013), *United States Army Special Operations Command (USASOC) Science and Technology (S&T) Gaps List,* https://www.fbo.gov/?s=opportunity&mode=form&id=6f534060f7c846f0f40d6d0829002eaa&tab=core&_cview=0 (accessed 15/09/2014)

SOHR (Syrian Observatory on Human Rights) (2013), 'More than 100 people killed in Syria', http://syriahr.com/en/index.php?option=com_news&nid=1072&Itemid=2&task=displaynews#.Uvuq5RZrFjE (accessed 13/09/2014)

Song, C. Qu, Z., Blumm, N, and Barabási, A. (2010), 'Limits of Predictability in Human Mobility', *Science,* 327, 1018-1021

Solovey, M. (2001), 'Project Camelot and the 1960s Epistemological Revolution: Rethinking the Politics-Patronage-Social Science Nexus', *Social Studies of Science,* 31(2), pp 171-206

SORBHQ (2013), Youtube video called "MISOC Capabilities", http://www.youtube.com/watch?v=ZelF95xZK-k (accessed 13/09/2014)

SORDAC (Special Operations Research, Development & Acquisition Center) (2014), Homepage, http://www.socom.mil/sordac/Pages/Default.aspx (accessed 15/09/2014)

Souter, J. and Heidger, C. (2013), 'The Future of MISO in Unconventional Warfare', *Special Warfare,* 26(1), pp 7-9

Spitaletta, J. (2013), 'Neuropsychological Operations: A Concept for Counter-Radicalization', in Reynolds, M. and Lyle, D., *Strategic Multi-layer Assessment – Periodic White Paper,* Washington, DC: NSI

Spitaletta, J. (2014), 'Operational Implications & Applications of NeuroS/T Based Influence and Deterrence, in Cabayan, H., Casebeer, W., DiEuliis, D., Giordano, J. and Wright, N. (eds.), *White paper on Leveraging Neuroscientific and Neurotechnological (NeuroS&T) Developments with Focus on Influence and Deterrence in a Networked World,* Washington, DC: Joint Chiefs of Staff

Spraragen, M., Landwehr, P., Ranganathan, B.. Zyda, M., Carley, K., Chang, Y. and Maheswaran, R. (2013), 'Cosmopolis: A Massively Multiplayer Online Game Designed for Social and Behavioral Research', *Journal of Artificial Societies and Simulation,* 16(1)

Stablization Unit (2012), 'Details for 'skyful of lies' and black swans', http://www.stabilisationunit.gov.uk/stabilisation-and-conflict-resources/thematic/doc_details/61-skyful-of-lies-and-black-swans.html (accessed 25/09/2012)

Stanford Persuasive Tech Lab (2014), *What is Captology?* http://captology.stanford.edu/about/what-is-captology.html (accessed 11/09/2014)

Steckman, L. (2014), 'The Use of Shared Socio-Cultural Information and Research Validation', in Ehlschlaeger, C. (ed.), *Understanding Megacities with the Reconnaissance, Surveillance, and Intelligence Paradigm,* SMA White Volume, April 2014

Stewart, K. (2012), 'NPS' CORE Lab Rethinks Traditional Intelligence Analysis', *Naval Postgraduate School,* 13/09/2012, http://www.nps.edu/About/News/NPS-CORE-Lab-Rethinks-Traditional-Intelligence-Analysis.html (accessed 15/09/2014)

Stoebner, G. and Wedlake, J. (2012), *Using Cyber Capabilities to Inform and Influence,* Thesis at Naval Postgraduate School, http://calhoun.nps.edu/bitstream/handle/10945/27908/12Dec_Stoebner_Wedlake.pdf?sequence=1 (accessed 15/09/2014)

Strobel, W. (2008), 'The Phillipines: America's other war on terrorism', *McClatchy DC,* 22/10/2008, http://www.mcclatchydc.com/welcome_page/?shf=/2008/10/22/54611_the-philippines-americas-other.html (accessed 09/09/2014)

Subrahmanian, V.S. (ed.) (2013), *Handbook of Computational Approaches to Counterterrorism,* Springer: London

Suen, C., Huang, S., Eksombatchai, C., Sosič, R., Leskovec, J. (2013), 'NIFTY: A System for Large Scale Information Flow Tracking and Clustering', http://cs.stanford.edu/people/jure/pubs/nifty-www13.pdf (accessed 15/09/2014)

Surowiecki, J. (2004), *The Wisdom of Crowds: Why the Many Are Smarter Than the Few,* New York: Anchor Books

Sussman, G. (ed.) (2011), *The Propaganda Society: Promotional Culture and Politics in Global Context,* Oxford: Peter Lang

Sussman, G. (2012), 'Systemic Propaganda as Ideology and Productive Exchange', *Triple C,* 10(2), pp 474-487

Sussman, G. and Krader, S. (2008), 'Template Revolutions: Marketing U.S. Regime Change in Eastern Europe', *Westminster Papers in Communication and Culture,* 5(3), pp 91-122

Tangey, J. and Lytle, J. (2008), 'Preface', in Liu, H., Salerno, J. and Young, M. (eds), *Social Computing, Behavioral Modeling, and Prediction, Proceedings of 1st International Conference,* London: Springer

Tatham, S. (2006), *Losing Arab Hearts and Minds,* London: Hurst and Company

Tatham, S. (2008), *Strategic Communication: A Primer,* ARAG: Defence Academy of the United Kingdom

Taverner, A. (2007), 'Dimensions of Perception: Shaping the British Approach to information Strategy During Military Operations', in Maltby, S. and Keeble, R. (eds.) (2007), *Communicating War: Memory, Media and Military,* Bury St Edmonds: Arima

Taylor, P. (1995), *Munitions of the Mind: A history of propaganda from the ancient world to the present era,* Manchester: Manchester UP

Terranova, T. (2007), 'Futurepublic: On Information Warfare, Bio-racism and Hegemony as Noopolitics', *Theory, Culture & Society* 24(3), pp 125-145

Thaler, R. and Sunstein, C. (2009), *Nudge: Improving Decisions About Health, Wealth and Happiness,* London: Penguin

The Social Corps (2011), *The Marines – The Social Corps: The USMC Social Media Principles,* Quantico, VA: US Marine Corps

Thomas, T. (2007), 'Hezballah, Israel, and Cyber PSYOP', *IOSphere,* Winter 2008, pp 30-35

Thomson, A. (1992), *Smokescreen: The Media, the Censors, the Gulf,* Essex: Laburnham and Spellmount

Thornton, R. (2007), *Asymmetric WarfareL Threat and Response in the 21st Century,* Cambridge: Polity

Thrall, T. (2000), *War in The Media Age,* Hampton Press: Cresskill, NJ

Tilly, C. (1991) 'Domination, Resistance, Compliance…Discourse.', *Sociological Forum*, 6(3): pp 593-602

Tirman, J. (2008), 'Pentagon Priorities and the Minerva Program', *Social Science Research Council – The Minerva Controversy,* http://essays.ssrc.org/minerva/2008/10/09/tirman/ (accessed 15/09/2014)

Tiropanis, T., Hall, W., Shadbolt, N., Roure, D., Contractor, N. and Hendler, J. (2013), 'The Web Science Observatory', http://wstweb1.ecs.soton.ac.uk/wp-content/uploads/2013/08/The-Web-Science-Observatory.pdf (accessed 15/09/2014)

Tompkins, P. and Bos, N. (eds.) (2013), *Human Factors Considerations of Undergrounds in Insurgencies, Second Edition,* Fort Bragg, NC: US Army Special Operations Command

Trethewere, A., Corman, S., and Goodall, B. (2009), *Out of Their Heads and Into Their Conversation: Countering Extremist Ideology,* Report by the Consortium for Strategic Communication, http://www.comops.org/article/123.pdf (accessed 15/09/2014)

Trilling, D. (2011), 'Propagandistan', *Foreign Policy,* 22/11/2011, http://www.foreignpolicy.com/articles/2011/11/21/propagandastan (accessed 13/09/2014)

Tufekci, Z. (2011), 'Delusions Aside, the Net's Potential is Real', *The Atlantic,* 12/01/11 http://www.theatlantic.com/technology/archive/2011/01/delusions-aside-the-nets-potential-is-real/69370/ (accessed 10/05/12)

Tumber, H. and Webster, F. (2006), *Journalists Under Fire: Information War and Journalistic Practice,* London: Sage

Turk, V. (2014), 'As Obama Speaks, Why is the UK So Quiet on Surveillance?', *Vice Motherboard,* 17/01/2014, http://motherboard.vice.com/blog/as-obama-speaks-why-is-the-uk-so-quiet-on-surveillance (accessed 27/01/2014)

Turse, N. (2012), *The Changing Face of Empire: Special Ops, Drones, Spies, Proxy Fighters, Secret Bases, and Cyberwarfare,* Chicago: Haymarket Books

TweetTracker (2014), TweetTracker homepage, http://tweettracker.fulton.asu.edu/ (accessed 15/09/2014)

Ulicny, B. (2008), 'Modeling Malaysian Public Opinion by Mining the Malaysian Blogosphere', Liu, H., Salerno, J. and Young, M. (eds), *Social Computing, Behavioral Modeling, and Prediction,* Proceedings of 1st Conference, London: Springer

Urban, M. (2010), *Task Force Black: The Explosive True Story of the SAS and the Secret War in Iraq,* Little, Brown: London

US Advisory Commission on Public Diplomacy (2011), *Edited Transcript of the Public Meeting of the U.S. Advisory Commission on Public Diplomacy,* 29/11/2011, http://www.state.gov/documents/organization/178912.pdf (accessed 15/09/2011)

USAF (US Air Force) – *Functional Concept for Cyberspace Operations,* (2010), Peterson, Colorado: Air Force Space Command

USAF (US Air Force) – *FY2012.1 Topics* (2012), *Small Business Innovation Research Topics 2012,* http://www.acq.osd.mil/osbp/sbir/solicitations/sbir20121/af121.pdf (accessed 15/09/2014)

US Army – *APD 3-05* (2012), *Special Operations,* Washington, DC: Headquarters, Department of the Army

US Army – *ATP 3-05.20* (2013), *Special Operations Intelligence,* Washington, DC: Headquarters, Department of the Army

US Army - *FM 3-05.301* (2007), *Psychological Operations Process Tactics, Techniques, and Procedures,* Washington, DC: Headquarters, Department of the Army

US Army – *FM 3-13* (2013), *Inform and Influence Activities,* Washington, DC: Headquarters, Department of the Army

US Army – *FM 3-55* (2013), *Information Collection,* Washington, DC: Headquarters, Department of the Army

US Army – *FM 3-38* (2014), *Cyber and Electromagnetic Activities*, Washington, DC: Headquarters, Department of the Army

US Army – *Training Circular 18-01* (2010), *Special Forces Unconventional Warfare,* Washington, DC: Headquarters, Department of the Army

US Army/Marine Corps – *FM 2.01.3* (2009), *Intelligence Preparation of the Battlefield/Battlespace,* Washington, DC: Departments of the Army and Navy

US Army/Marine Corps – *FM 3-24,* (2006), *The Counterinsurgency Field Manual,* Washington, DC: Headquarters, Department of the Army

US Army Office of the Chief of Public Affairs (2011), *The United States Army Social Media Handbook,* Washington, DC: Online and Social Media Division of Office of the Chief of Public Affairs

USA Today (06/12/2013), 'Special Operations Command Becoming Emerging Player in Propaganda War', 13/12/2013, http://stratrisks.com/geostrat/9842 (accessed 12/09/2014)

US CYBERCOM – *Wargame 13* (2013), Training package for Cyber Wargare 13, https://www.fbcinc.com/e/WarGame/files/Cyber_Wargame_Welcome_Execution_Read-Ahead_v7b.pdf (accessed 11/12/2013)

US Embassy, Abuja (2009), 'Nigeria: Mission Plans for POTUS Ghana Speech Event', Leaked cable from 09/07/2009, http://www.wikileaks.org/plusd/cables/09ABUJA1256_a.html (accessed 13/09/2014)

US Joint Warfighter Command (2010), *Commander's Handbook for Strategic Communication and Communication Strategy,* US Joint Warfighter Center: Suffolk, Virginia

USMC (United States Marine Corps) Social Media (2014), *Marine Corps Social Media,* http://www.marines.mil/News/SocialMedia.aspx (accessed 09/11/2014)

US Senate – *Report 113-004* (2013), 'Limitation on funding for United States Special Operations Command National Capital Region, hearing for National Defense Authorization Act for FY 2014, http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp113DzuqB&r_n=sr044.113&dbname=cp113&&sel=TOC_271971& (accessed 13/09/2014)

US Strategic Command (2011), *US Strategic Command, History,* http://www.stratcom.mil/history/ (accessed 12/09/2014)

Van Burnen, P. (2012), 'Obama's War on Whistleblowers', *Mother Jones,* 12/06/2012, http://www.motherjones.com/politics/2012/06/obamas-whistleblowers-stuxnet-leaks-drones (accessed 25/09/2012)

Vanden Brook (2013), 'Report raps military propaganda efforts as ineffective', http://www.usatoday.com/story/news/nation/2013/05/23/military-propaganda-operations-poorly-coordinated-often-ineffective/2354235/ (accessed 13/09/2014)

Verilio, P. (2000), *The Information Bomb,* Verso: London

Ver Steeg, G. and Galstyan, A. (2011), 'Information Transfer in Social Media', http://arxiv.org/pdf/1110.2724v1.pdf (accessed 15/09/2014)

Waade, A. (2004), 'Mediatization of the tourist experience; cultural impacts on hyper tourism' Paper presented at 13th Nordic Symposium in Tourism and Hospitality Research, Denmark, http://www.13thnordic.aau.dk/ocs/viewabstract.php?id=61&cf=1 (accessed 25/09/2012)

Waldman, M. (2010), *Golden Surrender? The Risks, Challenges, and Implications of Reintegration in Afghanistan,* Afghanistan Analysis Network, http://www.humansecuritygateway.com/documents/AAN_GoldenSurrender_TheRisksChallengesAndImplicationsOfReintegrationInAfghanistan.pdf (accessed 25/09/2012)

Walker, S. (2013), U.S. Fleet Cyber Command, U.S. Tenth Fleet presentation, http://cryptome.org/2013/10/fcc-10th.pdf (accessed 12/09/2014)

Waller, M. (2007), *Fighting the War of Ideas like a Real War: Messages to Defeat the Terrorists,* Washington, DC.: The Institute of World Politics

Wallin, M. (2012), *The New Public Diplomacy Imperative: America's Vital Need to Communicate Strategically,* The American Security Project: Washington, DC

Wallsten, K. (2007), 'Agenda Setting and the Blogosphere: An Analysis of the Relationship betweein Mainstream Media and Political Blogs', *Review of Policy Research,* 24(6), pp 567-587

Wall Street Journal (17/06/2013), 'Corruption Currents: From Mayor of Montreal Arrested to Offshore Leaks Database', *Risk & Compliance Journal,* http://blogs.wsj.com/riskandcompliance/2013/06/17/corruption-currents-from-mayor-of-montreal-arrested-to-offshore-leaks-database/ (accessed 13/09/2014)

Wall Street Journal (26/07/2013), 'Corruption Currents: From Firing Squads to Snowden', *Risk & Compliance Journal,* http://blogs.wsj.com/riskandcompliance/2013/07/26/corruption-currents-from-firing-squads-to-snowden-sanctions/ (accessed 13/09/2014)

Wall Street Journal (13/12/2013), 'Corruption Currents: From Sextape Scandal to Halting Nuclear Deal With Iran', *Risk & Compliance Journal,* http://blogs.wsj.com/riskandcompliance/2013/12/13/corruption-currents-from-sextape-scandal-to-halting-nuclear-deal/ (accessed 13/09/2014)

Waltz, E. (2010a), 'HSCB Analytic Support to Influence Planning', *HSCB Newsletter No 7,* Fall 2010, pp 4-5

Waltz, E. (2010b), 'Anticipatory Intelligence Analysis: Integrating Multiple Models for Joint Intelligence Preparation', Presentation for BAE Systems, http://predictiveanalytics.pnnl.gov/isi2010_conference/presentations/anticipatory_waltz.pdf (accessed 15/09/2010)

Wang, X. (2013), *Connecting Users with Similar Interests for Group Understanding,* PhD thesis at Arizona State University

Ward, V. (2012), 'Officer who struck out at Ian Tomlinson had 'lost control', *The Telegraph,* 18/06/2012, http://www.telegraph.co.uk/news/uknews/crime/9339247/Officer-who-struck-out-at-Ian-Tomlinson-had-lost-control.html# (accessed 25/09/2012)

Ward, M., Beger, A., Cutler, J., Dickenson, M., Dorff, C. and Radford, B. (2013), 'Comparing GDELT and ICEWS Event Data', mdwardlab.com/sites/default/files/GDELTICEWS_0.pdf (accessed 15/09/2014)

Ware, C., Wright, W. and Pioch, N. (2013a), 'Visual Thinking Design Patterns', http://www.stresearch.com/Documents/WareEtAl_VTDP_6.pdf (accessed 15/09/2014)

Ware, C., Pioch, N. and Jones, E. (2013b), 'Visual Thinking Algorithms for Visualization of Social Media Memes, Topics, and Communities', http://www.stresearch.com/Documents/WarePiochJones-SocMedVis2013-final.pdf (accessed 15/09/2014)

Warnso, A. (2014), CV 'Arabic Translator Resume in Tampa, Florida' posted on FindJobz.com, http://www.findjobz.com/resume/boRRHMI1ydw=/arabic-translator-l-tampa-florida-33609 (accessed 15/09/2014)

Washington Times (2011), 'Editorial: Obama's Internet Passport', *The Washington Times,* 13/01/2011, http://www.washingtontimes.com/news/2011/jan/13/obamas-internet-passport/ (accessed 25/09/2012).

Watson, T. (2012), 'The lobbyists, the Russians, Google and "wife beater"', *Tom-Watson.co.uk,* 02/01/2012, http://www.tom-watson.co.uk/2012/01/the-lobbyists-the-russians-google-and-wife-beater (accessed 15/09/2014)

Weber, M., Owen, D., Strong,. T. and Livingstone, R. (2004), *Max Weber: The Vocation Lectures,* Indianapolis: Hackett

Webster, F. (2003), 'Information Warfare in an Age of Globalization', in Thussu, D. and Freedman, D. (eds.) (2003), *War and The Media,* London: Sage

Webster, S. (2011a), 'Revealed: Air Force ordered software to manage army of fake virtual people', *Raw Story,* 18/02/2011, http://www.rawstory.com/rs/2011/02/18/revealed-air-force-ordered-software-to-manage-army-of-fake-virtual-people/ (accessed 28/09/11)

Webster, S. (2011b), 'Exclusive: Military's 'persona' software cost millions, used for 'classified social media activities', *Raw Story,* 22/02/2011, http://www.rawstory.com/rs/2011/02/22/exclusive-militarys-persona-software-cost-millions-used-for-classified-social-media-activities/ (accessed 15/09/2011)

Wei, X., Valler, N. and Prakash, A. (2012), 'Competing Memes Propagation on Networks: A Case Study of Composite Networks', http://www.cs.cmu.edu/~badityap/papers/composite-ccr12.pdf (accessed 15/09/2014)

Weimann, G. (2010), 'Terror on Facebook, Twitter, and YouTube', *Brown Journal of World Affairs,* XVI(II), pp 45-54

Weinberger, S. (2012), 'A data-driven war on crime', *Nature,* Vol 484, Issue 7392, http://www.nature.com/news/a-data-driven-war-on-crime-1.10389 (accessed 15/09/2014)

Weiss, L., Briscoe, E., Hayes, H., Kemenova, O., Harbert, S., Li, F., Lebanon, G., Stewart, C., Steiger, D., and Foy, D. (2013), 'A Comparative Study of Social media and Traditional Polling in the Egyptian Uprising of 2011', in Greenberg, A., Kennedy, W., and Bos, N. (eds) (2013), *Social Computing, Behavioral-Cultural Modeling and Prediction,* Proceedings of 6th Conference, London: Springer

Weizman, E. (2006), *Hollow Land: Israel's Architecture of Occupation,* Verso: London

Weizman, E. (2011), T*he Least of All Possible Evils: Humanitarian Violence from Arendt to Gaza*, London: Verso

Welsh, W. (2014), 'Cyber warriors: The next generation', *Defense Systems,* 23/01/2014, http://defensesystems.com/Articles/2014/01/23/Next-generation-cyber-warriors.aspx?Page=1&p=1 (accessed 12/09/2014)

Weng, L, Ratkiewicz, J., Perra, N., Gonçalves, B., Castillo, C., Bonchi, F., Schifanella, R., Menczer, F. and Flammini, A. (2013), 'The Role of Information Diffusion in the Evolution of Social Networks', http://arxiv.org/pdf/1302.6276.pdf (accessed 15/09/2014)

West, R., & Turner, L. H. (2000), *Introducing communication theory: Analysis and application*, Mountain View: Mayfield

Wheaton, K. and Richey, M. (2014), 'The Potential of Social network Analysis in Intelligence', *e-International Relations,* 09/01/2014, http://www.e-ir.info/2014/01/09/the-potential-of-social-network-analysis-in-intelligence/ (accessed 15/09/2014)

Whitehead, N. and Finnström, S. (2013), *Virtual War and Magical Death,* London: Duke University Press

Whitlock, C. (2013), 'Somali American caught up in a shadowy Pentagon counterpropaganda campaign', *Washington Post,* 08/07/2013, http://www.washingtonpost.com/world/national-security/somali-american-caught-up-in-a-shadowy-pentagon-counterpropaganda-campaign/2013/07/07/b3aca190-d2c5-11e2-bc43-c404c3269c73_story_1.html (accessed 15/09/2014)

Williams, M. (2003), 'Words, Images, Enemies: Securitization and International Politics', *International Studies Quarterly* 47: 511-531

Williams, P. (2010), 'Amnesty, Reconcilliations and Reintegration: Conflict Termination in Counterinsurgency', US Military mongraph http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA523165 (accessed 25/09/2012)

Wilkerson, L. (2009), 'Guest Post: Some Truths About Guantanamo Bay', *Washington Note,* 17/03/2009, http://washingtonnote.com/some_truths_abo/ (accessed 15/09/2014)

Wilson, C. (2010), 'Searching for Saddam: Why social network analysis hasn't led us to Osama bin Laden', *Slate,* 26/02/2010, http://www.slate.com/articles/news_and_politics/searching_for_saddam/2010/02/searching_for_saddam.html (accessed 15/09/2014)

Wilson, J. (2012), 'MARFORCYBER: Marines Fight In a New Domain', *Defense Media Network,* 05/01/2012, http://www.defensemedianetwork.com/stories/marforcyber-marines-fight-in-a-new-domain/ (accessed 12/09/2014)

Wilson, T. (1979), 'Lord Bryce's Investigation into Alleged German Atrocities in Belgium, 1914-15), *Journal of Contemporary History,* 1979 (14), pp 369-383

Wolf, N. (2013), 'JSoc: Obama's secret assassins', *The Guardian,* 03/02/2013, http://www.theguardian.com/commentisfree/2013/feb/03/jsoc-obama-secret-assassins (accessed 11/09/2014)

World Bank (2013a), Population (Total), http://data.worldbank.org/indicator/SP.POP.TOTL (accessed 13/09/2014)

World Bank (2013b), Internet users (per 100 people), http://data.worldbank.org/indicator/IT.NET.USER.P2 (accessed 13/09/2014)

Wright, S. and Reinhold, S. (2011), ''Studying Through': A Strategy for Studying Political transformation. Or Sex, Lies, and British Politics', in Shore, C. Wright, S. and Pero, D. (eds.) *Policy Worlds: Anthropology and Analysis of Contemporary Policy,* Oxford: Berghan Books

Wurzman, R. and Giordano, J. (2014), '"NEURINT" and Neuroweapons: Neurotechnologies in National Intelligence and Defense', in Giordano, J. (ed.), *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Conerns,* Boca Raton, FL: CRC Press

Yahoo! News (15/11/2013), 'Al-Shabaab Launches Anti-Smartphone Campaign', *SA Breaking News (Yahoo! South Africa),* http://za.news.yahoo.com/al-shabaab-launches-anti-smartphone-campaign-071241239.html (accessed 13/09/2014)

Yang, S., Greenberg, A. and Endsley, M. (2012), *Social Computing, Behavioral-Cultural Modeling and Prediction*, Proceedings of 5th Conference, London: Springer

Yannakogeorgos, P. (2013), 'Considerations on Emergent Cyber Trends and Technologies', in Reynolds, M. and Lyle, D. (eds.), *Strategic Multi-Layer Assessment Periodic White Paper 2013,* Washington, DC: NSI

Young, J. (2012), 'The Unabomber's Pen Pal', *The Chronicle of Higher Education,* 20/05/2012, http://chronicle.com/article/The-Unabombers-Pen-Pal/131892/ (accessed 25/09/2012)

Yousufzai, Z. (2014), LinkedIn profile of Zafar Yousufzai, http://www.linkedin.com/pub/zafar-yousufzai/59/878/780 (accessed 15/09/2014)

YouTube – ccpnmike (2012), Lighthouse Brief video posted by user ccpnmike, https://www.youtube.com/watch?v=VTMyxpx1OvM (accessed 15/09/2014)

Yuce, S., Agarwal, N. and Wigand, R. (2013), 'Mapping Cyber-Collective Action among Female Muslim Bloggers for the *Women to Drive Movement*' , in Greenberg, A., Kennedy, W., and Bos, N. (eds), *Social Computing, Behavioral-Cultural Modeling and Prediction,* Proceedings of 6th Conference, London: Springer

Zafarani, R., Cole, W., and Liu, H. (2010), 'Sentiment Propagation in Social Networks: A Cast Study in LiveJournal', Chai, S., Salerno, J. and Maybry, P. (eds.), *Advances in Social Computing, Proceedings of Third International Conference on Social Computing, Behavioural Modeling, and Prediction,* SBP 2010, Lecture Notes in Computing Science 6007, London: Springer

Zafarani, R., Abbasi, M. and Liu, H. (2014), *Social Media Mining: An Introduction,* New York: Cambridge University Press

Zahran, G. and Ramos, L. (2010), 'From Hegemony to Soft Power', in Parmer, I. and Cox, M., *Soft Power and US Foreign Policy: Theoretical, Historical and Contemporary Persepctives,* New York: Routledge

Zaharna R.S. (2007), 'The Soft Power Differential: Networked Communicaiton and Mass Commmunication in Public Diplomacy', *The Hague Journal of International Diplomacy,* 2(2007) pp 213-228

Zajácz, R. (2013), 'WikiLeaks and the problem of anonymity: A network control perspective', *Media, Culture, Society,* 35(4), pp 489-505

Zalman, A. (2010) 'Narrative as an Influence Factor in Information Operations, *IO Journal,* 2(3), pp 4-10

Zetter, K. (2011), 'How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History', *Wired – Threat Level,* 11/07/2011, http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/ (accessed 09/09/2014)

Zhou, W., Jin, H., Liu, Y. (2012), 'Community Discovery and Profiling with Social Messages', http://wan.poly.edu/KDD2012/docs/p388.pdf (accessed 15/09/2014)

Zimmerman, D. (2012), '4th Psychological Operations Group (PSYOP)', *Defense Media Network,* 02/12/2012, http://www.defensemedianetwork.com/stories/4th-misga-45th-anniversary-the-word-will-conquer/ (accessed 09/09/2014)

Zunes, S. and hundreds of signatories (2008), 'Open Letter in Support of Gene Sharp and Strategic Nonviolent Action', http://stephenzunes.org/wp-content/uploads/2010/12/Open-Letter_Academics_Zunes.pdf (accessed 13/09/2014)