

Disappearing violence: JSOC and the Pentagon's new cartography of networked warfare

Security Dialogue

44(3) 185–202

© The Author(s) 2013

Reprints and permissions:

sagepub.co.uk/journalsPermissions.nav

DOI: 10.1177/0967010613485869

sdi.sagepub.com



Steve Niva

International Politics and Middle East Studies, Evergreen State College, Olympia, WA, USA

Abstract

In the twilight of the USA's ground wars in Iraq and Afghanistan, there has been an expanding shadow war of targeted killings and drone strikes outside conventional war zones, where violence is largely disappeared from media coverage and political accountability. While many attribute the growth in these shadowy operations to the use of new technologies and platforms such as drones, this article argues that the central transformation enabling these operations is the increasing emergence of network forms of organization within and across the US military and related agencies after 2001. Drawing upon evidence from unclassified reports, academic studies, and the work of investigative journalists, this article will show that elements within the US military and related agencies developed in the decade after 2001 a form of shadow warfare in which hybrid blends of hierarchies and networks combine through common information and self-synchronization to mount strike operations across transnational battle spaces. But, rather than a top-down transformation towards networks, this article will show how it was the evolution of the Joint Special Operations Command (JSOC) from an elite strike force into a largely autonomous networked command that has been central to this process. Although drone strikes have received the bulk of critical attention in relation to this expanding shadow war of targeted killing, this often-lethal networked warfare increasingly resembles a global and possibly permanent policing operation in which targeted operations are used to manage populations and threats in lieu of addressing the social and political problems that produce the threats in the first place.

Keywords

security studies, networks, global governance, counterinsurgency, US foreign policy

In bitter, bloody fights in both Afghanistan and Iraq, it became clear to me and to many others that to defeat a networked enemy we had to become a network ourselves. (McChrystal, 2011)

Corresponding author:

Steve Niva

Email: nivas@evergreen.edu

We're the dark matter. We're the force that orders the universe but can't be seen. (anonymous Navy Seal member of Joint Special Operations Command, cited in Priest and Arkin, 2011: 222)

Introduction

In the twilight of the USA's ground wars in Iraq and Afghanistan, there has been a reconfiguration of the political space of US military operations and violence through targeted kill-or-capture raids across diverse geographies carried out by special operations forces, the Central Intelligence Agency (CIA), and other US agencies. Although the targeted killings of Osama bin Laden in Pakistan and the US-born Al-Qaeda cleric Anwar al-Awlaki in Yemen briefly thrust this shadow war into the public spotlight, these operations are merely the visible trace of a dense matrix of highly secretive operations that occur on a daily basis across the globe (see Schmitt and Shanker, 2011; Sanger, 2012; Turse, 2012). The special operations forces raid against Bin Laden undertaken by SEAL Team 6, for example, was only one of nearly two thousand similar strike missions undertaken in both Afghanistan and Pakistan in the several years prior to that raid (Schmidle, 2011). Such kill-or-capture strikes were becoming so casual and common in terms of frequency that one US military official commented that it was like 'mowing the lawn' (cited in Schmidle, 2011). On the night of the Bin Laden strike, special operations forces personnel based in Afghanistan conducted 12 other missions in which they captured or killed between 15 and 20 targets. The sheer scale of these operations in Afghanistan, where hundreds of suspected insurgents were being killed or captured on a monthly basis, led retired Colonel John Nagl to tell PBS's *Frontline* (2011) that the capabilities of this shadow war amount to 'an almost industrial-scale counterterrorism killing machine'.

The expansion of this transnational shadow war reminds us that although Iraq and Afghanistan are typically seen as the prime examples of evolving forms of American warfare, they never constituted the totality of the military engagements known as the 'war on terror' under President George W. Bush that were continued under President Barack Obama. From the beginning, the USA claimed the right to act anywhere that a terrorism-related threat was alleged to exist, constituting a form of military engagement that the 2006 Pentagon's *Quadrennial Defense Review* characterized as the 'long war' that would require a new array of operations, including 'wars in countries we are not at war with' (US Department of Defense, 2006: vi). Under the Obama administration, this shadowy form of military engagement achieved a new density and centrality within US military and related agencies, such that it has now become a primary theatre of contemporary American warfare. Its signature actions are secretive and targeted kill-or-capture operations that do not so much move across static borders as render them contingent, producing proliferating 'grey areas' in which violence is largely disappeared from media coverage and political accountability.

Many contend that this increasingly visible shadow war is being driven by the employment of new 'information age' technologies and platforms, especially the robotic drones or unmanned aerial vehicles (UAVs) that are now playing greater roles in this expanded battlefield (Rohde, 2012; Miller, 2011; Lee, 2011). In a perceptive analysis of the rise of what he terms 'liquid warfare', Nick Denes (2010: 176) argues that UAVs play the central role in linking soldiers to advanced technologies derived from what military theorists in the 1990s termed the 'Revolution in Military Affairs' (RMA), with the integration of the two making possible these new forms of targeted warfare: 'The UAV now functions as the RMA's organizational hub, its revolutionary motor, and its symbolic paradigm.' More broadly, Peter Singer (2009: 191–195) has argued that the proliferation of new robotic platforms across the battlefield is leading to a 'fundamental revolution' in warfare itself.

Yet, while 'information age' technologies and platforms like UAVs have become essential tools in these operations, this article contends that the central transformation enabling this shadow warfare has less to do with new technologies and more to do with new forms of social organization – namely, the increasing emergence of *network* forms of organization within and across the US military after 2001. Writing prior to and after 2001, a number of scholars noted that although the US military had adopted many technological elements of the RMA-inspired doctrine of network-centric warfare, the full realization of more networked forms of warfare depended upon the shift from hierarchical to networked forms of organization, which did not appear forthcoming even after 2001 (Arquilla and Ronfeldt, 1996, 1997, 2001; Bousquet, 2008, 2009; Duffield, 2002; Hardt and Negri, 2004). Drawing upon evidence from unclassified reports, academic studies, and the work of investigative journalists, however, this article will show that many elements of this shift have since come to pass. Elements within the US military and related agencies engaged in the 'long war' after 2001 have increasingly adopted more networked forms of organization, which has made possible the integration of UAVs and new technologies into more networked forms of warfare that resemble what Arquilla and Ronfeldt (2001: 16) term 'counternetwar', in which hybrid blends of hierarchies and networks operate through common information and self-synchronization to mount strike operations across shadowy transnational battle spaces.

But, rather than a top-down transformation from hierarchies to networks, this article will show that this transformation came about through a largely self-organized and bottom-up process of military adaptation in the peripheries of the 'long war', at the center of which was the evolution of the Joint Special Operations Command (JSOC) from an elite special operations strike force into an 'organizational hub and revolutionary motor' of networked forms of organization and warfare across the military. The article will trace how JSOC, as both incubator and exemplar, became a largely autonomous network and instigated unprecedented horizontal networking across previously compartmentalized US military commands and agencies who share information and combine in shadowy targeted operations around the world. Although drone strikes have received the bulk of critical attention in relation to these types of operations, this form of networked warfare increasingly resembles, as Hardt and Negri (2004: 13) and others note, a global and possibly permanent policing operation in which targeted operations are used to continually manage populations and threats in lieu of addressing the social and political problems that produce the threats in the first place.

The networked emergence of counternetwar: From RMA to JSOC

A recurring theme in Eric Schmitt and Thom Shanker's (2011) *Counterstrike: The Untold Story of America's Secret Campaign Against Al-Qaida*, a journalistic account of US operations against alleged terrorist networks, is that these kinds of operations would not have been possible before 11 September 2001. Summarizing the mission on Bin Laden's compound in Pakistan, for example, US Defense Secretary Robert Gates asserted that 'this mission simply would not have been possible before' (cited in Schmitt and Shanker, 2011: 257). These operations utilized real-time surveillance and strike capabilities provided by drones, as well as an invisible army of spy satellites and banks of supercomputers that trawl phonelines and Internet transmissions – all of which did not exist or were just being tested before 2001. But, Defense Secretary Gates and other participants also frequently noted that it was the unprecedented horizontal cooperation and networked linkages between US military and intelligence actors and agencies such as the special operations forces, the

Central Intelligence Agency, and the National Security Agency (NSA) after 2001 that enabled the new operations to take place. 'One of the things we have seen since 9/11 is an extraordinary coming together, particularly of CIA and the military, in working together and fusing intelligence and operations in a way that just, I think, is unique in anybody's history,' said Gates days after the Bin Laden raid (cited in Schmitt and Shanker, 2011: 259). More than just new platforms and technologies, Schmitt and Shanker (2011: 258) concluded that the USA had developed new organizational forms and new doctrines to guide its fight against increasingly networked opponents: 'It was a network fighting a network.'

Although often overstating the extent to which US counterterrorism forces have truly become a 'network fighting a network', evidence from unclassified reports, investigative journalists, academic studies, and descriptions by participants indicate that there has been a significant embrace of more networked forms of organization within the US military and related agencies over the past decade, which has played a major role in making these operations possible (see, for example, Flynn et al., 2008; McChrystal, 2011; Ostlund, 2012; Priest and Arkin, 2011; Schmitt and Shanker, 2011; Sanger, 2012; Turse, 2012; Ucko, 2009, Urban, 2010). These accounts outline a growth in horizontal networking across the US military and related agencies involved with the 'war on terror' that includes elements of the special operations forces, the CIA, the NSA, the Federal Bureau of Investigation, and a variety of other organizations that share information and combine within an ongoing organizational matrix of operations around the world, often in real time. This networking has enabled a variety of new tactical and operational forms undertaken by increasingly decentralized and autonomous actors who launch raids across proliferating geographies.

The theoretical basis of this transformation was articulated by a number of scholars writing about the rise of networked warfare before and after 2001 who argued that American exploitation of more networked forms of warfare would only become possible once the US military had adopted more decentralized and networked forms of organization (Arquilla and Ronfeldt, 1996, 1997, 2001; Bousquet, 2008, 2009; Duffield, 2002; Hardt and Negri, 2004). These scholars traced the rise of networked warfare to broader shifts in the organizational structure of global capitalism over the past several decades and the emergence of what Manuel Castells (1996: 151–200) described as the *network enterprise* as the generic institutional expression of the new global/informational economy. In contrast to more hierarchical forms of organization, networks are interconnected sets of decentralized components having significant autonomy, which combine to work together on the basis of shared information and a shared strategy (Duffield, 2002: 154). These scholars claimed that this development foreshadowed an era of networked actors that could challenge states by organizing 'sprawling networks more readily than can traditionally hierarchical nation-state actors' (Arquilla and Ronfeldt, 1997: 456). Drawing upon an analysis of the ways in which various technoscientific regimes have shaped techniques of modern warfare in different periods, Bousquet (2008: 923) contended that the global trend from cybernetic concepts towards 'chaoplectic' concepts of 'non-linearity, self organization and emergence' was leading to forms of warfare fought by decentralized and self-synchronizing networks able to bring force to bear in a new manner, similar to what Arquilla and Ronfeldt (2001: 6) conceptualized as 'netwar'.

Prior to 2001, the US military had embraced networked information technology as mandated by the Revolution in Military Affairs in the 1990s. This trend was reinforced by the US military's experiences in the 1991 Gulf War and aerial campaign in Kosovo, in which satellites, 'smart' weapons, and communications technology were believed to have increased the enormous relative power of the USA against conventional military opponents (Ucko, 2009: 51–53). Incoming Secretary of Defense Donald Rumsfeld (2002) rebranded the RMA as 'Defense Transformation' in 2001 and

sought to further institutionalize the new information technology-driven vision of the RMA as the way to fight the 'wars of the twenty-first century'. At the operational core of 'Defense Transformation' was the concept of network-centric warfare. Drawing a vision from large business organizations such as Wal-Mart, network-centric warfare seeks to capitalize on the synergistic effects of electronically linking decentralized actors together through common information in order to increase the power of individual nodes at the point of attack (Cebrowski and Garstka, 1998). This synergy would enable networks to engage in new tactical modes of operation by self-synchronizing forces who engage in 'organizing efforts resembling "packs" and "swarms"' (Alberts and Hayes, 2003: 169).

Nevertheless, despite the US military's adoption of elements of network-centric warfare, these scholars argued that the full realization of more advanced networked warfare implied in the network-centric warfare concept depended upon the adoption of more decentralized and networked forms of organization and doctrine, which did not appear forthcoming even long after 2001. Hardt and Negri (2004: 51–68), for example, argued that while the RMA dictated that traditional military apparatuses use communication networks more and more effectively, it was not enough just to mimic guerilla warfare at the tactical level. Rather, more significant changes 'would need also to involve the command structure and ultimately the form of social power in which the military apparatus is embedded' (Hardt and Negri, 2004: 59). They concluded that traditional, centralized, hierarchical military structures built for conventional warfare would be increasingly incapable of implementing adequate strategies for combating network opponents:

In order to combat and control network enemies, which is to say, in order for traditional sovereign structures themselves to become networks, imperial logics of political, military, and diplomatic activity on the part of the United States and other dominant nation-states will have to win out over imperialist logics and military strategy will have to be transferred from centralized structures to distributed network forms. (Hardt and Negri, 2004: 61–62)

Similarly, Bousquet (2008, 2009) noted that while network-centric warfare marked the onset of a doctrinal shift from cybernetic to chaoplexic forms of warfare owing to its emphasis on bottom-up coordination between decentralized networks who share common schema, command and control would need to become more decentralized in order to provide the autonomy, self-organization, and self-synchronization needed to make possible more chaoplexic forms of warfare. Because the RMA was largely premised on the notion that computers, telecommunications links, and precision-guided munitions would finally deliver the frictionless, automated operations associated with cybernetic warfare, Bousquet (2008: 928) points out that 'in several respects it has not significantly broken with cybernetic warfare and therefore may not in fact implement all the features of a truly chaoplexic way of warfare'. He concludes that the key change to unlock these new operational forms of war would have to come at the level of social organization:

Ultimately, chaoplexic warfare will depend more on doctrinal and organizational commitments than on any particular information technologies, which are liable to be employed to quite contrary purposes. The full arrival of chaoplexic warfare may therefore still lie ahead; but the debates around network-centric warfare clearly show an impetus towards greater decentralization and the use of the network form of organization within armed forces. (Bousquet, 2008: 929)

Although the full realization of distributed networks and chaoplexic warfare has not yet arrived – the US military has not become a distributed network fighting chaoplexic warfare – many elements of the social transformation towards networked forms of organization and warfare outlined by these scholars have come to pass over the past decade. Rumsfeld's 'transformation' vision of 'light footprints' and information dominance was found badly wanting in the quagmires of Iraq and Afghanistan. But, outside of the conventional battlefields, important sectors of the US military have increasingly adopted more decentralized networked forms of organization and doctrine. As these theorists anticipated, the shift from using networks to increasingly adopting the network form has enabled the emergence of forms of warfare similar to what Arquilla and Ronfeldt (2001: 16) term 'counternetwar', with elements of what Bousquet (2008, 2009) terms 'chaoplexic warfare', in which hybrid blends of hierarchies and decentralized networks operate through common information and self-synchronization to target and strike increasingly networked opponents. Unlike operations conducted by more hierarchical actors, the spatial character of these operations 'tends to defy and cut across standard spatial boundaries, jurisdictions, and distinctions between state and society, public and private, war and crime, civilian and military, police and military, and legal and illegal ... to operate in the cracks and gray areas of the society' (Arquilla and Ronfeldt, 1996: 13).

But, rather than a linear process of institutional transformation from above, the organizational embrace of networks has emerged through the largely self-organized and bottom-up expansion of networks from the peripheries of the 'long war' to the centers of military organization and operational practice over the past decade. In his discussion of adaptive capacities of networks, Bousquet (2008: 924) noted that 'self-organization is the process by which the autonomous interaction of individual entities results in the bottom-up emergence of complex systems' that can 'display the ability to change and learn from experience'. Following this bottom-up process, this article will show how the evolution of the Joint Special Operations Command (JSOC) from an elite clandestine strike force to a largely autonomous networked command has played a major role in generating the expansion of networked forms of organization and warfare within the US military since 2001. The article will trace three key developments in the bottom-up process by which the largely self-organized emergence of JSOC as a networked force using more chaoplexic forms of warfare has contributed to the development of the shadowy counternetwar operations that we see today: how JSOC became a network; how it networked with the broader US military in Iraq after 2007; and how its network expanded to conduct operations outside of official war zones.

JSOC becomes a network

The emergence of JSOC as a central vector of the social transformation from hierarchical to more networked organizational forms within the US military can be traced to the years immediately after 2001 when, in defining the battlefield of the 'global war on terror' as *global*, the Bush administration effectively reserved the right to intervene anywhere it felt necessary, ostensibly under the auspices of counter-terrorism. In addition to the Authorization for Use of Military Force passed by the US Congress on 14 September 2001 that granted the president sweeping authority to use military force against those deemed responsible for the attacks that had taken place three days earlier, on 17 September 2001 President Bush also signed an open-ended Presidential Finding authorizing covert activities by the CIA and other agencies to kill or capture those responsible for the 2001 attacks, which Priest and Arkin (2009: 6) call the 'most sweeping and lethal covert action' in CIA history, effectively abrogating the existing US ban on assassinations. Within a year, senior officials at the Pentagon and the CIA reportedly began to develop broader plans for hunting, killing, or

capturing alleged terrorists and their associates around the world, developing target lists with authorizations to carry out strikes on these targets (Schmitt and Shanker, 2011: 34).

In this context, the key policy move that elevated JSOC to becoming what Priest and Arkin (2011: 237) term 'the dark matter that would shape the global war against al-Qaeda' came about largely as a bureaucratic maneuver by Rumsfeld, who sought to edge out the CIA and insert the Pentagon as the lead actor in covert anti-terror operations. Recognizing that conventional military forces were insufficient to undertake these operations, in 2002 Secretary of Defense Rumsfeld turned to the US Special Operation Command (SOCOM), a recent addition to the geographic regional military commands, to act as the lead unified military command for planning and synchronizing the 'global war on terror', a decision formally authorized in the 2004 Unified Command Plan identifying SOCOM as the lead (Ryan, 2011). Although the CIA had led special operations forces in Afghanistan, Rumsfeld followed this up on 16 September 2003 by signing an execute order ('EXORD') that placed JSOC at the center of global counter-terrorism operations (Priest and Arkin, 2011: 236). The EXORD listed 15 nations and the types of operations (kill, capture or provide assistance) permitted under various scenarios, and it gave the pre-approvals required for JSOC to carry them out. Unlike the CIA, whose *covert* operations under Title 50 of the US Code required congressional notification, JSOC's *clandestine* operations were governed by Title 10 of the US Code governing traditional military activity, which relaxed this standard. In other words, JSOC was given the rare authority to select individuals for its kill list and then to kill or capture them without notification, which amounted to considerable executive authority, leading critics such as Seymour Hersh (2008) to refer to JSOC as 'an executive assassination ring'.

But, the organizational breakthrough towards networks came about after the appointment of General Stanley McChrystal, a former Army Ranger, as head of JSOC from 2003 to 2008. McChrystal began building JSOC as a networked command that would link with, draw from, and contribute to actions across the military structure by breaking down bureaucratic barriers to cooperation and enhancing communications between the various elements. In contrast to the centralized and separate military commands that constitute the pyramid structure of the US military, JSOC was itself established as a 'joint' command made up of elements of the military's most elite units, including the Navy's SEAL Team 6, sometimes called the Naval Special Warfare Development Group or DEVGRU; the Army's 1st Special Forces Operational Detachment-Delta, or Delta Force; the 75th Ranger Regiment; the 160th Special Operations Aviation Regiment; the Air Force's 24th Special Tactics Squadron; plus elements from other even more secret units and intelligence organizations (Feickert, 2006). As one retired SEAL officer recounted, before McChrystal 'we were really good at what we did [in JSOC], but we were pirates and totally disorganized' (cited in Naylor, 2011). Upon taking over, 'McChrystal took the Ranger discipline, applied it systematically to the organization and then completely changed the way the organization works within the government, within the Defense Department and then within the greater interagency', referring to the US military and intelligence agencies involved in the 'war on terror'.

Within three years, JSOC developed many of the elements and capacities of a networked form of organization composed of interconnected sets of decentralized and largely autonomous components that combine and work together on the basis of shared information and strategy. First, reflecting McChrystal's reported distaste for information hierarchies and preference for 'agile groupings' of information sharing drawn from a McKinsey management science approach, McChrystal set up an intranet with a common homepage, which allowed every member of JSOC to share intelligence and have access to real-time battlefield information (Urban, 2010: 53). Within a year after McChrystal's arrival, JSOC moved into a state-of-the-art Joint Operations Center in Balad, Iraq,

and had linked 65 stations around the globe to enable viewers to participate in twice-daily, 45-minute video teleconferences held by the general (Priest and Arkin, 2011: 246). Moreover, McChrystal spent his commander's discretionary fund not on hi-tech weaponry but on purchasing bandwidth, so that all the nodes of his network could speak to each other, sometimes during missions.

Second, McChrystal built bridges to the CIA and also recruited satellite analysts from the National Geospatial-Intelligence Agency, regional experts from the State Department, and surveillance specialists from the NSA as members of JSOC's extended network (Priest and Arkin, 2011: 242). By the summer of 2004, 'not only would every single troop in JSOC have access to a real-time picture of evolving targets on the battlefield but so would the unit's historic rivals: the CIA, the NSA, the FBI, the Defense Intelligence Agency, and even certain elements within the State Department' (Priest and Arkin, 2011: 241). In a sense, JSOC effectively became a networked experiment in intelligence crowd-sourcing as it expanded into a networked force. 'If you look at JSOC, you're looking at arguably the single most integrated, most truly joint command within the U.S. military,' said Andrew Exum (cited in Ackerman, 2011), who served in the Army's Ranger Regiment in Iraq and Afghanistan in 2003 and 2004 and who advised McChrystal as a civilian in 2009.

Finally, McChrystal reorganized JSOC into specialized 'Task Forces' in various locations across the world, sometimes subdivided into more specialized 'task forces' in particular locations. In Iraq, for example, the JSOC command known as TF 145 (Global Security, n.d.) was divided into four subordinate regional task forces:

- Task Force West, organized around a SEAL Team 6;
- Task Force Central, organized around a Delta squadron;
- Task Force North, organized around a Ranger battalion; and
- Task Force Black, organized around a British Special Air Service (SAS) squadron.

The various task forces were networked closely with intelligence agencies and with one another through what became known as *fusion centers*, the hi-tech hubs for JSOC's hybrid teams of special operations forces and intelligence and forensic professionals, political analysts, mapping experts, and computer specialists piloting unmanned aircraft. Most importantly, each TF 145 element was increasingly given greater operational autonomy, each with the ability to authorize a raid without seeking approval from the top of the TF 145 hierarchy.

This organizational decentralization and tactical autonomy was the key organizational innovation that enabled JSOC to experiment with more networked and increasingly chaotic operations in Iraq, where McChrystal had built a sophisticated network of soldiers and intelligence operatives to hunt Sunni insurgent leaders and decapitate Al-Qaeda in Iraq from 2003 to 2006 (Priest and Arkin, 2011: 228). TF 145's method of operating was to target a safe house, capture individuals, exploit whatever was found for intelligence, and use that to drive a new mission. The key difference between this operational style and previous ones was that each TF 145 unit had the authority to launch missions immediately based on raw intelligence, whereas in the past units would have had to bring intelligence material back to the rear and have it analyzed before striking again. This operational autonomy, combined with large amounts of intelligence generated on missions, created a faster operational tempo for the TF 145 elements and increasingly resembled what Arquilla and Ronfeldt (1997: 465) describe as '*sustainable pulsing* – swarm networks must be able to coalesce rapidly and stealthily on a target, then dissolve and redisperse, immediately ready to recombine for new pulses'.

The methodology behind this networked operational style is often attributed to McChrystal's top intelligence officer, then Brigadier General Michael Flynn, who developed a new approach to intelligence gathering. Flynn marshaled the diverse organizations within the US intelligence network – from the NSA, the CIA, and the State Department – in order to pool intelligence on individuals, known as 'massing intelligence', and turned to 'social network analysis' for measuring the number of direct interactions between individuals or 'nodes' in the network in order to reveal the structure and key elements of a network (MacGinty, 2010: 209–226). Emphasizing the speed of the collection, McChrystal and Flynn introduced the concept of 'F3EA' (find, fix, finish, exploit, and analyze), which meant obtaining new data from each raid that could be used to add to the target list for future raids, often within hours of the previous one (Schmitt and Shanker, 2011: 85). Flynn and two colleagues later gave an unclassified look into their methodology of F3EA in an article published in 2008 in which they emphasized the importance of massing all elements of 'intelligence, surveillance and reconnaissance' (ISR) on 'selected parts of the enemy's network', a method that became known as the 'unwavering eye' (Flynn et al., 2008: 57).

The result was that while the broader US military in Iraq was mired in the bloody and confusing process of waging a conventional war against insurgent groups among a civilian population, JSOC was emerging within a parallel universe within Iraq and elsewhere as a self-synchronized force experimenting with new forms of network-oriented hunt-and-kill operations. By the summer of 2005, JSOC teams undertook an estimated 300 raids per month, hitting targets every night, eventually turning their focus from traditional high-value targets to suspected local players and middle managers in insurgent networks (Urban, 2010: 81). During the spring of 2006, using the expanded bandwidth and constant surveillance by unmanned aircraft, JSOC executed a series of raids, known as Operation Arcadia, in which it hunted and killed large numbers of alleged Al-Qaeda operatives, ultimately leading to the 7 June 2006 killing of Abu Musab al-Zarqawi by a JSOC airstrike. Driven by McChrystal's central idea that the Al-Qaeda networks had to be dismantled faster than they could regenerate themselves, it was reported that JSOC often sacrificed target development and accuracy in the interests of high-tempo raids producing intelligence, resulting in an overall success rate that was less than 50%, with little information about civilian casualties (Priest and Arkin, 2011: 229). Moreover, the secret force of JSOC hunter-killer teams also had their own detention and interrogation centers, where accusations of torture and abuse were raised (Schmitt and Marshall, 2006).

Networked synergy in Iraq: JSOC becomes a machine

The next key development in the bottom-up emergence of more networked forms of organization and operations was the synergistic integration of the JSOC network into the more conventional US military battlespace in Iraq. It was during the 2007 'surge' in Iraq and the implementation of population-centric counterinsurgency doctrine (COIN) under General David Petraeus that the JSOC network became more visible and integrated within the broader US military command. Heretofore, JSOC had largely acted autonomously from broader regional commands as a largely parallel and separate universe of operations. During the 2007 'surge', however, JSOC was brought into increasing organizational and strategic synchronicity with the local command, which resulted in what Schmitt and Shanker (2011: 75) claim were 'new and more cordial relations between the conventional and Special Operations forces, historic rivals within the American military'. An unclassified publication of the US Army's Institute of Land Warfare prepared in 2012 by Colonel William Ostlund (2012: 6) noted that special operations forces in Iraq 'dramatically and continuously

increased internal and external coordination and cooperation [with local command] in order to increase [their] freedom of action – ability to operate – and achieve sought effects'. This enabled JSOC to leverage its networked capabilities to more fully develop its distinctive form of counter-netwar into what some participants called a 'machine' that could be deployed elsewhere, either within the conventional battlespace or outside of it.

The 2007 'surge' was presented to the American public as a major shift in military strategy away from conventional warfare towards defeating insurgencies indirectly by separating the civilian population from the insurgents through improving the security of the former and addressing their political grievances (US Department of the Army, 2007). As part of this strategy, US forces left their bases and began to set up walls, checkpoints, and outposts between and within neighborhoods and conducted more on-the-ground patrols to obtain intelligence about the local population, signaling a shift from conventional military operations to those more akin to domestic policing. But, alongside the publicized strategy, and only revealed in the later years of the 'surge', there was a major escalation of JSOC's networked operations across Iraq. While US troops built blast walls to separate populations and moved troops out of distant bases into neighborhoods to patrol, JSOC task forces fanned across the country to hunt and kill opponents either within or between the segmented enclaves. JSOC dramatically increased the number and pace of its operations to locate, target, and kill key individuals in groups that not only included Al-Qaeda in Iraq, but also members of the Sunni insurgency and renegade Shi'a militias. JSOC's TF 145, now renamed TF 16, continued to focus on Sunni insurgents, while a new command designated TF 17, drawn from Army Special Forces (Tier 2), was given the mission of focusing on Shi'a networks such as the Mahdi Army and Badr Brigades (Urban, 2010: 213).

In *The War Within*, Bob Woodward (2008a), the journalist who first drew attention to the escalation of JSOC's shadow war in Iraq after 2007, described how JSOC had used 'some of the most highly classified techniques' in the US government system of classification in 2006 and 2007 to target and kill Al-Qaeda and Shi'a militia fighters. Echoing this emphasis on the remarkable technological innovations employed by special operations forces in Iraq, David Kilcullen claimed that 'the capabilities for high-end special joint operations that exist now only existed in Hollywood in 2001' (cited in Warrick and Wright, 2008). Moreover, Woodward (2008b) contributed to the emerging myth of omniscient JSOC operators by claiming that JSOC operations were the most important factor in reducing the overall levels of violence in Iraq over the next few years from their 2006 levels. This claim ignores the arguably more important political developments leading in this direction, including the bloody sectarian partition of Baghdad, the Anbar Awakening in which tens of thousands of former Sunni insurgents turned against Al-Qaeda in Iraq, and the August 2007 suspension of Mahdi Army operations ordered by the militant Shi'a cleric Moqtada al-Sadr (Rosen, 2008).

But, what Woodward and others overlook is that it was JSOC's networked integration within the broader US military and intelligence community in Iraq that largely enabled it to utilize new technologies in ways that were unprecedented before that time. As Joint Chiefs of Staff Chairman Admiral Michael Mullen pointed out regarding these developments: 'It's been the synergy, it's been the integration that has had such an impact' (cited in Warrick and Wright, 2008). On the one hand, as an increasingly complex adaptive network, JSOC was able to successfully adapt to the new battlespace now occupied by conventional forces pursuing population-centric COIN, which employed concepts of operation similar to JSOC's networked warfare, such as constructing the population in terms of networks and advocating social network analysis as 'a tool for understanding the organizational dynamics of an insurgency and how best to attack or exploit it (US Department of the Army, 2007: 317). Another factor was the doctrinal synergy between population-centric counterinsurgency

and high-tempo kill-or-capture operations undertaken by JSOC. While Petraeus repeatedly emphasized the mantra 'you cannot kill your way out of an insurgency', the role of JSOC was not envisioned as a military solution to the insurgency. Rather, JSOC takedowns and operations were directed at 'irreconcilable' insurgent networks so that the conventional COIN troops could build up their presence and enhance security among the more 'reconcilable' populations. JSOC's role in all this was, according to one American commander, to act as 'a hammer which could be used to smash insurgent groups against the anvil of conventional forces' (cited in Urban, 2010: 252).

As a result of this synergy between JSOC and the broader military campaign, JSOC was able to accelerate its distinctive operational style of swarming against opponents' networks on and off the battlefield through accelerating campaigns, as opposed to targeting enemies in discrete engagements. JSOC operations increasingly did not aim to eliminate the center (or larger command) of a network, but rather were increasingly targeted against mid-level operatives within insurgent networks. The focus was on increasing the speed and the swarming effect of operations – which by many accounts amounted to dozens per day, with tens of Iraqi targets being killed or captured each day – generating a furious tempo during this period. As McChrystal described it:

The aim was to go after the middle of their network – in a regular army, their senior noncommissioned officers. We tried to cause the network to collapse.... We took it to an art form. *It really became a machine.* (cited in Filkins, 2009, emphasis added)

Emphasizing the speed of the collection, McChrystal and Flynn further refined the concept of 'F3EA' by leveraging the capabilities and assets of more conventional forces, including cornering the lion's share of UAVs that were introduced into Iraq after 2007 (Schmitt and Shanker, 2011: 85). The development of a more refined and networked operational style in Iraq was later described by Pentagon strategist Michael Vickers:

We had overwhelming force so that this is how insurgents fought us. Faced with that kind of threat, that is where these counter-network operations came in. It's the 'F3EA'. Find. Fix, Finish. Exploit. Analyze – and now! It's intelligence-driven operations and the use of technology, in particular persistent surveillance – an unblinking eye – that lets you conduct a sustained campaign. One mission leads to another. We didn't know how to do these kinds of operations before 9/11. A lot of intelligence investment we had made came together in 2007. (cited in Schmitt and Shanker, 2011: 85)

Although it remains unclear to what extent JSOC operations were consequential in reducing overall levels of violence in Iraq, the increasingly visible and synergistic integration of JSOC into broader military operations provided evidence for the broader application of JSOC's shadow warfare to new battlefields among many influential figures. Buried in an unclassified assessment of the Iraq war undertaken by retired General Barry McCaffrey was a rare reference to the clandestine JSOC network, in which McCaffrey (2007) reported that

the US Tier One special operations [JSOC] capability is simply magic.... The comprehensive intelligence system is phenomenal. We need to re-think how we view these forces. They are a national strategic system akin to a B1 bomber. We need to understand that the required investment level in the creation of these forces demands substantial dedicated UAV systems, intelligence, and communications resources. These special operations formations cannot by themselves win the nation's wars. However, with them we have a tool of enormous and decisive strategic significance which has crucial importance in the global war on terrorists.

Networked expansion: JSOC's surge to Afghanistan and beyond

The final moment in the bottom-up emergence of more networked forms of organization across the US military that we see in today's shadow wars can be traced to the expansion of JSOC's networked warfare to the Afghanistan campaign after 2008 and then the extension of a dense matrix of highly secretive and networked strike operations beyond the conventional battlefield in the years that followed. The emergence of networked special operations forces under the Bush administration left a powerful institutional legacy that shaped and constrained the options and choices of the Obama administration when it entered office in early 2009. By 2007, Assistant Secretary of Defense for Special Operations Michael Vickers stated that SOCOM's global counter-terrorism plan focused on a list of 20 'high priority' countries, a further 29 'priority' countries, as well as 'other' countries that were not named (Tyson, 2007). Nevertheless, the new administration came into office with a marked predisposition toward a less visible, less public war in the shadows, and one more specifically directed at non-state and irregular opponents, especially the Al-Qaeda network (Ryan, 2011).

The administration's embrace of JSOC's shadow warfare model was signaled by Secretary of Defense Robert Gates's appointment of then JSOC commander General Stanley McChrystal to the top commander in Afghanistan, citing the need for 'new thinking and new approaches from our military leaders' (cited in MacAskill, 2009). Similar to the strategic template of the 2007 'surge' in Iraq under Petraeus, McChrystal advertised and implemented aspects of a more population-centric counterinsurgency approach that included putting more troops within civilian populations in the name of protecting the population and building relations with local communities, including some efforts at development and especially road projects (Kilcullen, 2009: 39–114). But, also as in Iraq, McChrystal unleashed the shadow war model of night raids that focused on 'taking down the network' of Taliban insurgents (Oppel and Nordland, 2010). With the tripling of the elite special operations forces after 2009 and the increased militarization of the CIA in Afghanistan, these two organizations began to carry out an estimated average of five raids a day against a constantly updated list of targets, mostly in southern Afghanistan, which was the focus of the troop increase ordered by President Obama (Shanker and Rubin, 2010). Moreover, the targets of the night raids shifted from 'high-value targets' to anyone contributing to the Taliban war effort, which resulted in an exponential increase in the level of targeted raids. According to Porter (2011), between 2009 and 2010, special operations forces and CIA raids increased from 20 raids per month to nearly 250 a month. Following McChrystal's replacement by General David Petraeus in the summer of 2010, the number increased to nearly 600 raids a month.

In addition to the surge in targeted raids in Afghanistan, the Obama administration also built upon a once-covert programme to kill suspected Al-Qaeda leaders to engage in a full-scale – if undeclared – shadow war against the insurgent networks based in Pakistan's tribal areas bordering Afghanistan (Warrick, 2011: 11). In 2009, President Obama authorized the drone war to target anyone in Pakistan's tribal areas it considered a potential threat, without authorization from outside the CIA as long as targets were in approved geographical 'boxes' near the Afghan border (Dilanian, 2011). As a result, the CIA reportedly launched 53 drone and missile strikes in 2009, 114 in 2010, and 64 in 2011, with the death toll estimated at around 2,000 alleged militants (Dilanian, 2011).

The extension of the networked shadow warfare to Pakistan, although officially directed by the CIA, marks the crystallization of the networked intelligence and targeting model of warfare originally developed by JSOC into a modular form of war that could be delinked from the conventional military battlespace and extended across new cartographies. Citing threats to the United States that included Al-Qaeda in Afghanistan and Pakistan, along with its regional affiliates in Yemen,

Somalia, and northern Africa, senior officials described plans to rely more heavily on clandestine campaigns to destroy Al-Qaeda's network, saying that US strategy would no longer focus on 'deploying large armies abroad'; instead, military and intelligence operatives would deliver 'targeted, surgical pressure' on militant groups intent on attacking the United States (Schmitt and Mazzetti, 2011). The new strategy included military raids and drone strikes, but it also includes network-disrupting tactics to deter 'terror enablers' such as gun-runners, financiers, and brokers, as well as computer and cellphone hacking to instil doubts among potential terrorists and their supporters.

The outcome of this new posture was that the shadowy network of special operators and related agencies extended this form of warfare to southern Arabia and the Horn of Africa, among other regions outside of the conventional war zone, with a particular focus on Yemen and Somalia. Previously, US strikes against suspected militants in Yemen and Somalia were conducted by either the CIA or US military forces under rules of engagement that were more restrictive than those of JSOC in Iraq and Afghanistan. By 2010, however, the Obama administration had given the go-ahead for a new programme in both locations that was modeled on the rules of engagement employed by the joint CIA and JSOC operations in Pakistan. This programme authorized special operations forces hunt-or-kill raids and drone strikes from a new network of bases that include a secret drone base in the Arabian peninsula along with drone bases in the Seychelles and Ethiopia, as well as a massive build out of JSOC's longstanding base in Djibouti (Mazzetti and Worth, 2010).

What is unique about the acceleration of these shadow campaigns after 2011 was the growing convergence between the CIA and JSOC and their overlapping commands, who share intelligence and equipment as well as operational details, often drawing from one another in the very same raid. The clandestine US military campaign to combat Al-Qaeda's franchise in Yemen also expanded to fight the Islamist insurgency in Somalia (Mazzetti and Schmitt, 2011). The new campaign, also jointly run by the CIA and JSOC, included targeted strikes by special operations forces, drone attacks, and expanded surveillance operations in Mogadishu and deeper into the Horn of Africa. Following the joint CIA/JSOC strike that killed Anwar al-Awlaki in Yemen, the *New York Times* claimed that this marked a turning point:

Disillusioned by huge costs and uncertain outcomes in Iraq and Afghanistan, the Obama administration has decisively embraced the drone, along with small-scale lightning raids like the one that killed Osama bin Laden in May, as the future of the fight against terrorist networks. (Shane and Shanker, 2011)

From the 'long war' to permanent war

What was bureaucratically unthinkable and operationally impossible before the emergence of JSOC as an adaptive and highly networked force that experimented with more networked and chaoplectic forms of warfare is now increasingly routine. JSOC, the CIA, and a broad network of agencies and commands are increasingly networked together to share information, compile target lists, and then hunt, kill, and capture enemies worldwide through shadowy operations in which violence is largely disappeared from media coverage and political accountability. While employing UAVs and new technologies, the emergence of this American form of shadow warfare is largely the result of the growing embrace of more networked and horizontal forms of organization, which a number of scholars had argued was the key development necessary for the American exploitation of more networked forms of warfare (Arquilla and Ronfeldt, 1996, 1997, 2001; Bousquet, 2008, 2009; Duffield, 2002; Hardt and Negri, 2004).

At the center of this transformation has been the explosive growth of networked special forces operations largely under the command of JSOC, which has evolved from a marginal actor to a major ‘hub and enabler’ of more networked forms of organization and warfare within the US military. By 2010, the *Washington Post* could report that US special operations forces were deployed in 75 countries, up from 60 at the end of the Bush presidency, and the number is likely growing (DeYoung and Jaffe, 2010). An estimated 20,000 full-time special operators undertake daily operations somewhere on the planet from an estimated 60 bases across several continents (Turse, 2011). The special operations forces menu of operations goes beyond unilateral strikes and raids to now include the training of local counter-terrorism forces and the conducting of joint operations with them. With its own intelligence division, drones, and satellites, JSOC increasingly operates more like a military within the military, possessing domestic power and global reach. The broader command within which JSOC is housed, SOCOM (Special Operations Command), now has control over budgeting, training and equipment procurement – powers usually reserved for departments (such as the Army or the Navy) – which signals that it is now a powerful institutional presence across the military (Priest and Arkin, 2011: 253–255). A JSOC command center was even established in Washington, DC, in late 2011, whose ‘mission is to replicate McChrystal’s model for operations under consideration in other countries’, including drug-cartel-ravaged Mexico (Priest and Arkin, 2011: 254).

Nevertheless, the growing institutional clout of JSOC and special operations forces networks within the US military has not meant that the American military, or even its most clandestine networked forces, have become fully distributed and chaoplexic horizontal organizations. But, it has led the US military to build networks and to develop a style of warfare similar to what Arquilla and Ronfeldt (2001: 16) term ‘counternetwar’, with elements of what Bousquet (2008, 2009) terms ‘chaoplexic warfare’, in which hybrid blends of hierarchies and decentralized networks operate through common information and self-synchronization to target and strike networked opponents in a process that is still ongoing. As the former head of JSOC, retired General Stanley McChrystal (2011), commented about the future of this networked model,

From its birth in Iraq, both the actual network – and the hard-earned appreciation for that organizational model – increasingly expanded to Afghanistan, especially as our nation’s focus turned toward that theater... As we learned to build an effective network, we also learned that leading that network – a diverse collection of organizations, personalities, and cultures – is a daunting challenge in itself. That struggle remains a vital, untold chapter of the history of a global conflict that is still under way.

This networked matrix of targeted counter-network operations emerged separately from but then worked in synergy with the adoption of population-centric counterinsurgency doctrine in Iraq and Afghanistan owing to their overlapping focus on social networks and information-led operations. But, in the midst of a shrinking Pentagon budget and the public and professional aversion to conventional troop deployments in foreign countries, the expansion of lethal counter-network operations may become the preferred way of carrying out wars abroad. The US military is being reconfigured away from mobilizing and sending large armies to fight or invade countries, towards using more efficient and agile networked forces to disrupt and take down irregular and networked opponents anywhere in the world (Klare, 2010).

The evolution of a distinctively American style of counternetwar has largely escaped public comment and scrutiny owing to the phenomenon’s origins as a deeply clandestine counter-terrorism programme. Public criticism has largely focused on concerns about unlawful drone strikes, civilian casualties, and the unchecked automation of warfare through these new technologies (Hastings,

2012; *Economist*, 2011; Singer, 2012). Drones, however, are a synecdoche for a bigger issue: the expanding system of a high-tempo regime of targeted strikes, special operations forces raids, and detention practices that are largely unaccountable to the public and draped in secrecy rules. Some critics have drawn parallels between these shadowy operations and the infamous Phoenix Program in Vietnam in which unaccountable hit squads executed thousands of alleged Viet Cong operatives and sympathizers in the shadows of more conventional war (Hayden, 2009). Moreover, SOCOM is cultivating new relationships with special operations forces commandos in other countries as it creates a network of potential partners that may allow the USA to intervene in other countries in a covert way. As Jacob Levich (2012) notes in a perceptive commentary on the political aims of drone warfare, 'all this points towards a future of worldwide "virtual occupations" in which US power is projected primarily by drone-based COIN, supplemented with relatively small teams of Special Forces'.

The emergence of a shadowy form of war in which targeted operations can occur anytime and anywhere suggests that warfare and violence have not so much disappeared but are increasingly, as Hardt and Negri (2004: 12) explain, extending even further into the social fabric of life in different parts of the world, becoming a permanent social relation. The older model of war identifies enemies as foreign citizens and territories, and ends when soldiers surrender and territories are occupied. What we are now seeing, however, is the development of a form of warfare that more closely resembles a global and possibly permanent policing operation that is focused on managing risks and preempting potential challenges through continuous surveillance and strike operations across diverse geographies, which undermines norms of sovereignty and blurs the distinction between war and peace. As Hardt and Negri (2004: 13) argue:

If war is no longer an exceptional condition but the normal state of affairs, if, that is, we have now entered a perpetual state of war, then it becomes necessary that war not be a threat to the existing structure of power, not a destabilizing force, but rather, on the contrary, an active mechanism that constantly creates and reinforces the present global order.

The prosecution of this new form of warfare may thus become a normal and ongoing function of state governance – like collecting taxes, enacting laws, or even 'mowing the lawn' – that is sold to the public as ways of providing 'security'. Winning such a war does not mean ceasing hostilities but rather managing risk through continuous population management – which replaces ending violence or solving the social and political problems that produce the challenges to 'the present global order' in the first place.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

- Ackerman S (2011) How special ops copied al-Qaida to kill it. *Danger Room*, 9 September.
- Alberts D and Hayes R (2003) *Power to the Edge: Command ... Control ... in the Information Age*. Washington, DC: Department of Defense CCRP.
- Arquilla J and Ronfeldt D (1996) *The Advent of Netwar*. Santa Monica, CA: RAND.
- Arquilla J and Ronfeldt D (1997) Looking ahead: Preparing for Information Age conflict. In: Arquilla J and Ronfeldt D (eds) *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, 439–499.

- Arquilla J and Ronfeldt D (2001) *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica, CA: RAND.
- Bousquet A (2008) Chaoplectic warfare or the future of military organization. *International Affairs* 84(5): 915–929.
- Bousquet A (2009) *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. New York: Columbia University Press.
- Castells M (1996) *The Rise of the Network Society*. Oxford: Blackwell.
- Cebrowski A and Garstka J (1998) Network-centric warfare: Its origin and future. *Proceedings* 124(1). Available at: <http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future> (accessed 27 February 2013).
- Denes N (2010) From tanks to wheelchairs: Unmanned aerial vehicles, Zionist battlefield experiments, and the transference of the civilian. In Zureik E, Lyon D and Abu-Laban Y (eds) *Surveillance and Control in Israel/Palestine: Population, Territory and Power*. New York: Routledge, 171–195.
- DeYoung K and Jaffe G (2010) U.S. ‘secret war’ expands globally as Special Operations forces take larger role. *Washington Post*, 4 June.
- Dilanian K (2011) CIA has suspended drone attacks in Pakistan, U.S. officials say. *Los Angeles Times*, 23 December.
- Duffield M (2002) War as a network enterprise: The new security terrain and its implications. *Cultural Values* 6(1&2): 153–165.
- Economist* (2011) Flight of the drones: Why the future of air power belongs to unmanned systems, 8 October.
- Feickert A (2006) U.S. Special Operations Forces (SOF): Background and issues for Congress. *CRS Report RS21048*. Washington, DC: Congressional Research Service.
- Filkins D (2009) The general’s long war. *New York Times Magazine*, 18 October.
- Flynn M, Juergens R and Cantrell TL (2008) Employing ISR: SOF best practices. *Joint Forces Quarterly Online* 50(3): 55–61.
- Frontline* (2011) Kill/Capture. PBS, 9 May (written and produced by Stephen Grey and Dan Edge).
- Global Security (n.d.) Task Force 145. Available at: <http://www.globalsecurity.org/military/agency/dod/tf-145.htm> (accessed 30 March 2012).
- Hardt M and Negri A (2004) *Multitude: War and Democracy in the Age of Empire*. New York: Penguin.
- Hastings M (2012) The rise of the killer drones: How America goes to war in secret. *Rolling Stone*, 12 May.
- Hayden T (2009) Kilcullen’s long war. *The Nation*, 2 November.
- Hersh S (2008) Preparing the battlefield. *The New Yorker*, 7 July.
- Kilcullen D (2009) *The Accidental Guerilla: Fighting Small Wars in the Midst of a Big One*. New York: Oxford University Press.
- Klare M (2010) Two, three, many Afghanistans. *The Nation*, 26 April.
- Lee C (2011) Drones transform how America fights its wars. *New York Times*, 20 June.
- Levich J (2012) Collectivized torture: Drone warfare and the dark side of counterinsurgency. *Monthly Review*, 18 October. Available at: <http://mrzine.monthlyreview.org/2012/levich181012.html> (accessed 1 November 2012).
- MacAskill E (2009) Top general sacked as US bids to turn around Afghan war. *Guardian* (London), 11 May.
- McCaffrey B (2007) After action report: General Barry R McCaffrey USA (Ret) VISIT IRAQ AND KUWAIT 9–16 March. Available at: http://media.washingtonpost.com/wp-srv/nation/documents/McCaffrey_Report_032707.pdf (accessed 5 October 2012).
- McChrystal SA (2011) It takes a network: The new front line of modern warfare. *Foreign Policy* March/April: 1–6.
- MacGinty R (2010) Social network analysis and counterinsurgency: A counterproductive strategy? *Critical Studies on Terrorism* 3(2): 209–226.

- Mazzetti M and Schmitt E (2011) U.S. expands its drone war into Somalia. *New York Times*, 1 July.
- Mazzetti M and Worth R (2010) A secret assault on terror widens on two continents. *New York Times*, 15 August.
- Miller G (2011) Under Obama, an emerging apparatus for drone killing. *Washington Post*, 27 December.
- Naylor S (2011) Bin Laden raid a triumph for Spec Ops. *Air Force Times*, 9 May.
- Oppel R Jr and Nordland R (2010) U.S. is reining in special operations forces in Afghanistan. *New York Times*, 15 March.
- Ostlund W (2012) Irregular warfare: Counterterrorism forces in support of counterinsurgency operations. Land Warfare Papers No. 91. Arlington, VA: Institute of Land Warfare.
- Porter G (2011) How McChrystal and Petraeus built an indiscriminate killing machine. *Truthout*, 26 September.
- Priest D and Arkin W (2011) *Top Secret America: The Rise of the New American Security State*. New York: Little, Brown & Co.
- Rohde D (2012) The drone wars. *Reuters Magazine*, 26 January.
- Rosen N (2008) The myth of the surge. *Rolling Stone*, 6 March.
- Rumsfeld D (2002) Transforming the military. *Foreign Affairs* 81(3): 20–32.
- Ryan M (2011) 'War in countries we are not at war with': The 'war on terror' on the periphery from Bush to Obama. *International Politics* 48(2/3): 364–389.
- Sanger D (2012) *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown.
- Schmidle N (2011) Getting Bin Laden. *New Yorker*, 8 August.
- Schmitt E and Marshall S (2006) In secret unit's 'Black Room' a grim portrait of U.S. abuse. *New York Times*, 19 March.
- Schmitt E and Mazzetti M (2011) Obama adviser outlines plans to defeat Al Qaeda. *New York Times*, 29 June.
- Schmitt E and Shanker T (2011) *Counterstrike: The Untold Story of America's Secret Campaign Against Al-Qaeda*. New York: Times Books.
- Shane S and Shanker T (2011) Yemen strike reflects U.S. shift to drones as cheaper war tool. *New York Times*, 2 October.
- Shanker T and Rubin A (2010) Quest to neutralize Afghan militants is showing glimpses of success, NATO says. *New York Times*, 28 June.
- Singer P (2009) *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*. New York: Penguin.
- Singer P (2012) Drone strikes on democracy. *International Herald Tribune*, 21 January.
- Turse N (2011) Mapping America's shadowy drone wars. *TomDispatch.com*, 16 October.
- Turse N (2012) *The Changing Face of Empire: Special Ops, Drones, Spires, Proxy Fighters, Secret Bases and Cyberwar*. New York: Haymarket Books.
- Tyson AS (2007) Sorry Charlie. This is Michael Vicker's war. *Washington Post*, 28 December.
- Ucko D (2009) *The New Counterinsurgency Era: Transforming the U.S. Military for Modern Wars*. Washington, DC: Georgetown University Press.
- Urban M (2010) *Task Force Black: The True Story of the Secret Special Forces War in Iraq*. New York: St Martin's Griffin.
- US Department of the Army (2007) *US Army/Field Corps Counterinsurgency Manual No. 3–24*. Chicago, IL: Chicago University Press.
- US Department of Defense (2006) *Quadrennial Defense Review Report*. Washington, DC: Department of Defense.
- Warrick J (2011) *The Triple Agent: The Al-Qaeda Mole Who Infiltrated the CIA*. New York: Doubleday.
- Warrick J and Wright R (2008) U.S. teams weaken insurgency in Iraq. *Washington Post*, 6 September.

Woodward B (2008a) *The War Within: Secret White House History 2006–2008*. New York: Simon and Schuster.

Woodward R (2008b) Why did violence plummet? It wasn't just the surge. *Washington Post*, 8 September.

Steve Niva teaches International Politics and Middle East studies at the Evergreen State College in Olympia, WA. His primary areas of research and writing include the Israeli–Palestinian conflict; US foreign policy in the Middle East; and evolving forms of contemporary warfare in the Middle East. He has written for and served on the editorial board of *Middle East Report* magazine (www.merip.org). This article is based on a paper presented to the interdisciplinary workshop on 'Wars Beyond War: Mass Violence in an Age of Terror, Catastrophe and the Responsibility To Protect', organized by the Peace and Conflict Studies Program at Colgate University, 30–31 March 2012.