GJ TheGeographicalJournal

Royal Geographical Society with IBG
Advancing geography and geographical learning

The Geographical Journal, Vol. **177**, No. 3, September 2011, pp. 238–250, doi: 10.1111/j.1475-4959.2011.00426.x

The everywhere war

DEREK GREGORY

Department of Geography, University of British Columbia, 217-1984 West Mall, Vancouver, British Columbia, Canada V6T 1Z2

E-mail: derek.gregory@geog.ubc.ca

This paper was accepted for publication in May 2011

Much of the discussion of 9/11 has debated its historical significance, but it is equally important to explore the geographical dimensions of the wars that have been conducted in its shadows. Subsequent transformations in the American way of war have played a major role in the increased militarisation of the planet. Most attention has been focused on Afghanistan and Iraq as the principal theatres of the 'war on terror', but one of the characteristics of late modern war is the emergent, 'event-ful' quality of military, paramilitary and terrorist violence that can, in principle, occur anywhere. Vulnerabilities are differentially distributed but widely dispersed, and in consequence late modern war is being changed by the slippery spaces through which it is conducted. This paper explores three global borderlands to bring those changes into focus: Afghanistan–Pakistan (particularly the deployment of CIA-controlled drones in Pakistan), US–Mexico (particularly the expansion of Mexico's 'drug war' and the US militarisation of the border), and cyberspace (particularly the role of stealth attacks on critical infrastructure and the formation of US Cyber Command).

KEY WORDS: Pakistan, Mexico, United States, war, borderlands, cyberspace

War time

For many, particularly in the United States, 9/11 was a moment when the world turned; for others, particularly outside the United States, it was a climactic summation of a longer history of American imperialism in general and its meddling in the Middle East in particular. Either way, it is not surprising that many commentators should have emphasised the *temporality* of the military violence that followed in the wake of the terrorist attacks on the World Trade Center and the Pentagon on that bright September morning: the 'war on terror' that became 'the long war'. For the RETORT collective, the invasions of Afghanistan and Iraq marked 'the elevation – into a state of permanent war – of a long and consistent pattern of military expansionism in the service of empire' (RETORT 2005, 80). Keen (2006) wrote of 'endless war', Duffield (2007) of 'unending war' and Filkins (2008) of 'the forever war'. The sense of permanence endures, and yet Engelhardt (2010, 2–3) ruefully notes that it remains difficult for Americans to understand 'that Washington is a war capital, that the United States is a war state, that it garrisons much of the planet, and that the norm for us is to be at war somewhere at any moment'. Bacevich (2010, 225) traces this state of affairs to what he calls the 'Washington rules' that long pre-date 9/11. These are 'the conviction that the obligations of leadership require the United States to maintain a global military presence, configure its armed forces for power projection, and employ them to impose changes abroad', which he argues have formed 'the enduring leitmotif of US national security policy' for the last 60 years and 'propelled the United States into a condition approximating perpetual war'.

Each of these temporal formulations implies spatial formations. For RETORT (2005, 103) 'military neoliberalism' is 'the true globalization of our time'. The planetary garrison that projects US military power is divided into six geographically defined unified combatant commands – like US Central Command, CENTCOM – whose Areas of Responsibility cover every region on earth and which operate through a global network of bases. If you think this unremarkable, ask yourself Bacevich's question: how would the United States react if China were to mirror these moves? Think, too, of the zones in which the shadow of US military violence still falls: not just Afghanistan and Iraq, but also Iran, Libya, Pakistan, Somalia, Yemen. Then think of the zones where the rhetoric of the 'war on terror' has been used by other states to legitimise repression: Chechnya, Libya, Palestine, the Philippines, Sri Lanka. And then think of the cities that have become displacements of the space of war, punctuation points in what Sassen (2010, 37) calls 'a new kind of multi-sited war': Casablanca, Lahore, London, Madrid, Moscow, Mumbai. All these lists are incomplete, but even in this truncated form they suggest the need to analyse not only 'the

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

forever war' but also what we might call 'the everywhere war'.

This is at once a conceptual and a material project whose scope can be indexed by three geo-graphs that trace a movement from the abstract to the concrete: Foucault's (1975–6) prescient suggestion that war has become the pervasive *matrix* within which social life is constituted; the replacement of the concept of the battlefield in US military doctrine by the multi-scalar, multi-dimensional *'battlespace'* with 'no front or back' and where 'everything becomes a site of permanent war' (Graham 2009, 389; 2010, 31); and the assault on the global *borderlands* where the United States and its allies now conduct their military operations. The first two are never far from the surface of this essay, but it is the third that is my primary focus.

Borderlands and blurred boundaries

Duffield (2001, 309) once described the borderlands as 'an imagined geographical space where, in the eyes of metropolitan actors and agencies, the characteristics of brutality, excess and breakdown predominate'. There, in the 'wild zones' of the global South, wars are supposed to occur 'through greed and sectarian gain, social fabric is destroyed and developmental gains reversed, non-combatants killed, humanitarian assistance abused and all civility abandoned'. This imaginative geography folds in and out of the rhetorical distinction between 'our' wars – wars conducted by advanced militaries that are supposed to be surgical, sensitive and scrupulous – and 'their' wars. In reality, however, the boundaries are blurred and each bleeds into its other (Gregory 2010). Thus the US-led invasion of Afghanistan in October 2001 combined a long-distance, high-altitude war from the air with a ground war spearheaded by the warlords and militias of the Northern Alliance operating with US infantry and Special Forces; counterinsurgency in Afghanistan and Iraq has involved the co-option of ragtag militias to supplement US military operations; and in Afghanistan the US Army pays off warlords and ultimately perhaps even the Taliban to ensure that its overland supply chain is protected from attack (Report of the Majority Staff 2010).

In mapping these borderlands – which are also shadowlands, spaces that enter European and American imaginaries in phantasmatic form, barely known but vividly imagined – we jibe against the limits of cartographic and so of geopolitical reason. From Ratzel's view of *der Krieg als Schule des Raumes* to Lacoste's stinging denunciation – *'la géographie, ça sert, d'abord, à faire la guerre'* – the deadly liaison between modern war and modern geography has been conducted in resolutely territorial terms. To be sure, the genealogy of territory has multiple valences, and Ratzel's *Raum* is not Lacoste's *espace*, but a critical analysis of the everywhere war requires cartographic reason to be supplemented by other, more labile spatialities. This is not only a matter of transcending the geopolitical, connecting it to the biopolitical and the geo-economic, but also of tracking space as a 'doing', precarious, partially open and never complete. It is in something of this spirit that Bauman (2002, 83) identifies the 'planetary frontierlands' as staging grounds of today's wars, where efforts to 'pin the divisions and mutual enmities to the ground seldom bring results'. In the course of 'interminable frontierland warfare', so he argues, 'trenches are seldom dug', adversaries are 'constantly on the move' and have become for all intents and purposes 'extraterritorial'. I am not sure about the last (Bauman is evidently thinking of al Qaeda, which is scarcely the summation of late modern war), but this is an arresting if impressionistic canvas and the fluidity conveyed by Bauman's broad brush-strokes needs to be fleshed out. After the US-led invasion of Iraq it was commonplace to distinguish the Green Zone and its satellites (the US political-military bastion in Baghdad and its penumbra of Forward Operating Bases) from the 'red zone' that was everywhere else. But this categorical division is misleading. The colours seeped into and swirled around one another, so that occupied Iraq became not so much a patchwork of green zones and red zones as a thoroughly militarised landscape saturated in varying intensities of brown (khaki): 'intensities' because within this warscape military and paramilitary violence could descend at any moment without warning, and within it precarious local orders were constantly forming and re-forming. I think this is what Anderson (2011) means when he describes insurgencies oscillating 'between extended periods of absence as a function of their dispersion' and 'moments of disruptive, punctual presence', but these variable intensities entrain all sides in today's 'wars amongst the people' – and most of all those caught in the middle.

This is to emphasise the emergent, 'event-ful' quality of contemporary violence, what Gros (2010, 260) sees as 'moments of pure laceration' that puncture the everyday, as a diffuse and dispersed 'state of violence' replaces the usual configurations of war. Violence can erupt on a commuter train in Madrid, a house in Gaza City, a poppy field in Helmand or a street in Ciudad Juarez: such is the contrapuntal geography of the everywhere war. It is also to claim that, as cartographic reason falters and military violence is loosed from its frames, the conventional ties between war and geography have come undone: that, as Münkler (2005, 3) has it, 'war has lost its well-defined contours'. In what follows, I propose to take Münkler at his word and consider three borderlands beyond Afghanistan and Iraq that illuminate some of the ways in which, since 9/11, late modern war is being transformed by the slippery spaces within which and through which it is conducted. I focus in turn on 'Af-Pak', 'Amexica' and cyberspace, partly because these concrete instances remind us that the every-

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

where war is also always *somewhere* (Sparke 2007, 117), and partly because they bring into view features of a distinctly if not uniquely *American* way of war.

'Af-Pak'

'Af-Pak' is the cover term coined by the Obama administration, and probably by its Special Representative for Afghanistan and Pakistan Richard Holbrooke, to describe the regional battlespace in which the United States pursues its armed conflict with the Taliban and al Qaeda. The term is widely disliked in Afghanistan and Pakistan, but its hyphen marks a profoundly ambiguous zone. The border was surveyed between 1894 and 1896 to delimit British colonial territories in India along the north-west frontier with Afghanistan. This so-called Durand Line bisected the cultural region of Pashtunistan, dividing villages and extended families with strong culture and kinship connections between them, and ever since the formation of Pakistan in 1947, Afghanistan has insisted that the demarcation lapsed with the end of colonial rule. The established body of international law rejects the Afghan position, but Mahmud (2010) argues that the continued entanglements of law and colonial power show that in this post-colonial space law is still part of the problem rather than the solution because the border freeze-frames colonial demarcations. Not surprisingly, the borderlands are highly porous and many of their inhabitants routinely cross from Afghanistan into Pakistan and back without bothering about any border formalities. This includes the Taliban, whose movements are both episodic, fleeing hot pursuit from Afghanistan, and seasonal, returning from Pakistan when fighting resumes in the spring. This recent history has compounded the porosity of the region so that 'Af-Pak' also conjures up a shadowy, still more dispersed 'risky geography' that wires Afghanistan and Pakistan to 'Londonistan' and other European cities, and to terrorist cells and militant groups that threaten Europe and the continental United States (Amoore and de Goede 2011).

Although the Taliban is predominantly Pashtun, it is not a monolith that straddles the border. The Taliban emerged in the early 1990s as an armed and predominantly Pashtun response to the brutalising rule of the militias of the Northern Alliance who governed Afghanistan in the turbulent aftermath of the Soviet occupation in 1989. The Taliban sought to impose its own stringent version of Islamic law, and its advance drew thousands of veterans from the guerilla war against the Red Army and from Afghan refugee camps in Pakistan. The civil war that ensued was a bloody and protracted affair; hundreds of al-Qaeda fighters fought alongside Taliban troops, although the relations between the two were far from straightforward, and by the end of the decade Afghanistan had been virtually consumed by the violence. The insular, ultra-nationalist project of the Taliban was supported by Pakistan throughout the 1990s, and the neo-Taliban that regrouped after the US-led invasion of Afghanistan has continued to seek an accommodation with Islamabad (Gregory 2004, 41–2). Its leadership council was driven from Kandahar and is now based in Quetta; its four regional military councils are based in Pakistan too, and it enjoys the support of Pakistan's Directorate for Inter-Services Intelligence. These affiliations sharply distinguish the Afghan Taliban from the Pakistan Taliban, or Tehrik-i-Taliban (TTP), which was formed in December 2007 as a loose coalition of militant Islamicist groups under Baitullah Mehsud. The Pakistan Taliban endorses the struggle against the US-led International Security Assistance Force (ISAF) in Afghanistan, but its primary target is the Pakistani state: it seeks to establish its own rule over the Federally Administered Tribal Areas (FATA) on the border. The Pakistan military has conducted a series of offensive operations against the TTP in those areas, punctuated by wavering truces, but the FATA continue to have a tense and attenuated relationship to Islamabad, and in Urdu they are known as *ilaqa ghair*, 'alien', 'foreign', or even 'forbidden' lands.

These ambivalences have a direct impact on strikes by Unmanned Aerial Vehicles (UAVs) in the FATA. The attacks are carried out by armed MQ-1 Predators and MQ-9 Reapers launched from bases in Afghanistan (and until early this year in Pakistan too) but remotely controlled by the CIA from the continental United States. The Predator was jointly developed for the US Air Force and the CIA, and at the CIA's request it was armed with Hellfire missiles in early 2001. After 9/11 President George W. Bush signed an authorisation that gave the CIA wide latitude in the 'war on terror' through the issue of 'kill, capture or detain' orders against members of al Qaeda. Its immediate consequence was the initiation in October of the same year of the program of extraordinary rendition conducted in the shadows of the global war prison: the seizure, incarceration and torture of terrorist suspects at 'black sites'. This was subsequently supplemented by a program directed at killing named individuals – 'High Value Targets' – who were on a list compiled by the CIA's Counterterrorism Center. The first UAV strike in Pakistan took place on 18 June 2004. The initial pace was slow, in part because the number of UAVs was limited but also because the target list was restricted and ground intelligence meagre. There were eight more strikes before the assassination of Benazir Bhutto on 27 December 2007 prompted Bush to expand the target list from al Qaeda to a wider array of individuals, and thus to increase the rate of strike; by the end of 2008 there had been 46 strikes in Pakistan. As extraordinary renditions were terminated and black sites closed, President Barack Obama widened the scope of the target list still further and dramatically stepped up the tempo; faster and more powerful Reapers were pressed into service, borrowed from Air Force operations in Afghanistan, and by the

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

end of 2010 there had been a further 180 strikes. Baitullah Mehsud was assassinated by a Predator strike in August 2009 – after 16 unsuccessful strikes over 14 months that killed several hundred others (Mayer 2009) – but this seems to have been a rare success. The vast majority killed in the last 2 years have reportedly been ordinary foot soldiers – people 'whose names were unknown or about whom the Agency had only fragmentary information' (Cloud 2010), although it had no hesitation in declaring virtually none of them civilians – and this has led to doubts about the purpose and parameters of the campaign (Miller 2011).

These operations raise troubling questions. Some arise from the resort to extra-judicial killing that the United States once condemned: if it is wrong to torture suspects, how can it be right to assassinate them? How secure is the evidential basis on which targeting decisions are made? Others arise from the use of UAVs and the time–space compressions produced by the techno-cultural armature of this new mode of war, although I think that most of the criticism about video feeds reducing war to a video game is misplaced – these are profoundly immersive technologies that have quite other (and more serious) consequences for killing – but in any case these concerns apply with equal force to the strikes carried out by the Air Force's Predators and Reapers in Afghanistan that use the Pentagon's Joint Integrated Prioritised Target List to 'put warheads on foreheads' (Gregory 2011). Still others arise from the legal apparatus that constitutes the extended war zone, and it is these that concern me here. Plainly the United States is not at war with Pakistan, and even though Islamabad gives the nod to the strikes – while closing its eyes to their effects – Murphy (2009, 10) claims that the authority of Islamabad to sanction US military actions in the FATA is far from clear. For its part, the Obama administration represents the strikes as legitimate acts of self-defence against the Afghan Taliban who are engaged in a transnational armed conflict and seek sanctuary across the border and as effective counter-terrorism tactics against al Qaeda and its affiliates hiding in Pakistan. But these are inadequate responses for at least three reasons that all revolve around the battlespace as a grey zone.

First, even though the Air Force may be involved to some degree, it is the CIA that plans and executes the strikes. The CIA was created in 1947 as a civilian agency to counterbalance the influence of the military. Since then there has been a general 'civilianisation' of war in all sorts of ways, which includes the outsourcing of support services to contractors, and the CIA has been transformed from a civilian agency into 'a paramilitary organisation at the vanguard of America's far-flung wars' operating from an 'archipelago of fire-bases' in Afghanistan and beyond (Mazzetti 2010; Shane *et al*. 2010). But the CIA does not operate under military control so that, as Singer (2010) observes, the clandestine air war in Pakistan is commanded not by an Air Force general but by 'a former congressman from California', Leon Panetta, the Director of the CIA. According to Horton (2010), this is 'the first time in U.S. history that a state-of-the-art, cutting-edge weapons system has been placed in the hands of the CIA'. Hence Singer's (2010) complaint that civilians are operating advanced weapons systems outside the military chain of command and 'wrestling with complex issues of war' for which they have neither the necessary training – this is a moot point: it may be that CIA operators follow similar procedures protocols to their Air Force counterparts, including the incorporation of legal advisers into the kill-chain to endorse the 'prosecution of the target' (Etzioni 2010; Mckelvey 2011) – nor, according to the National Security Act, the legal authority. This is the most damaging objection because it turns CIA operators into the category that Bush so confidently consigned to the global war prison after 9/11: unlawful combatants (O'Connell 2009). This is such an obvious point that Paust (2010, 45), who otherwise endorses the strikes as acts of self-defence, concludes that the CIA's lawyers must be leftovers from the Bush administration 'who have proven either to be remarkably ignorant of the laws of war or conveniently quiet and complicit during the Bush–Cheney program of serial and cascading criminality'. These considerations radically transform the battlespace as the line between the CIA and the military is deliberately blurred. Obama's recent decision to appoint Panetta as Secretary of Defense and have General David Petraeus take his place as Director of the CIA makes at least that much clear. So too do the braiding lines of responsibility between the CIA and Special Forces in the killing of Osama bin Laden in Abbottabad in May 2011, which for that reason (and others) was undertaken in what Axe (2011) portrays as a 'legal grey zone' between two US codes, Title 10 (which includes the Uniformed Code of Military Justice) and Title 50 (which authorises the CIA and its covert operations) (Stone 2003). The role of the CIA in this not-so-secret war in Pakistan thus marks the formation of what Engelhardt and Turse (2010) call 'a new-style [battlespace] that the American public knows remarkably little about, and that bears little relationship to the Afghan War as we imagine it or as our leaders generally discuss it'.

Second, representing each drone strike as a separate act of self-defence obscures the systematic and cumulative nature of the campaign. Although the Obama administration insists that its targeting procedures adhere to the laws of armed conflict, the covert nature of a war conducted by a clandestine agency ensures that most of its victims are wrapped in blankets of secrecy. Accountability is limited enough in the case of a declared war; in an undeclared war it all but disappears. There is little or no recognition of civilian casualties, no inquiries into incidents that violate the principles of discrimination and proportionality, and

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

no mechanism for providing compensation. The Campaign for Innocent Victims in Conflict reports from the FATA that:

> Drone victims receive no assistance from the Pakistani or US governments, despite the existence of Pakistani compensation efforts for other conflict-victims and US compensation mechanisms currently operating in Iraq and Afghanistan. Victims are left to cope with losses on their own while neither the Pakistani nor the US governments acknowledge responsibility for the strikes or the civilian status of those collaterally harmed.
>
> Rogers (2010, 64)

The single exception to date has been the decision by Islamabad to compensate victims of a US drone strike in North Waziristan in March 2011. The details, such as they are, are revealing. Local people had gathered at a market with Taliban mediators to settle a dispute over a chromite mine; two UAVs launched four missiles that killed at least 40 people. Pakistan's Prime Minister and the Chief of Army Staff both sharply condemned the strike as a reckless attack on civilians, including elders and children, but US officials insisted that the meeting was a legitimate terrorist target not 'a bake sale', 'county fair', 'charity car wash' or 'the local men's glee club' (sic) (Masood and Shah 2011; Rodriguez 2011). As even this case shows, the advanced technology that makes the UAV campaign possible – the combination of sensor and shooter in a single platform – does not dispel the fog of war. Far from making the battlespace transparent, this new apparatus actively exploits another grey zone, the space between civilian and combatant that is peopled by the spectral figures that haunt the landscape of insurgency.

Third, the legal logic through which the battlespace is extended beyond the declared zone of combat in Afghanistan is itself infinitely extendible. If the United States is fighting a global war, if it arrogates to itself the right to kill or detain its enemies wherever it finds them, where does it end? (Blank 2010–11). Human Rights Watch posed the key questions in a letter to Obama on 7 December 2010:

> While the United States is a party to armed conflicts in Afghanistan and Iraq and could become a party to armed conflicts elsewhere, the notion that the entire world is automatically by extension a battleground in which the laws of war are applicable is contrary to international law. How does the administration define the 'global battlefield' and what is the legal basis for that definition? What, if any, limits exist on ordering targeted killings within it? Does it view the battlefield as global in a literal sense, allowing lethal force to be used, in accordance with the laws of war, against a suspected terrorist in an apartment in Paris, a shopping mall in London, or a bus station in Iowa City? Do the rules governing targeted killing vary from one place to another – for example, are different criteria used in Yemen and Pakistan?'
>
> Human Rights Watch (2010)

These bloody geographies exploit another grey zone. Legal opinions are sharply divided about the regulation of armed conflict between state and non-state actors that takes place beyond state borders ('transnational armed conflicts'). It is those states that have most strenuously pressed for the regulation of intrastate wars and the establishment of international criminal tribunals for conflicts in Ruanda and the former Yugoslavia that have most vigorously insisted on being allowed the maximum freedom to conduct their own trans-border campaigns against non-state actors (Benvenisti 2010). Law and war have always been intertwined, and international law is often re-made through war – in fact operating at the margins of the law is one of the most powerful ways of changing it – and the UAV strikes in Pakistan are evidently no exception. They seek at once to expand the battlespace and to contract the legal armature that regulates its constitution.

'Amexica'

The United States–Mexico borderlands are an ambiguous space too, 'Amexica', famously described by Anzaldúa (1987, 25) as '*una herida abierta* [an open wound] where the Third World grates against the First and bleeds.' Before a scab can form, she continued, 'it hemorrhages again, the lifeblood of two worlds merging to form a third country – a border culture'. Coleman (2005) sees the border as a trickster figure, at once being opened to the passage of capital and commodities under the sign of neoliberalism and closed to the movement of migrants who are often themselves victims of neoliberalism, and he is right to treat 'de-bordering' and 're-bordering' as a tense and countervailing constellation of transnational, national and local practices. But Anzaldúa's original sanguinary metaphor seems ever more appropriate as the border has come to be performed as the front-line in what Vulliamy (2010, 12) calls 'the first real twenty-first century war' because, he says, it is also a 'post-political war'. What he has in mind is the trans-border 'war on drugs', but his characterisations fail to capture the twentieth-century histories that are embedded in the conflict, the intimate connections between narco-trafficking and the Mexican state, and the ways in which this increasingly militarised campaign forms one plane in a multi-dimensional battlespace where drug traffickers and undocumented migrants are being transformed into insurgents and terrorists. All of these violent geographies are freighted with political implications.

In the 1980s the major drug trafficking routes into the United States from Central and South America ran through the Caribbean, and there have been persistent

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

claims that CIA support for the Contra rebels in Nicaragua involved at least tacit support for an ongoing arms-for-drugs exchange. The increasing public scrutiny of these arrangements combined with the success of counter-narcotics operations to prompt Colombian drug cartels to develop new trafficking routes through Mexico's border cities. These routes were controlled by one major Mexican trafficker, Félix Gallardo, but when he was imprisoned in 1989 he had his lieutenants divide the border into territories and reach an accommodation with Mexican authorities so that they could concentrate on fighting what he saw as 'the real enemy': the agents of the United States. These arrangements soon broke down. Fighting between the new regional cartels spiralled into a battle for profits through territorial expansion, and as the violence intensified the state militarised its response. Federal troops had long been used to destroy marijuana and poppy fields in rural areas, especially in the mountainous Golden Triangle that spans Chihuahua, Sinaloa and Durango, but despite their raids domestic production soared. The army was ill-prepared for the switch to interdiction in cities, where its record proved even more mixed and the consequences far bloodier: more than 35,000 people have been killed in the last 4 years, more than the toll in Afghanistan over the same period. Fifty thousand federal troops and thousands more private security contractors, many of them employed by US security companies, are now deployed.

The conventional and I dare say dominant reading treats all these deaths as confined to those caught up in the drug trade. Leaving on one side those who are literally caught, trapped in the trade by spiralling circles of poverty set spinning by the rapid neoliberalisation of the economy, some Mexican scholars insist that the victims include human rights activists, community leaders and labour organisers. Certainly, Mexico is no stranger to military repression. During the 'dirty war' from the 1960s through to the 1980s, the Army was given *carte blanche* to put down student demonstrations and guerilla groups, and it carried out 'disappearances' and illegal detentions, torture and killings on such a scale that the United States noted 'an emerging security problem'. The cloak for these bloody operations was the Cold War, and some scholars believe that the 'drug war' now serves as a convenient cover for the renewed criminalisation of social protest. When President Calderon describes the campaign as 'a war', therefore, the word is freighted with layers of political meaning. He and his ministers constantly speak in these terms, and Calderon has even compared the fight against the cartels to Mexico's celebrated defeat of an invading French expeditionary force on 5 May 1862; but for many Mexicans the reverberations are more recent than Cinco de Mayo. Yet the declaration has to be seen as something more than the intensified militarisation of security. 'It is no longer a matter of organised crime', *El Universal* declared in a June 2010 editorial, 'but rather of the loss of the state'. Calderon said much the same on 4 August 2010: 'it [has] become a challenge to the state, an attempt to replace the state', he claimed, because the cartels 'are trying to impose a monopoly by force of arms, and are even trying to impose their own laws'.

The United States had been fighting its own narco-war even before President Nixon declared a 'war on drugs' in 1971, and its shots were fired in September 1969 when the US–Mexico border was closed for several weeks and all vehicles entering the US were stopped and searched for marijuana. But it is the new political conjuncture in Mexico that has transformed America's militarisation of its southern border. The process has a long history; the Mexican–American war of 1846–8 still casts long shadows, and the origins of the US Border Patrol lie in the mounted guards of the Immigration Service at the dawn of the last century whose patrols were intermittently reinforced by federal troops. Three moments index the emergence of a military–security nexus along the border. From 1978 the US Army's doctrine for 'low-intensity conflict' was repatriated to the United States; in 1982 federal law restricting the role of the military in domestic policing was relaxed; and in 1989 President George H.W. Bush committed the Pentagon to the 'war on drugs' with the formation of Joint Task Force 6 (JTF-6) to support law enforcement along the border and, eventually, within the continental United States (Dunn 1996; Rosas 2006). The initial collaboration between the Border Patrol and the military targeted not only drug traffickers but also undocumented migrants from Mexico. A cascading series of joint operations, from Operation Blockade in El Paso in 1993 through Gatekeeper in San Diego and Safeguard in Arizona to Rio Grande in Texas in 1997, was designed to capture undocumented migrants (who were held to be responsible for increased criminal activity in border cities) and to deflect countless others into remote desert areas where they were knowingly exposed to death; in what Doty (2011) indicts as 'an endless deferral of human responsibility', their deaths were (mis)attributed to 'natural causes' (Nevins 2002; Sundberg 2011). The risk of dying on the crossing has steadily increased (Jimenez 2009).

9/11 prompted and permitted the formation of a still more intensive military–security nexus that rendered undocumented migrants even more vulnerable to an emergent necropolitics by imaginatively placing them in a warzone where they become, in effect, unlawful combatants (Mbembe 2003; Castro 2007, 12). Many of the military units involved in border support now saw the mission as a pre-deployment exercise for combat in Afghanistan and Iraq, and this imaginative re-mapping was reinforced by a cascading series of institutional, technical and cultural developments. In 2004 JTF-6 was incorporated into US Northern Command as JTF-North and counter-terrorism and

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

homeland security were added to its mission. It continued to operate in close concert with the Border Patrol, which was now part of the Department of Homeland Security, and it too defined its priority mission as deterring and preventing 'transnational threats to the homeland'. Then, in May 2006, even as Bush peddled the fiction that 'the United States is not going to militarize the southern border', he announced the deployment of 6000 National Guard troops to the border and what he hailed as 'the most technologically advanced border security initiative in American history'. These measures hastened the rhetorical collapse of the alien into the terrorist and, as Rosas (2007, 97) observed, allowed 'the violent subjugation of immigrants to the special relation of illegality'.

The violence of this reduction is legitimated by a series of cultural productions that use the language of war. Here are three examples from the last year alone. National Geographic's *Border wars* series promised to take viewers to the 'front line'; as in Iraq, camera crews were 'embedded' with the Border Patrol, and filmed its operations from Blackhawk helicopters and Forward Operating Bases. Afterwards its producer said that he had some sense 'of what it must be like to come back from Iraq or Afghanistan' (Cavanaugh and Heilbrunn 2010). Fox News' *War stories on the border: the third front* took its viewers to the 'front line of the war on narco-terror'; hosted by Oliver North, a central figure in the other Contra supply scandal of the 1980s, which involved covertly selling arms to Iran to fund the rebels; the series was advertised as exposing 'the war *for* the border' (my emphasis). Finally, in Gareth Edwards' science-fiction film *Monsters*, set 6 years after a NASA space probe crashes in northern Mexico and sets loose alien life-forms, the region becomes 'the infected zone', and an American photojournalist has to escort his employer's daughter home through a landscape scattered with burned-out tanks and wrecked warplanes ('Mexican and US military struggle to contain the creatures') to the safety of the massively militarised border. It's not difficult (or paranoid) to view productions like these as moments in the staging of the borderlands as a liminal zone of danger that *requires* a militarised response. Popular culture has also assumed a more directly interventionist form through the mobilisation of right-wing citizen militias like the Minutemen, whose training manual provides volunteers with a 'virtual lexicon of war' in which military and paramilitary logics and languages are paramount and border watch is explicitly framed as combat (Castro 2007, 19–20; Doty 2007, 125).

The hi-tech Secure Border Initiative was a failure, and it was finally abandoned in January 2011, but it is to be replaced by a series of regional initiatives that continue the martial stance. This is more than formal resemblance. The accelerated expansion of the Border Patrol, from 4000 in the 1990s through 9000 in 2000 to over 20 000 by 2010, attracts veterans from Afghanistan and Iraq, and many of the additional National Guard troops being deployed have also served in Afghanistan and Iraq. Many of the new border technologies have been tested in those theatres too. A Predator was first deployed for surveillance and reconnaissance on the southern border in 2005; since September 2010 four Reapers have been in service, transmitting hi-resolution full-motion video and infrared imagery to ground control stations, and the UAV fleet will increase to six in 2011; and from February 2011 high-altitude Global Hawks have been flying over Mexico to provide imagery to joint counternarcotics fusion centres. In fact, US commanders are now reported to be considering the transfer of border control technology from the southern border back to Afghanistan to interdict the Taliban's 'rat lines' into Pakistan (Robinson 2011).

These developments have primed the pump for making a direct connection between cartels and insurgency. This is a central contention of one school of counterinsurgency theory that links 'third-generation gangs' to 'fourth-generation warfare' as part of 'a new urban insurgency' (Manwaring 2005). Third-generation gangs are transnational criminal organisations that are supposed to reside 'at the intersection between crime and war'. They seek to increase profits and consolidate power by providing shadow governance, and so combine 'political and mercenary aims' in ways that are held to threaten not only security but also ultimately sovereignty (Sullivan 2006, 488–9; Manwaring 2006). There are parallels between the *mano dura* and *mano amiga* strategies used against gangs and the kinetic and non-kinetic operations of mainstream counterinsurgency too, but here again the claim involves more than family resemblances. The cartels are said to have evolved into 'criminal states' that pose a strategic threat to the Mexican state and, for that very reason, to the United States too. The fear is not simply that violence will spill across the border but that 'lawless Mexico' will become 'a staging ground for terrorists' (Sullivan and Elkus 2008).

These claims are not the work of fringe commentators. US Joint Forces Command (2008) has described the state failure of either Pakistan or Mexico as 'worst case scenarios' for US national security. Alarmed at the 'growing assault' on the Mexican state by the cartels, it warned that 'any descent by Mexico into chaos would demand an American response based on the serious implications for homeland security alone' (US Joint Forces Command 2008, 34, 38). In 2010 the Center for a New American Security (CNAS) issued a report arguing that 'criminal networks linking cartels and gangs are no longer simply a crime problem, but a threat that is metastasising into a new form of widespread, networked criminal insurgency' that is no longer simply a problem for law enforcement but a 'strategic threat' (Killebrew and Bernal 2010, 5). The oncological metaphor has become commonplace in

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

discussions of insurgency and converts counterinsurgency into a form of chemotherapy in which some are killed in order for others to live. The CNAS report drew a direct (biomedical) line from the United States to Mexico. 'No state in the hemisphere is more important to U.S. security than Mexico, which is fighting for its life against a widespread criminal insurgency' (Killebrew and Bernal 2010, 15). Secretary of State Hillary Clinton lost no time in echoing these concerns. Addressing the Council on Foreign Relations just days before the anniversary of 9/11, she announced that the US faced 'an increasing threat from a well-organised network[ed], drug-trafficking threat that is, in some cases, morphing into or making common cause with, what we would consider an insurgency, in Mexico and in Central America' (Richter and Delanian 2010). Her remarks were condemned in Mexico, whose military has often had a tense relationship with that of the United States, but they confirmed the relocation of the 'drug wars' to a still wider military–security nexus. NORTHCOM has started to work with Mexico's armed forces, and officers 'see similarities with their own counterinsurgency efforts' and are providing instruction in techniques developed in Afghanistan and Iraq (Sheridan 2010).

These collaborations reach far beyond 'Amexica' and even beyond insurgency. In February 2011 Secretary of Homeland Security Janet Napolitano revealed that the US had been monitoring the cartels 'for possible connections to al Qaeda' and its affiliates, and that 'we have for some time been thinking about what would happen if al Qaeda were to unite with the Zetas' (Yager 2011). Indeed, a report from the Council on Foreign Relations claimed that the tactics used by cartels 'often resemble those of terrorists or insurgents'; while the objectives of drug trafficking organisations remained 'profit-seeking rather than politically motivated', the threat to national security was sufficiently serious to require joint action (Shirk 2011). Ultimately, Grandin (2010 2011) suggests that there are grounds for suspecting that the Obama administration is seeking to establish a 'security corridor' from Colombia through Central America to Mexico, presided over by a 'unified, supra-national counterinsurgent infrastructure'. He sees this not only as the military armature for neoliberalisation but also as an experimental laboratory for the construction of 'a perfect machine of perpetual war'.

Cyberspace

Cyberspace is another ambiguous domain, where virtual space and physical space, online and offline worlds, intermingle, support and transform one another. That late modern war should take advantage of these intimacies is not surprising. The technical core of the internet was the packet-switching protocol devised for the US Defense Advanced Research Projects Agency (DARPA) in 1969, and the Revolution in Military Affairs has involved concepts of network-centric warfare in which advanced surveillance and communication systems occupy a central place. For this reason military nodes in the network have become prime targets, and the 'forced de-modernisation' of late modern infrastructural war – what Graham (2010) calls 'switching cities off' – has made civilian nodes prime targets too. The possibility of cyber warfare was latent within the system from its very beginning: the first message to be transmitted over ARPANET was to have been 'login', but the system crashed after only 'lo' had been sent. Deliberately disabling selected systems is the core of cyber warfare, which is a form of autoimmune attack that turns the network against itself. Its most common forms to date have involved targeting sites through barrages of distributed denial of service (DDS) attacks that overwhelm servers but there have also been stealth attacks that use malware to degrade operating systems.

DDS attacks are relatively straightforward. From July 2008, for example, Georgia government servers were subjected to coordinated barrages of millions of requests that overloaded and eventually shut them down. Georgia accused Russia of conducting a cyber warfare campaign against its websites as part of the escalating conflict over South Ossetia. Botnets (computers taken over by hackers) were traced to hosting services controlled by the Russian Business Network, a criminal organisation based in St Petersburg, and when Russian troops entered South Ossetia a posting on a Russian hacker forum invited 'would-be cyber-militia members to enlist at a private, password-protected online forum' where they were provided with target lists and instructions. This episode is significant not only because it was 'the first time a known cyber-attack had coincided with a shooting war' (Markoff 2008) but also because it suggests an emerging model of cyber warfare that involves both the outsourcing of cyber attacks and the militarisation of cybercrime. 'Nearly every significant cyber event reported since 2005 involves tradecraft, techniques and code tied to the cyber-crime community' (Farwell and Rohozinski 2011, 26).

Advanced militaries rely heavily on outsourcing for logistics and other functions, but the practice has an additional advantage in cyber warfare because the distributed nature of cyber attack capitalises on 'the dark ecology of cyberspace' to conceal the identity of the aggressor (Farwell and Rohozinski 2011, 27). Stealth attacks compound this advantage by concealing the attack itself. Here Stuxnet, which was launched in November 2008 but only discovered in July 2010, may be exemplary. This is malware that exploits four unpatched Microsoft Windows vulnerabilities to modify the code on programmable logic controllers (PLCs). Software security analysts describe Stuxnet as a 'precision, military-grade cybermissile' that is capable of digitally 'fingerprinting' a computer system to determine whether it is the target it is tasked

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

to destroy. It is aimed at PLCs made by Siemens; it intercepts commands to specific frequency-converter drives running at unusually high speeds and changes the output frequencies for short periods of time. Some of the most revealing forensic analysis has been undertaken by cyber-security consultant Ralph Langner:

> Stuxnet can be thought of as a stealth control system that resides on its target controllers along with legitimate program code. The ultimate goal of the attack is not the controller; it is what the controller controls. Attack code analysis reveals that the attackers had full knowledge of project, installation and instrumentation details. The attackers took great care to make sure that only their designated targets were hit. It was a marksmen's job. On target, the attack is surgical and takes advantage of deep process and equipment knowledge. The attack is not performed in a hit-and-run style, where it would be executed immediately after attaching to the controller or at the next best opportunity. Instead, the attack code carefully monitors the hijacked process for extended periods of time before executing the strike. Outputs are then controlled by Stuxnet, with neither legitimate program code nor any attached operator panel or SCADA [supervisory control and data acquisition] system noticing. Stuxnet combines denial of control and denial of view, providing for the ultimate aggressive attack.
>
> Langner (2011b)

Symantec had identified 100 000 infected hosts by September 2010; 60% of them were in Iran, which made this the likely target zone. Since the most probable candidates for Stuxnet are PLCs governing centrifuges and turbine control systems, Langner initially narrowed the geography of attack to the uranium-enrichment plant at Natanz and the light-water reactor at Bushehr. The latter does not produce weapons-grade plutonium, however, and experts now agree that Natanz was the target.

There is ongoing debate about how effective the attack has been – Israel and the United States estimate that Iran's development program has been delayed by several years but Teheran has shrugged this off – but also, given its stealth geography, about the origin of the attack. Two intersecting lines of investigation have been pursued. One proposes some sort of collaboration between the United States' Idaho National Laboratory, which in 2008 had worked in conjunction with the Department of Homeland Security and Siemens to identify vulnerabilities in its PLCs, and Israel's Negev Nuclear Research Center at Dimona, which is alleged to have replicated Iran's nuclear centrifuges in order to test Stuxnet (Broad *et al*. 2011). It is surmised that operational control then passed to Unit 8200, the Central Collection Unit of the Intelligence Corps of the Israeli Defense Force, as part of what Langner (2011a) has identified as Myrtus, 'a multi-year cyberwar campaign aiming to corrupt the Iranian uranium enrichment program up to the point where the cost for Tehran to pursue this program under tightening sanctions gets too high'. The other, which may well be embedded in the first, detects a link:

> between the code used by the worm and the burgeoning Russian offshore programming community, where talented programmers work in the grey market of code. In this community, there is no neat division between programmers working one day with Siemens SCADA equipment for an industrial client in Saratov and the next programming online gaming software for the Israeli-owned offshore gaming services in Ireland and the UK.
>
> Farwell and Rohozinski (2011, 27)

It is virtually impossible to determine how far the US was involved in the attack, though Gross (2011) believes there is now 'vanishingly little doubt that the United States played a role in creating the worm'. In any event, although Stuxnet spread virally far beyond its presumed target, its *operational* precision shows that cyber warfare has developed far beyond the capacity proposed for the United States by a USAF colonel who once urged the development of 'the ability to carpet bomb in cyberspace'. 'Not every attack has to be made with a laser-guided bomb', he argued, and since 'area bombing' against the Taliban had been so successful (sic) in Afghanistan he could not see what was wrong with its equivalent in cyberspace (Williamson 2008). He clearly had DDS attacks in mind, but he saw these as a deterrent – a defensive capacity – and recommended the staging of 'live-fire exercises on the Internet' to demonstrate the effect. His model of deterrence assumed that it is possible to identify the source of an attack, however, whereas the problem of attribution combines with the practice of outsourcing to make such a strategy in cyberspace at best ineffective and at worst misdirected. Conventional notions of neutrality are compromised in cyberspace, and presumably for those reasons the United States has preferred to develop alternative modes of cyber defence.

US Cyber Command was activated on 1 May 2010, and endorsing Williamson's insistence that 'the time for fortresses on the Internet has passed', US Deputy Secretary of Defense William J. Lynn accepted that 'a fortress mentality will not work'. Cyberspace is 'an offense-dominated environment', he explained, and 'the United States cannot retreat behind a Maginot Line of firewalls, or it will risk being overrun' (Lynn 2010, 97–8). Public statements have emphasised CYBERCOM's role in protecting digital infrastructure as a 'strategic national asset'. The US military operates more than seven million computer devices on 15 000 networks, and every hour there are hundreds and thousands of unauthorised probes of Pentagon and associated computer systems, but Lynn assured his audience that the Department of Defense had in place robust and

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society
(with the Institute of British Geographers)

layered cyber defences that could detect, rebut and repair intrusions across the .mil domain (Lynn 2010). He floated the possibility of applying these capabilities beyond the .mil and .gov domains to protect .com domains in the US defence industry. The commander of CYBERCOM has continued to maintain that 'this is not about efforts to militarize cyberspace' – any more, I imagine, than the United States is militarising its southern border – but for Hersh (2010) the prospect raised questions about 'where the battlefield begins and where it ends': 'If the military is operating in cyberspace, does this include civilian computers in American homes?'

The question is a good one, but it needs to be directed outwards as well as inwards. For the United States is also developing an offensive capacity in cyberspace, and the mission of CYBERCOM includes the requirement 'to prepare to, and when directed conduct, full-spectrum military cyberspace operations in order to enable actions in all domains'. This is a programmatic statement, and there are difficult conceptual, technical and operational issues to be resolved. The concept of the 'cyber kill-chain' has already made its appearance: software engineers at Lockheed Martin have identified seven phases or 'border-crossings' in cyberspace through which all advanced persistent intrusions must pass so that, conversely, blocking an attack at any one of them (dislocating any link in the kill-chain) makes it possible 'to turn asymmetric battle to the defender's advantage' (Croom 2011; Holcomb and Shrewsbury 2011). The issues involved are also ethical and legal. Debate has been joined about what constitutes an armed attack in cyberspace and how this might be legally codified (Dipert 2010; Nakashima 2010), and most of all about how to incorporate the protection of civilians into the conduct of cyber warfare. In the 'borderless realm of cyberspace' Hughes (2010, 536) notes that the boundary between military and civilian assets – and hence military and civilian targets – becomes blurred, which places still more pressure on the already stressed laws of armed conflict that impose a vital distinction between the two (Kelsey 2008). Preparing for offensive operations includes developing a pre-emptive precision-strike capacity, and this is – precisely – why Stuxnet is so suggestive and why Shakarian (2011) sees it as inaugurating 'a revolution in military affairs in the virtual realm'. Far from 'carpet bombing' cyberspace, Gross (2011) describes Stuxnet as a 'self-directed stealth drone' that, like the Predator and the Reaper, is 'the new face of twenty-first century warfare'. Cyber wars will be secret affairs, he predicts, waged by technicians 'none of whom would ever have to look an enemy in the eye. For people whose lives are connected to the targets, the results could be as catastrophic as a bombing raid but would be even more disorienting. People would suffer, but [they] would never be certain whom to blame.'

Contrapuntal geographies

I have argued elsewhere that the American way of war has changed since 9/11, though not uniquely because of it (Gregory 2010), and there are crucial continuities as well as differences between the Bush and Obama administrations: 'The man who many considered the peace candidate in the last election was transformed into the war president' (Carter 2011, 4). This requires a careful telling, and I do not mean to reduce the three studies I have sketched here to a single interpretative narrative. Yet there are connections between them as well as contradictions, and I have indicated some of these en route. Others have noted them too. Pakistan's President has remarked that the war in Afghanistan has grave consequences for his country 'just as the Mexican drug war on US borders makes a difference to American society', and one scholar has suggested that the United States draws legal authority to conduct military operations across the border from Afghanistan (including the killing of bin Laden, codenamed 'Geronimo') from its history of extra-territorial operations against non-state actors in Mexico in the 1870s and 1880s (including the capture of the real Geronimo) (Margolies 2011). Whatever one makes of this, one of the most persistent threads connecting all three cases is the question of legality, which runs like a red ribbon throughout the prosecution of late modern war. On one side, commentators claim that new wars in the global South are 'non-political', intrinsically predatory criminal enterprises, that cartels are morphing into insurgencies, and that the origins of cyber warfare lie in the dark networks of cyber crime; on the other side, the United States places a premium on the rule and role of law in its new counterinsurgency doctrine, accentuates the involvement of legal advisers in targeting decisions by the USAF and the CIA, and even as it refuses to confirm its UAV strikes in Pakistan provides arguments for their legality.

The invocation of legality works to marginalise ethics and politics by making available a seemingly neutral, objective language: disagreement and debate then become purely technical issues that involve matters of opinion, certainly, but not values. The appeal to legality – and to the quasi-judicial process it invokes – thus helps to authorise a widespread and widening militarisation of our world. While I think it is both premature and excessive to see this as a transformation from governmentality to 'militariality' (Marzec 2009), I do believe that Foucault's (2003) injunction – 'Society must be defended' – has been transformed into an unconditional imperative since 9/11 and that this involves an intensifying triangulation of the planet by legality, security and war. We might remember that biopolitics, one of the central projects of late modern war, requires a legal armature to authorise its interventions, and that necropolitics is not always outside the law. This triangulation has become such a common-

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

place and provides such an established base-line for contemporary politics that I am reminded of an interview with Zizek soon after 9/11 – which for him marked the last war of the twentieth century – when he predicted that the 'new wars' of the twenty-first century would be distinguished by a radical uncertainty: 'it will not even be clear whether it is a war or not' (Deichmann *et al*. 2002).

Neither will it be – nor is it – clear where the battlespace begins and ends. As I have tried to show, the two are closely connected. For this reason I am able to close on a less pessimistic note. As I drafted this essay, I was watching events unfold on the streets of Cairo and other Egyptian cities, just weeks after similar scenes in Tunisia. I hope that the real, lasting counterpoint to 9/11 is to be found in those places, not in Afghanistan, Pakistan or Iraq. For those events show that 'freedom' and 'democracy' cannot be limited to the boastful banners of military adventurism, hung from the barrels of guns or draped across warships, and that ordinary people can successfully rise up against autocratic, repressive and corrupt regimes: including those propped up for so long by the United States and its European allies. Perhaps one day someone will be able to write about 'the nowhere war' – and not from Europe or North America.

Acknowledgements

This essay is a revised version of 'War in the borderlands', first delivered as a Miliband Lecture at the London School of Economics in December 2010. I am deeply grateful to Simon Dalby, Klaus Dodds, Craig Jones, Matt Sparke, Juanita Sundberg, Melissa Wright and two anonymous referees for their comments on my first fumbling attempts to convert the lecture into written form. My work on these issues has been supported by a grant from the Social Sciences and Humanities Research Council.

References

Amoore L and de Goede M 2011 Risky geographies: aid and enmity in Pakistan *Environment and Planning D: Society & Space* 29 193–202

Anderson B 2011 Facing the future enemy: US counterinsurgency doctrine and the pre-insurgent *Theory, culture and society* forthcoming

Anzaldúa G 1987 *Borderlands/La Frontera: the new Mestiza* Aunt Lute Books, San Francisco

Axe D 2011 Bin Laden killing in legal gray zone, 6 May (www-.politico.com) Accessed 20 May 2011

Bacevich A 2010 *Washington rules: America's path to permanent war* Metropolitan Books, New York

Bauman Z 2002 Reconnaissance wars of the planetary frontierland *Theory, Culture and Society* 19 81–90

Benvenisti E 2010 The legal battle to define the law on transnational asymmetric warfare *Duke Journal of Comparative International Law* 20 339–59

Blank L 2010–11 Defining the battlefield in contemporary conflict and counter-terrorism: understanding the parameters of the zone of combat *Georgia Journal of International and Comparative Law* 39 forthcoming

Broad W, Markoff J and Sanger D 2011 Israeli tests on work called crucial in Iran nuclear delay *New York Times* 15 January

Carter S 2011 *The violence of peace: America's wars in the age of Obama* Beast Books, New York

Castro R 2007 Busting the Bandito Boyz: militarism, masculinity and the hunting of undocumented persons in the US-Mexico borderlands *Journal of Hate Studies* 6 7–24

Cavanaugh M and Heilbrunn S 2010 Behind the scenes of *National Geographic's* 'Border Wars' documentary, 5 January (www.kpbs.org/news/2010/jan/05/border-wars) Accessed 20 May 2011

Cloud D 2010 CIA drones have broader list of targets *Los Angeles Times* 5 May

Coleman M 2005 US statecraft and the US–Mexico border as security/economy nexus *Political Geography* 24 185–209

Croom C 2011 The cyber kill-chain: a foundation for a new cyber-security strategy *High Frontier* 6 52–6

Deichmann T, Reuel R and Zizek S 2002 About war and the missing center in politics *Eurozine* 15 March

Dipert R 2010 The ethics of cyberwarfare *Journal of Military Ethics* 9 384–410

Doty R 2007 States of exception on the Mexico–US border: security, 'decisions' and civilian border patrols *International Political Sociology* 1 113–37

Doty R 2011 Bare life: border-crossing deaths and moral alibi *Environment and Planning D: Society & Space* forthcoming

Duffield M 2001 Governing the borderlands: decoding the power of aid *Disasters* 25 308–20

Duffield M 2007 *Development, security and unending war* Polity, Cambridge

Dunn T 1996 *The militarization of the U.S.–Mexico border, 1978–1992: low intensity conflict doctrine comes home* CMAS Books, Center for Mexican American Studies, Austin TX

Engelhardt T 2010 *The American way of war: how Bush's wars became Obama's* Haymarket Books, New York

Engelhardt T and Turse N 2010 The shadow war: making sense of the new CIA battlefield in Afghanistan *TomDispatch* 10 January (www.tomdispatch.com) Accessed 20 May 2011

Etzioni A 2010 The secret matrix *The world today* 66 11–14

Farwell J and Rohozinski R 2011 Stuxnet and the future of cyber war *Survival* 53 23–40

Filkins D 2008 *The forever war* Knopf, New York

Foucault M 2003 *'Society must be defended': Lectures at the* Collège de France *1975–1976* (trans. David Macey) Picador, New York

Graham S 2009 Cities as battlespace: the new military urbanism *City* 13 383–402

Graham S 2010 *Cities under siege: the new military urbanism* Verso, London

Grandin G 2010 Muscling Latin America *The Nation* 21 January

Grandin G 2011 Building a perfect machine of perpetual war Nation Institute, 11 February (www.thenation.com/blog) Accessed 20 May 2011

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

Gregory D 2004 *The colonial present: Afghanistan, Palestine, Iraq* Blackwell, Oxford
Gregory D 2010 War and peace *Transactions of the Institute of British Geographers* 35 154–86
Gregory D 2011 From a view to a kill: drones and late modern war *Theory, culture and society* forthcoming
Gros F 2010 *States of violence: an essay on the end of war* Seagull, London
Gross M 2011 A declaration of cyber-war *Vanity Fair* April
Hersh S 2010 The online threat *New Yorker* 1 November
Holcomb L and Shrewsbury J 2011 Securing our cyber-borders *Innovation* 9 (1) n.p.
Horton S 2010 The trouble with drones *Harper's* 3 May
Hughes R 2010 A treaty for cyberspace *International Affairs* 86 523–41
Human Rights Watch 2010 Letter to Obama on targeted killings and drones (www.hrw.org/en/news/2010/12/07/letter-obama-targeted-killings) Accessed 20 May 2011
Jimenez M 2009 *Humanitarian crisis: migrant deaths at the US–Mexico border* American Civil Liberties Union, San Diego, California October
Keen D 2006 *Endless war? Hidden functions of the 'war on terror'* Pluto Press, London
Kelsey J 2008 Hacking into International Humanitarian Law: the principles of distinction and neutrality in the age of cyber warfare *Michigan Law Review* 106 1427–51
Killebrew B and Bernal J 2010 *Crime wars: gangs, cartels and US National Security* Center for a New American Security, Washington DC
Langner R 2011a What Stuxnet is all about, 10 January (www.langner.com) Accessed 20 May 2011
Langner R 2011b How to hijack a controller, 13 January (www.controlglobal.com) Accessed 20 May 2011
Lynn W 2010 Defending a new domain: the Pentagon's Cyberstrategy *Foreign Affairs* 89 97–108
Mahmud T 2010 Colonial cartographies, postcolonial borders and the enduring failures of international law: the unending wars along the Afghanistan–Pakistan frontier *Brooklyn Journal of International Law* 36 1–75
Manwaring M 2005 *Street gangs: the new urban insurgency* Strategic Studies Institute, United States Army War College, Carlisle PA
Manwaring M 2006 Gangs and coups d'streets in the new world disorder: protean insurgents in post-modern war *Global crime* 7 505–43
Margolies J 2011 Geronimo, Bin Laden and US foreign policy *History News Network* 5 May
Markoff J 2008 Before the gunfire, cyberattacks *New York Times* 12 August
Marzec R 2009 Militariality *The Global South* 3 139–49
Masood S and Shah P Z 2011 CIA drones kill civilians in Pakistan *New York Times* 17 March
Mayer J 2009 The Predator war *New Yorker* 26 October 36–45
Mazzetti M 2010 CIA takes on bigger and riskier role on front lines *New York Times* 1 January
Mbembe A 2003 Necropolitics *Public Culture* 15 11–40
Mckelvey T 2011 Inside the killing machine *Newsweek* 13 February
Miller G 2011 Increased drone strikes in Pakistan killing few high-value militants *Washington Post* 21 February
Münkler H 2005 *The new wars* (trans. P. Camiller) Polity, Cambridge
Murphy S 2009 The international legality of US military cross-border operations from Afghanistan into Pakistan, George Washington University Law School, Public Law and Legal Theory Working Paper, 451/Legal Studies Research Paper 451
Nakashima E 2010 US eyes pre-emptive cyber-defense strategy *Washington Post* 29 August
Nevins J 2002 *Operation Gatekeeper: the rise of the 'illegal alien' and the making of the US–Mexico boundary* Routledge, New York
O'Connell M 2009 Unlawful killing with combat drones: a case study of Pakistan, 2004–2009, Notre Dame Law School, Legal Studies Research Paper 09-43
Paust J 2010 Self-defense targetings of non-state actors and permissibility of US use of drones in Pakistan, University of Houston Public Law and Legal Theory Series 2009-A-36 *Journal of Transnational Law and Policy* 19 237–80
Report of the Majority Staff 2010 *Warlord, Inc. extortion and corruption along the US supply chain in Afghanistan* Report of the Majority Staff, Subcommittee on National Security and Foreign Affairs, US House of Representatives, Washington DC
RETORT 2005 *Afflicted powers: capital and spectacle in a new age of war* Verso, London and New York
Richter P and Delanian K 2010 Clinton says Mexico drug wars starting to look like insurgency *Los Angeles Times* 9 September
Robinson M 2011 US looks to Mexico to tighten Afghan border Reuters, 1 March
Rodriguez A 2011 Pakistan denounces US drone strike *Los Angeles Times* 18 March
Rogers C 2010 *Civilian harm and conflict in Northwest Pakistan* Campaign for Innocent Victims in Conflict (CIVIC), Washington DC
Rosas G 2006 The thickening of the borderlands *Cultural dynamics* 18 335–49
Rosas G 2007 The fragile ends of war: forging the United States–Mexico border and borderlands consciousness Social text 25 81–102
Sassen S 2010 When the city itself becomes a technology of war *Theory, culture and society* 27 33–50
Shakarian P 2011 Stuxnet: cyberwar revolution in military affairs *Small Wars Journal*, April (www.smallwarsjournal.com) Accessed 20 May 2011
Shane S, Mazzetti M and Worth R 2010 Secret assault on terrorism widens on two continents *New York Times* 14 August
Sheridan M B 2010 US military helping Mexican troops battle drug cartels *Washington Post* 10 November
Shirk D 2011 *The drug war in Mexico: confronting a shared threat* Council on Foreign Relations, Washington DC
Singer P 2010 We, Robot *Slate* 19 May
Sparke M 2007 Everywhere but always somewhere: critical geographies of the global South *The Global South* 1 117–26
Stone K 2003 *'All means necessary': employing CIA operatives in a warfighting role alongside Special Operations Forces* US Army War College, Strategic Research Project

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)

Sullivan J 2006 *Maras* morphing: revisiting third generation gangs *Global crime* 7 487–504

Sullivan J and Elkus A 2008 State of siege: Mexico's criminal insurgency *Small Wars Journal* (http://smallwarsjournal.com) Accessed 20 May 2011

Sundberg J 2011 Diabolic *Caminos* in the desert and cat fights on the Rio: a posthumanist political ecology of boundary enforcement in the United States–Mexico borderlands *Annals of the Association of American Geographers* 101 318–36

US Joint Forces Command 2008 *Joint operating environment 2008: challenges and implications for the future joint force* (www.jfcom.mil/newslink/storyarchive/2008/JOE2008.pdf) Accessed 8 June 2011

Vulliamy E 2010 *Amexica: war along the borderline* Farrar, Strauss and Giroux, New York

Williamson C 2008 Carpet bombing in cyberspace *Armed Forces Journal* May

Yager J 2011 Napolitano warns of threat from homegrown radicalization, terrorism *The Hill* 9 February

© 2011 The Author. The Geographical Journal © 2011 Royal Geographical Society (with the Institute of British Geographers)