The “Revolution in Military Affairs” and Counter-Insurgency

Written by Philip Stibbe

This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

The “Revolution in Military Affairs” and Counter-Insurgency

https://www.e-ir.info/2012/08/25/how-relevant-is-the-revolution-in-military-affairs-to-counter-insurgency/

PHILIP STIBBE, AUG 25 2012

How Relevant is the “Revolution in Military Affairs” to Counter-Insurgency?

Throughout military history, various technological innovations – such as the stirrup, the tank, and the nuclear bomb – have had differentiated effects upon the conduct and outcomes of warfare.[1] Academics have even branded some of these innovations “Revolutions in Military Affairs” (RMAs); i.e., major changes to longstanding and entrenched characteristics of warfare.[2] Since the early 1990s, however, many military analysts have pointed to a particular RMA. That is, a revolution featuring distinctive advances in stealth and long-range precision-strike weapons technology, as well as innovations in information and communications technology (ICT) (e.g. advanced sensor equipment and internet-based information warfare).[3] In this RMA, furthermore, advances in ICT are thought to facilitate military commanders’ labours to attain complete, instantaneous and near-flawless battlefield information for identifying and eliminating the enemy.[4] Additionally, ICT improvements enable the development of Admiral Owens’ ‘system of systems’, whereby the information systems of particular units within an armed force (land, air, and sea) can be accumulated and synchronised within an overarching system in order to maximise unit coordination and combat effectiveness.[5] This ICT innovation, combined with complex precision-weaponry (notably in the forms of airpower), thus presents a RMA which is intended to minimise casualties (both non-combatant and friendly combatant), and aid commanders in achieving a swift and decisive victory over an enemy force with as few resources as possible.[6]

The concerned RMA has distinctly affected outcomes in specific inter-state conflicts. Indeed, the swift US-led victory over Iraq during the First Gulf War (which featured devastating F-117A and Tornado GR-1 precision bombings) has even led some analysts to conclude that the US is ‘unbeatable when fighting on their own terms’. [7] This study, however, seeks to analyse the significance of the RMA to counterinsurgency (COIN). COIN may be defined as the amalgamation of those efforts – political, economic, military, and social – intended to protect a state against an insurgency, with the aim of defeating the latter.[8] An insurgency, moreover, may be conceived as an irregular armed force which opposes the existing political order through protracted armed conflict.[9] An insurgency moreover comprises members from at least one specific population, and operates illegally within a state’s territory.[10]

This study is divided into two sections. Firstly, it analyses the influence of the RMA upon overtly political COIN operations; i.e., those operations intended to bolster support and legitimacy for the COIN government, specifically from the local population.[11] Secondly, the impact of the RMA upon military COIN operations will be examined; i.e. those operations intended to identify, isolate, and destroy insurgent forces.[12] Although these categories inevitably overlap (indeed, Clausewitz rightly highlighted that politics permeates war), they do highlight the ‘interplay between ...political and military actions’ in COIN operations.[13]

Many scholars have rightly questioned whether the RMA has truly “revolutionised” contemporary warfare.[14] It is the contention of this analysis that technological innovations have bestowed COIN practitioners with limited advantages over insurgents only in specific military “clearing” operations. Additionally, it will also be argued that the RMA has failed to markedly improve political COIN operations, and has actually bequeathed more advantages to the insurgent. This study draws upon a range of COIN case studies to make its argument, including Afghanistan, Pakistan, Iraq
Section 1: the RMA and political COIN operations

It is an oft-cited maxim amongst military analysts that COIN operations should be four-fifths political and one-fifth military; i.e. COIN should prioritise population security over elimination of the enemy through military means.[15] Underlying this conventional thinking is the notion that insurgencies survive and thrive by portraying themselves as the embodiment of a population’s grievances against the prevailing political order.[16] Consequently, addressing these grievances (whether political, economic, religious etc.) is vital if a state is to gain popular support and thus undermine an insurgency’s support base. In Afghanistan, for instance, General Stanley McChrystal in 2009 argued that bolstering the Afghan government’s legitimacy in the eyes of Afghans required ISAF to focus their efforts mainly upon population security, rather than troop protection and kinetic operations against the Taliban.[17] To achieve this goal, McChrystal maintained that additional ISAF and ASF troops were needed on the ground in order to provide a greater sense of security amongst Afghans. [18] It was thought that this would boost the population’s confidence in the Afghan government, whilst also providing extra space for development and humanitarian assistance in areas cleared of insurgents during ‘clear, build, hold, transfer’ operations.[19]

At face value, this classical COIN approach contradicts certain teleological aims of the RMA. In particular, the former emphasises the need for a large military contingent (at least 20 COIN troops per 1,000 civilians) which is willing to accept considerable risk of casualties, which is committed to prioritising civilian security, and which is prepared to do so over several years.[20] The predominant RMA vision, however, envisages commanders employing minimal troops and resources, at minimal risk/cost, into a military theatre in order to attain decisive military victory over an enemy as soon as possible.[21] Consequently, this underlying purpose to current RMA technological can actually encourage the predisposition of certain military establishments to tailor their armed forces towards swift/decisive conventional conflicts (like the 1991 Gulf War) instead of protracted COIN operations.[22] Adamsky, for instance, rightly highlights how the US public and political-military establishment are extremely sensitive to US troop losses, such that US strategic culture emphasises sending ‘metal into battle instead of vulnerable flesh’ wherever possible.[23] Moreover, US strategists are thought to typically possess considerable confidence in the capacity of technology (e.g. precision airstrikes) to resolve strategic problems, as well as an expectation that action should produce discernible near-term results.[24] The RMA can thus buttress a military organisational culture which believes that conventional forces/tactics can be applied easily and appropriately to COIN operations.[25] This appeared to be the case in Iraq. Indeed, until 2004, US commanders in Iraq failed to prepare US forces to counter the rising insurgency at least partly because the Bush administration was preoccupied with developing precision-weapony for conventional inter-state warfare.[26] Moreover, when the insurgent threat was finally acknowledged, the US began constructing Iraqi forces designed for border-policing rather than intra-state COIN operations.[27]

As such, the common ‘techno-euphoria’ underlying the RMA which emphasises weapon speed, range and precision certainly seems at odds with COIN’s classical emphasis on providing a pervasive military presence and ‘very long time frames’. [28]

However, ICT innovations underlying the RMA certainly seem highly relevant to information warfare during COIN. In COIN, information warfare involves both sides seeking to obtain superior information about the other in order to gain the tactical advantage.[29] Additionally, both sides endeavour to manipulate information in order to sway the opinions of allies, non-aligners, and enemies in the civilian populace to their cause.[30] Typically, COIN theatres feature a population which is largely uncommitted to neither the government nor the insurgency, whilst minority groups support either side; accordingly, victory for COIN entails persuading the non-committed majority to accept the legitimacy of the government.[31] This aim, therefore, forms the basis of COIN “hearts and minds” (or “political”) operations, and is thought to be accomplished by delivering civilian protection, political stability and humanitarian assistance.[32] The ICT revolution, as such, has enabled both the COIN and insurgent to disseminate their messages, in a virtual dimension, to a wider range of audiences at home and abroad.[33] Civilians worldwide are thus increasingly more able to access information about an insurgency or COIN campaign, particularly through use of the international media, mobile/smart phones and laptops with internet availability.[34] Indeed, Betz correctly notes that ‘propaganda of the deed’ has become a form of ‘political marketing’ in the virtual dimension for both COIN and the insurgent,
The ICT innovations of the RMA certainly intensify the responsibility of COIN practitioners to communicate truth to civilians at home and abroad, in order to preserve their credibility and legitimacy.[36] During the Second Russian-Chechen War, for instance, Chechen separatists were able to discredit Russian accounts of battles and incidents by publicising video recordings of the real events on internet websites.[37] These videos were also important propaganda tools for recruiting fighters locally and also internationally, such as Wahhabites from the Persian Gulf who perceived the Russian-Chechen war as a *jihadist* struggle against an oppressive atheist regime.[38] Indeed, the Chechen case shows how ICT innovations have assisted insurgencies in becoming more "globalised"; i.e. whilst 20th century insurgencies (e.g. Malaya) were usually nationalistic and obtained their support principally from the local populace, contemporary insurgencies increasingly feature a support-base, a military constitution and a financial-base which stem considerably from international as well as local sources.[39]

The implications of this are huge for COIN. In Malaya, for instance, the British were able to "choke" the insurgency by forcibly relocating civilians, which inhibited communication and supplies-trading between insurgents and the civilian population (the Briggs Plan).[40] In Afghanistan, however, ISAF/NATO cannot use similar tactics to "choke" the Taliban, whose membership comprises Afghan and Pakistani-based Pashtuns (a transnational ethnic group), as well as foreign fighters. Besides, to attempt to do so would undermine ISAF’s strategic narrative of promoting democracy, good governance and self-determination in Afghanistan.[41] Moreover, ICT innovations – in conjunction with the international media – magnify the inescapable failings of COIN forces in the public eye. In Afghanistan during January 2012, for instance, US credibility was undermined when international media outlets circulated a videotape showing four US marines urinating on Taliban corpses.[42] Afghan outrage was further exacerbated the following month when U.S. soldiers burned confiscated Korans from detained Taliban prisoners, which sparked anti-U.S. demonstrations across Afghanistan.[43]

Whilst an insurgency’s actions may affect civilian perceptions of its legitimacy, “propaganda of the deed” seems far more vital for COIN success. Consequently, COIN practitioners are more vulnerable to ICT innovations which highlight inconsistencies in their strategic narrative.[44] This is because COIN practitioners’ legitimacy hinges on their ability to preserve order/security in a respective society. Accordingly, the insurgent can weaken the COIN’s legitimacy even through flagrant terror tactics against civilians (since this undermines both order and security).[45] Moreover, the RMA creates an ‘illusion of war that …engenders false expectations of its risks and potential costs’, which thus exacerbates public outrage at home when international COIN forces fail to thwart insurgent terror attacks against civilians (which are frequently assumed to be preventable).[46]

Section 2: the RMA and military COIN operations

Whilst population security is widely understood to form the foundation of successful COIN operations, military analysts typically understand this to regularly involve both defensive and offensive military COIN operations which aim to identify, isolate and eliminate insurgent forces.[47] Such operations, however, are inevitably constrained by ethical, political and practical limitations, since insurgents are typically able to blend in with the indigenous population (i.e. they are ‘fish’ swimming in the ‘sea’ of the population).[48] As such, hostilities between belligerents ensue ‘in the streets and houses and fields’ of the civilian populace rather than a distant battlefield.[49] Additionally, since COIN forces are characteristically endowed with greater firepower, training and equipment, insurgent forces typically employ guerrilla tactics (ambushes, hit-and-run attacks and aversion of overt military confrontation) in order to exhaust the morale of COIN forces in a protracted struggle.[50] Consequently, given an insurgency’s capability to conceal itself, analysts such as Kitson contend that effective COIN employs maximal use of intelligence (human, signals and electronic) to uncover the insurgent from the civilian crowd in order to detain/eliminate him.[51]

Owen’s ‘system of systems’ thus seems highly relevant to military COIN operations.[52] For instance, in Afghanistan the ISAF/NATO Command and Control system enables HQ commanders to share information and communications near-instantaneously with military units – in several Areas of Operations (AOs) – across an entire military theatre.[53] Subsequently, COIN land forces can be provided Rules of Engagement (ROE) promptly from central command centres in the event of an insurgent attack upon COIN forces, whilst HQ can order Allied Rapid Reaction Corps
The “Revolution in Military Affairs” and Counter-Insurgency
Written by Philip Stibbe

(AARC) to swiftly reinforce a particular unit in a specific military engagement.[54] Additionally, many technological innovations (e.g. PCs with internet capacity and mobile phones) have filtered-down into many societies where COIN is conducted. Consequently, civilians can swiftly and anonymously SMS the known locations, movements and activities of insurgents to COIN forces for interception.[55] Sophisticated ICT systems also enable COIN intelligence analysts to track emails, online money transfers and IP addresses of insurgents propagating their cause online (which might then present leads to other insurgents’ whereabouts).[56] This can then result in detentions or targeted killings. For example, in 2004 two Russian intelligence agents – Vasily A. Bogachyov and Anatoly V. Belashkov – were able to follow the human/electronic trail of former Chechen president Zelimkhan Yandarbiyev to his location in Doha, where they assassinated him using a car bomb.[57] In Afghanistan, moreover, intelligence gathered from human, electronic and aerial sources (e.g. from unmanned aerial vehicles – or UAVs) have enabled ISAF special forces (SFs) to apprehend or kill roughly 300 insurgent leaders between July-September in 2010 alone.[58]

However, whilst technologies such as UAVs, satellite surveillance and airborne infra-red (IR) equipment can provide extensive 24-hour reconnaissance in a given AO, there are enormous limitations to their utility in protracted COIN operations.[59] ICT technologies – whilst often useful to COIN for tracing/locating insurgents – are limited by the insurgent’s ability to conceal their identity using online aliases (e.g. on Youtube or MySpace), and by utilising software which facilitates user-anonymity.[60] Moreover, intelligence concerning insurgents’ whereabouts can still be limited, or misleading to the fallible human observer. The US-led Operation Anaconda in Afghanistan (2002) is a compelling example; although extensive reconnaissance was undertaken in the 100-square-kilometre AO prior to the battle, less than half of Al-Qaida’s actual defensive positions were located.[61] Indeed, dummy defences and force-camouflage remain effective tactics for insurgents wishing to protect their defensive positions against current RMA technologies; ground-contact between COIN and insurgent forces is often still necessary to locate and dislodge these positions.[62]

Precision-weaponry alone also usually cannot completely destroy defensive positions, even in conventional warfare. In Afghanistan’s Qala-e-Gangi stronghold, for example, hideaway Taliban fighters managed to survive ‘entire ammunition payloads of multiple AC-130 Spectre gunships’ as well as ‘seven 2,000-pound satellite-guided bombs’.[63] Furthermore, different types of aerial reconnaissance each possess distinct limitations within a specific COIN theatre. For instance, both the Joint Surveillance Target Attack Radar System (JSTARS) and the Airborne Warning and Control System (AWACS) can manage more information than UAVs, and generally possess better sensor technology for identifying/tracking enemy targets.[64] UAVs, however, possess greater ‘loiter time’ than AWACS and JSTARS, and have greater stealth-capability, yet they are vulnerable to sandstorms, powerful winds and light insurgent weapons.[65] Indeed, in February 2012 Taliban fighters claimed to have shot down a UAV in North Waziristan, which served as a powerful propaganda tool for undermining popular confidence in the COIN coalition forces.[66] Moreover, whilst UAVs, AWACS and JSTARS may be useful tools for COIN forces during the “clearing” stage in an AO, in the “hold” and “build” phase they seem to diminish in utility compared to the need for ‘constabulary’ troops on the ground.[67]

Indeed, the relevance of UAVs to COIN is particularly controversial because of their potential to injure or kill civilians (despite their intention to facilitate discrimination). In March 2011, for example, over 40 people were killed by US drones in North Waziristan; many of these mortalities were believed to be non-combatants.[68] The incident sparked anger and anti-American sentiment amongst indigenous tribal leaders, and almost certainly increased sympathy for the Taliban amongst the population.[69] Advancements in precision-technology therefore do not appear to have eliminated the human potential for errors in COIN, and indeed, seem to increase the political costs when such errors occur.[70] Repercussions can be particularly detrimental for COIN practitioners when precision weapons hit allied forces. In November 2011, for instance, a NATO UAV attack resulted in the deaths of 24 Pakistani troops; consequently, a significant disruption in US-Pakistani relations ensued whereby the latter responded by obstructing NATO supplies travelling through Pakistan.[71] Additionally, Pakistan removed its forces from two Border Security Centres along the Durand Line (there are three in total), which hindered Afghan-Pakistani cooperation in undermining insurgent movement across the 1,500km border.[72]

The Pakistani case additionally highlights the controversial role of stealth technology in COIN; in May 2011, US Navy Seals used state-of-the-art stealth helicopters to fly from Afghanistan to Abbottabad, Pakistan, where they killed Al-
The “Revolution in Military Affairs” and Counter-Insurgency
Written by Philip Stibbe

Qaida leader Osama bin Laden.[73] Afterwards, the U.S. proclaimed the attack a symbolic military victory against Islamist militancy, yet Islamabad perceived it as a violation of Pakistani sovereignty, and a serious deterioration in US-Pakistani relations followed.[74] Building cooperation and trust between Pakistan and NATO/ISAF is undeniably crucial if Taliban sanctuaries and cross-border incursions into Afghanistan are to be effectively denied.[75] Stealth technology, however, can tempt COIN commanders to rely on unilateral cross-border military operations against a transnational insurgency instead of laboriously building trust with regional COIN partners.[76] Finally, the utility of stealth technology to the constabulary aspects of COIN are highly limited. Indeed, stealth technology aims to enhance concealment of a specific military unit/force – particularly an air force – from enemy radar during an offensive operation.[77] In the “hold” and “build” side of COIN, however, COIN forces must provide a widespread and visible presence amongst the populace to facilitate their security; since insurgents “swim” in the “sea” of the people, however, these COIN forces must necessarily be observable to the insurgent as well as to the civilian.[78]

Various RMA technologies have had differentiated effects upon both the political and military operations in COIN, although the RMA generally seems to have enhanced the strength of the insurgent. In particular, the RMA, with its emphasis on rapid and long-range precision strikes, force protection and surgical destruction has typically reinforced traditional US strategic thinking which favours tailoring forces for conventional inter-state warfare rather than protracted COIN operations. Additionally, many ICT innovations underpinning the RMA “system of systems” (e.g. the internet) have filtered down into society. This proliferation of technology has generally favoured the insurgent, who are able to broadcast their message to a wider audience, both at home and abroad, particularly through the internet and the international media. Consequently, ICT advances have presented insurgents with more potential sources of recruits, supplies, finances and political support. Moreover, the proliferation of ICT has exacerbated the liabilities of COIN practitioners. In particular, COIN practitioners are increasingly bound to the truth (since facts are more readily accessible), and failures/errors are significantly more noticeable to civilians through the international media.

The RMA has, however, bestowed COIN forces with some advantages in their military operations against insurgents. ICT technologies can be used to track and target the locations of insurgents (particularly leaders), who can then be apprehended/eliminated with special forces. Moreover, the RMA has indeed bolstered COIN with superior battle space knowledge when identifying and “clearing” an AO of insurgent positions, although insurgents can still “deceive” current technologies (e.g. through dummy defensive positions). However, airborne reconnaissance technologies have limited use in the “build” and “hold” phase in an AO. Moreover, precision-strike technologies (e.g. Hellfire-armed UAVs) are often ineffective in completely dislodging insurgent defences, and moreover frequently undermine the crucial objectives of COIN by causing collateral damage.

In conclusion, therefore, whilst the RMA has generally favoured the COIN practitioner with regards to military operations, in the more crucial political operations for “hearts and minds” the RMA has generally favoured the insurgent.

Bibliography


The “Revolution in Military Affairs” and Counter-Insurgency
Written by Philip Stibbe


The “Revolution in Military Affairs” and Counter-Insurgency
Written by Philip Stibbe


The “Revolution in Military Affairs” and Counter-Insurgency
Written by Philip Stibbe

No. 3, pp. 408-427.


[17] McChrystal (2009), pp. 5-6  
[18] Ibid., p. 1.  
[34] Ibid.  
[38] Ibid.  
The “Revolution in Military Affairs” and Counter-Insurgency

Written by Philip Stibbe

[43] Ibid.
[56] Ibid., p. 137.
[65] Ibid.
[71] Ibid.
[72] Ibid.

Written by: Philip Stibbe
Written for: Kings College London
Written at: Professor Anatol Lieven
Date written: April 2012