**Networked Power: Insurgents versus "Big Army"**

Hekmat Karzai & Paul T. Mitchell[*]

27 January 2006

Just as Microsoft with its Windows operating system dominates the computer industry, new operational concepts emerging from the United States over the past decade are coming to shape how other militaries pursue their objectives in the field. The most important of these new "operating system" concepts is that of Network Centric Warfare (NCW). However, while most modern militaries are busy attempting to implement variations on this idea, it is actually insurgents and terrorists that are likely to be the most successful in realising the promise of NCW. While US forces sometimes style themselves as "knowledge warriors", the 18th Century roots of today's military establishments will undermine their hopes for military "transformation": terrorists and insurgents are the real 21st Century organisations.

**Network Centric Warfare and Military Power**

Concepts of NCW began to emerge from the writings of Alvin and Heidi Toffler who have predicted the economic shifts to knowledge industries since their early publications. In the mid-1990s, US Department of Defense analysts began analysing corporations such as Walmart to determine how they were using information to enhance the speed of business operations and make them more efficient. By flattening management hierarchies and placing information about consumers and product choices on line with supplier inventories, stores were able to enhance their turnover of product in ways that centralised inventory control was unable to anticipate. Product purchasing became linked directly to localised sales figures, minimising inefficiency and inventory costs.

These concepts were redeveloped into a military context in the hope of eliminating the traditional fog of battle. The hope was that by freeing up information, especially in terms of intelligence and planning details, operational commanders would be able to use their forces more efficiently, increasing the speed and manoeuvrability of their forces in ways the enemy would find difficult to respond. This in turn would permit smaller forces to deal with more numerous opponents as a side benefit. The outcome of the conflict in Afghanistan and the initial outcome of the Iraq war seemed to suggest that the US was in fact on the verge of creating a "transparent" battlefield where commanders possessed a "God's eye view" of everything, permitting immediate control of all operations.

The current imbroglio in Iraq has failed to curb this enthusiasm. However, aside from the difficulties of US forces to control events in the streets of Karbala in the fashion anticipated by the theorists of NCW, there are solid reasons why NCW is unlikely to generate a transparent battlefield. Information on the Internet flows seamlessly amongst users. Type a

question into Google and it consults its list of more than eight billion pages and sends the most likely answer. Such searches, however desirable, are simply not feasible in a military context. Military information concerns life and death and matters of national security. As such, information is constrained in many ways. Its flow is hindered by rank levels (corporals see different information than generals), by military occupation, by classification and by service. Air Forces pursue operations differently than armies and frequently regard their service compatriots as bigger competition than their putative enemies. As the 9/11 Commission uncovered, inter-service cooperation within bureaucratic organisations is frequently oxymoronic.

## Insurgents and Information

Information flows far more efficiently in terrorist organisations. Terrorism is above all a means of communication, a highly dramatic way of sending a message. The new information revolution has empowered terrorists to disseminate their own message in their own particular means, completely bypassing traditional established media outlets. Even before Al Qaeda was established, its future leadership knew the valuable role of the media. Abdullah Azzam, the ideologue of Al Qaeda, and Osama Bin Laden established Maktab al-Khidmat (Service Bureau or MAK) to disseminate propaganda, raise funds and recruited new members through a network of offices in 35 countries (including thirty in the US cities). Under Azzam's leadership, MAK was responsible for producing the most comprehensive 11 volume 'Encyclopedia of Jihad' that has become the standard manual for the average Jihadist and can be found all over the Internet for training. Hence, there is no need or reason to travel to places like Afghanistan, Bosnia or Iraq. A future terrorist has the luxury of downloading any manuals from anywhere to train him and his future cell members.

The structure of terrorist and insurgent groups facilitate this transfer of information amongst themselves. Lacking the traditional bureaucracy of modern militaries, information flows rapidly and efficiently between participating subunits. Indeed, Al Qaeda's organisation has gone virtual as many of their former activities are conducted solely on line: spreading propaganda, recruiting new Jihadist, fundraising, indoctrination and psychological warfare. They even have the ability to produce and disseminate their own professionally produced and mass marketed CD-Roms and DVDs.

Al Qaeda's shift is a clear and natural progression as the Internet provides easy access, little or no regulation, censorship, or other forms of government control, potentially huge audiences spread throughout the world, anonymity of communication, fast flow of information, inexpensive development and maintenances of a web presence, a multimedia environment (the ability to combine text, songs, books, posters, and so forth), and the ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source of stories.

## Anarchy and the Internet

Ultimately, the power of the Internet lies in its anarchical nature. As such, information is persistent – difficult to remove once posted, transportable – easily moved from place to place, and universal – everything is shared with everyone, everywhere. Hierarchically flat, informal groups are best positioned to take advantage of these characteristics, unlike the highly organised, highly centralised, highly rationalised organisations like the military. Not only can flat informal organisations access information more effectively, they can use it faster as

well. The military talks about operating inside an enemy's decision cycle, but nothing illustrates this tendency better than the rapid dissemination and growing sophistication of how insurgents are using and adapting improvised explosive devices in Iraq and Afghanistan.

Ultimately, networking and using networked information requires 21st century organisational principles. Modern militaries came of age in the 18th century under the demands imposed by industrial culture. Discipline and standardisation were required to survive the Napoleonic battlefields of mass fire and movement. Adaptation and flexibility will be required on the modern (complex) battlefields of urban conflicts in tribal cities. Can militaries adapt to this style of conflict?

Special Forces seem to be leading the way, but only if they can rise above the challenges presented by the traditional military hierarchy. Insurgents and terrorists are still unlikely to win battles against their traditional opponents, given the disparity of resources militaries can deploy against them. As in all guerilla wars, the solutions will require military persistence and political acumen. Until then, networks will guarantee terrorists and insurgents a place on the battlefield, rather than ensuring their demise.

---

* Hekmat Karzai is a Research Fellow specialising in Afghan politics and modern terrorism and Paul T. Mitchell is a Visiting Senior Fellow with the Revolution in Military Affairs Programme at the Institute of Defence and Strategic Studies.