RSIS COMMENTARIES (49/2007)

RSIS Commentaries are intended to provide timely and, where appropriate, policy relevant background and analysis of contemporary developments. The views of the authors are their own and do not represent the official position of the S.Rajaratnam School of International Studies, NTU.

The Digital Divide: Networks, Armies and Coalitions

Paul T. Mitchell[*]

30 May 2007

AFTER DESERT Storm in 1991, militaries and academics alike speculated that we were experiencing a revolution in military affairs (RMA). The lessons of Desert Storm were reinforced by Special Forces operations in Afghanistan and the spectacular campaign of 2003 resulting in the overthrow of Saddam Hussein after a rapid drive up the Tigris valley and the dramatic entrance of American armoured forces in the streets of Baghdad. As impressive as these victories were, they concealed real challenges in the development of information technologies (IT) within military formations, especially land forces. In many respects, the challenge of using information for military effect is a "bridge too far" for armies. When the problems of coalition operations are added to an already complex agenda, IT will create more barriers than synergies.

The Strategic Value of Information

So far, IT has had its greatest military impacts in the air and at sea. Network Centric Warfare's (NCW) practical origin can be found in World War II with the Battle of Britain's coordinated fighter operations and the development of aircraft carrier operations in the Pacific. Each developed the use of information to precisely position scarce military assets to achieve decisive tactical effects. It is no accident that information was first used for decisive military effect in the air and at sea as each "environment" is relatively simple, devoid of terrain offering places to hide. Using a variety of sensors, targets can generally be easily found. As such, air forces, and navies (especially the latter) lead developments in the tactical use of IT.

Still, land forces seemed to have made considerable progress in the 1990s. The Cold War challenge posed by the Soviet Union's massed tank armies was, to a degree, the same World War II problem of directing scarce military assets to precise areas where enemy forces could be eliminated before they had the chance to attack. Cued by airborne assets like the Joint Surveillance Target Attack Radar System (JSTARS), air strikes, long range artillery, and rocket systems could attack masses of tanks long before they could themselves come into firing range. Such technology was used to great effect in the Gulf War and was supplemented by the Global Positioning System (GPS), which enabled armies to navigate in the desert.

Where GPS and JSTARS were the notable technology of 1991, a GPS related device, known as "Blue Force Tracker" (BFT) stood out in 2003. BFT automatically reported the GPS coordinates of every so equipped platform to a centralised database; this information was then projected onto BFT's digital map, thus allowing units to see both where they were as well as all their counterparts on the battlefield. Opposing forces could be loaded manually into the database, but for this reason, they did not move on the digital maps in the same way

S. Rajaratnam School of International Studies, NTU, South Spine, Block S4, Level B4, Nanyang Avenue, Singapore 639798. Tel. No. 67906982, Email: wwwidss@ntu.edu.sg, Website: www.idss.edu.sg.

as friendly forces did. Still, knowing where all friendly forces were was of critical importance in reducing fratricide. It enabled land forces to manoeuvre even during the midst of dust storms that had immobilised Iraqi units. And it allowed forces to disperse over huge distances and be kept supplied in a coordinated fashion. All of these features permitted the Americans to race to Baghdad using far less than the typical three to one force ratio attacking forces prefer to rely on for decisive advantage.

Still, land forces are a significant way from realising the power of information that their counterparts at sea and in the air have come to expect. In a word, the land environment is significantly more complex. Trees, hills, rocks, caves, and buildings hide and shield opposing forces. While a maritime commander may have to manage a significant amount of traffic transiting through a chokepoint (naval forces tracked over 6000 contacts in the Straits of Hormuz on a daily basis during operations in 2003), the number of moving targets that would need to be detected, characterised, and tracked by a company commander to generate the same level of situational awareness exceeds this number significantly (imagine the challenge posed by downtown Singapore).

Beyond environmental challenges, land forces differ from their air and sea counterparts in the very nature of their organisation. An army is composed of a great many small moving parts that need to be kept in rigid coordination. In contrast to a tank, a ship at sea is a relatively large platform, capable of generating significant amounts of its own power as well as supporting powerful sensors and communication devices. Even mobile land headquarters suffer from limited capabilities. The further one travels down the command chain, the greater the difficulties that are encountered in connecting units to the network stemming from lack of power, bandwidth, and connectivity. The individual soldier is the most challenged to tap into the sophisticated situational awareness provided by IT.

If these challenges weren't enough for land forces, additional ones come from coalition operations. Technical interoperability, the equivalent of getting your Apple computer software to run on a Windows system is a significant coalition problem. Technical standards established by alliances like NATO's "STANAGs" have helped somewhat, but the real challenge in connecting digital networks in coalition operations, however, stem from policy issues concerning information sharing. In Operations Enduring Freedom and Iraqi Freedom, information was tightly controlled by the United States. Information is filtered through a series of concentric circles of access within the coalition. Inside partners like the United Kingdom have much greater access to information than outer partners. Nor is this exclusive club simple to join. The current "Five Eyes" grouping of Australia, Canada, New Zealand, the United Kingdom, and the United States has a long history of intelligence cooperation that dates back to World War Two. In this type of environment, full multilateral sharing of information limits coalition networks to unclassified material. The variety of information release policies at play in coalitions usually spawns multiple networks further hampering the already complex technical affair of moving information from one network to another.

Satellite communications are necessary to provide sufficient bandwidth for the rapid transfer of data and communications between nodes. This is an expensive consideration: for effective operations; not only must these gateways be numerous, broad enough in terms of bandwidth, and capable of multiplexing, but they must also be leased channels if they are to be continuously monitored. Such requirements do not come cheaply, but neither will they be provided as a matter of course by any other coalition partner. SATCOM resources are scarce in every organisation and militaries will have to arrive with their own dedicated links.

The danger for land forces in general is a perverse and decreasing capacity to work together in this complex digital environment. In the past, differences in doctrine could be

accommodated by geographically separating armies so that they did not interfere with each other or inadvertently fire upon their partners. The high levels of situational awareness provided by digitized forces means that small forces can control larger and larger areas. The implication of this, however, is that there will be less and less room to place non or lesser digitized forces. This is especially true for small nations sending less than brigade sized units to operations dominated by large actors. While the IT revolution has stimulated an explosion of open communication and collaborative efforts in the business and social environments, its implication for armies may threaten just the reverse.

---

* *Paul T. Mitchell is an Associate Professor with the Revolution in Military Affairs (RMA) Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.*