RSIS COMMENTARIES (98/2007)



# 21st CENTURY WARFARE:Computers as the New Centre of Gravity

Bernard Fook Weng Loo*

24 September 2007

*Computer networks are becoming the single most important aspect of modern nation-states. Government services, military organisations, economic activities, all are increasingly dependent on computer networks. The recent spate of computer attacks and hackings might presage a new approach to warfare, where states target the increasingly important – and vulnerable – parts of modern nation-states, namely the computer networks that virtually all aspects of national life depend fundamentally upon.*

**IN 2007, TWO** events have defined the changing face of warfare more than all the displays of precision weaponry on CNN and BBC since the 1991 Iraq war. The first was the Russian computer attacks against Estonian computer networks in May. The second was the Chinese computer attacks, this time hacking into American networks.

The public face of the Revolution in Military Affairs – the RMA for short – has always been the iconic image of so-called 'smart' weapons hitting their targets with pinpoint accuracy. This public face masked what is the more important aspect of the RMA, which is the ever-increasing importance of computing and networking technologies in all aspects of military activities. However, muddled strategic thinking is preventing a proper appreciation of the prospects – and the problems – of the central role of these technologies in the RMA.

## Understanding the Centre of Gravity

This muddled strategic thinking revolves around the centre of gravity, which was one of the most important concepts that the great German philosopher of war, Carl von Clausewitz, had proposed in his classic *Vom Kriege* (*On War*).

Unfortunately, Clausewitz himself was not entirely clear as to what precisely this concept – the centre of gravity – meant. As a consequence, this lack of clarity results in the debates within strategic communities as to what it actually means, and what it refers to. Basically there are two ways by which we can think of this concept – either as a critical vulnerability, or as a source of strength and stability. The problem with this debate over the concept is that it fails to see a third way – that the centre of gravity is both a source of strength and stability as well as a critical vulnerability.

**Computer Networks as Centre of Gravity**

It is when we think of the centre of gravity as this potentially self-contradictory concept – as strength and vulnerability – that the centrality of computers and networks in the RMA becomes clear. Everything about this RMA depends fundamentally on computing and networking technologies. It is computing technologies that underpins the various aspects of the RMA. These include increased battlespace awareness through the employment of multiple arrays of different sensor technologies to gain a pervasive ability to monitor any and every aspect of the battlespace; precision guidance technologies that give weapons systems increasing lethality and renders the battlespace an increasingly dangerous environment to be in. Both aspects of the RMA create this situation for the opponent: to survive in the battlespace, the opponent needs to be both concealed and covered; any movement on his part will reveal his position to battlespace sensors, which will then result in the projection of very precise firepower onto his position, and almost guarantee his destruction and death.

Secondly, it is networking technologies that allow for this battlespace awareness to be communicated throughout the organisation. More importantly, these allow for the joining of the different services – land, air and naval forces – into a cohesive whole whose power is greater than the sum of its individual parts. Networking allows for jointness in the military, and networked jointness promises force multiplier effects to unprecedented degrees. There used to be a clear divide between all three component forces – there were areas that were beyond the ability of naval, air or land forces to attack and destroy. Networked jointness allows *any* weapons platform to attack and destroy emerging enemy positions. Whereas in the past, it was quite common for an enemy position to become known, only to remain intact for lack of sufficient land or air force components to attack and destroy this position.

The end result is a picture where the modern military organisation undergoing the RMA comes to depend fundamentally on both technologies. If either technology is rendered inoperable, for even a short period, it can bring what is a highly complex organisation to a grinding halt. In so doing, it can render what is otherwise a highly lethal organisation strategically irrelevant. For any military organisation, the quality of its weapons systems is strategically meaningless if these weapons systems cannot be deployed for whatever reasons against the enemy where and when it matters the most.

**Understanding Computer Attacks**

It is in this light that the recent spate of computer attacks mentioned earlier ought to be regarded by RMA proponents and military planners as a source of potentially great concern. Computer hacking has traditionally been seen in terms of espionage – of seeking to gain access to otherwise classified information that might prove crucial to one's own strategic efforts. This aspect has not gone away. It is entirely likely that the recent spate of Chinese hackings into various national networks was espionage, for the purposes of gathering information. This is a source of concern, although one should not overreact, since espionage is an unavoidable fact of international life. Basically *all* states conduct espionage activities against each other.

What is the greater concern about these recent computer attacks is that it might presage a new approach to waging war. Given the centrality of computers and networks, the most powerful military organisation in the world can be rendered strategically impotent if its computer networks are shut down even for a few hours by a computer attack. It is generally well known, for instance, that the entire eastern seaboard of the USA can be shut down for several hours by a concerted attack against the key handful of nodes in the computer networks that control the power grids of that part of the country. The consequences of such a shutdown – economic, political and military – are only dimly comprehended. The worst case scenario is this: a concerted computer attack shuts down the nation's early warning and monitoring facilities, rendering the military blind. Such a computer attack is then followed by a devastating military attack against the most important military assets, rendering the state now defenceless. The opponent then imposes its demands on the state, and in this blind and

defenceless position, the state has no choice but to surrender.

**Ponder the Improbable**

This is a hypothetical scenario, something that probably remains within the realms of moviedom imagination. The point is this – we once considered the prospect of airplanes being deliberately flown into buildings to be the realm of pure fiction. This is no longer the case. Which means that the responsibility of policy makers and strategic planners is to ponder the improbable. However improbable it may seem, computer attacks may become the new way of warfare; it is something that all policy makers and strategic planners need to seriously consider.

---

[*] *Bernard Fook Weng Loo is an Assistant Professor with the Institute of Defence and Strategic Studies at the Rajaratnam School of International Studies, Nanyang Technological University. He specialises in war and strategic studies.*