

Information in Warfare from Sun Tzu to the “War on Terror”

Robert Addinall

PhD Student

War Studies Programme, Royal Military College of Canada

Robert Addinall’s interests in history, political science and strategic studies first developed at a young age. As an undergraduate he focused on a number of areas, including modern nationalism, international relations, late classical and early medieval history, political philosophy, and military history and history of technology from all periods. He graduated with high distinction in 2000 from the University of Toronto with a B.A. specialist degree in History and a minor in English. His M.A. thesis, also written at U of T, discussed the impact of intelligence and deception operations by both the Red Army and the Wehrmacht on the course of the campaigns on the eastern front in World War II. He has worked in both start-up information technology (IT) companies and in an IT marketing and consulting firm. He began the PhD program at the Royal Military College of Canada in the fall of 2002, with a focus on war and technology and how media development and public perception has affected contemporary warfare.

Abstract:

During the 1990s use of the term “information warfare” surged and then waned as the concepts of “information operations” and “strategic information warfare” replaced it. The emergence of the term can be tied at least partially to the mid to late 1990s concept of the “information revolution” and the related “new economy”. By the beginning of the next decade the terms “cyberwar” and “netwar” had also emerged. Throughout this period the meaning of the term information warfare and its follow-ons remained ambiguous. Although some commentators tended to treat these ideas as fundamentally new phenomena, others noted that the concept of an information component in warfare was in fact as old as war itself. In light of the attacks on the United States of September 11, 2001, interest in information operations as components of asymmetric warfare and intelligence systems increased. However, within this context some have challenged the importance of intelligence in military affairs not only at present but throughout history. Given the confusion and varying opinions surrounding the role of information in warfare, an examination of this idea in a long-term perspective appears opportune in the year 2004. This paper will examine the historical relationship of three main factors as together forming information warfare: intelligence, and what I will call ideological defence and ideological offense. There are at least two other major information components in warfare: reconnaissance and situational awareness. Both concepts blend into intelligence at their edges. However, both are simply a matter of tactical competency at their basic levels. It is when they are used in conjunction with intelligence that they become an important factor in information warfare at an operational or strategic level.

During the 1990s use of the term “information warfare” surged and then waned as the concepts of “information operations” and “strategic information warfare” replaced it.¹ The emergence of the term can be tied at least partially to the mid to late 1990s concept of the “information revolution” and the related “new economy”. By the beginning of the next decade the additional terms “cyberwar” and “netwar” had also emerged.² Throughout this period the meaning of the term information warfare and its follow-ons remained ambiguous. Although some commentators tended to treat these ideas as fundamentally new phenomena, others noted that the concept of an information component in warfare was in fact as old as war itself.³ In light of the attacks on the United States of September 11, 2001, interest in information operations as components of asymmetric warfare and intelligence systems increased. However, within this context some have challenged the importance of intelligence in military affairs not only at present but throughout history.⁴ Given the confusion and varying opinions surrounding the role of information in warfare, an examination of this idea in a long-term perspective appears opportune in 2004.

This paper will examine the historical relationship of three main factors as together forming information warfare: intelligence, and what I will call ideological defence and ideological offense. There are at least two other major information components in warfare: reconnaissance and situational awareness. Both concepts blend into intelligence at their edges. However, both are simply a matter of tactical competency at their basic levels. It is when they are used in conjunction with intelligence that they become an important factor in information warfare at an operational or strategic level. To understand these distinctions it is logical to start with the arguments of one of the first military philosophers, Sun Tzu.

As Samuel B. Griffith has illustrated, the strategy and tactics described by Sun Tzu are based on the use of deception, adaptability and speed.⁵ Under this philosophy the enemy’s communications are a primary target. Sun Tzu speaks of tactical reconnaissance, observation, flank patrolling, and probing attacks as important in battle and on the march,⁶ but he also notes that moral strength and intellectual prowess are decisive in long-term strategy. By breaking up alliances, turning enemy leaders against one another, sowing subversion and causing demoralization, a state can at times be destroyed without an open battle between armies.⁷ Sun Tzu also argues that true victories can only be won by a state in which the people are united behind the government, free from oppression.⁸ Griffith points out that with these arguments, Sun Tzu is one of the first thinkers to appreciate the difference between what in the twentieth century would be called “national strategy” and “military strategy”.⁹

The points noted by Griffith appear readily in the original text.¹⁰ Sun Tzu states that there are five fundamental factors in warfare: moral influence, weather, terrain, command, and doctrine.¹¹ “By moral influence”, he writes, “I mean that which causes the people to be in harmony with their leaders, so that they will accompany them in life and unto death without fear of mortal peril.”¹² In addition to the above factors, he adds that “all warfare is based on deception”.¹³ He lays out the principles of deception: “when capable, feign incapacity; when active, inactivity... When near, make it appear that you are far away, when far away, that you are near... Offer the enemy bait to lure him; feign disorder and strike him... Pretend inferiority and encourage his arrogance.”¹⁴ In terms of offensive strategy, he writes that “to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill. Thus, what is of supreme importance in war is to attack the enemy’s strategy... Next best is to disrupt his alliances... The next best is to attack his army.”¹⁵ The above actions are effective

both tactically and strategically. During engagements between armies, knowledge of terrain combined with deception can lure enemy forces into encirclement and disintegration, while strategically one state can cause another to mistake its situation and launch a war from a position of weakness.

The connecting factor in all these elements, as can be discerned from the statements quoted above, is information. A military commander has to know the details of the terrain around a potential battlefield before it can be used to advantage; the general must also know his own troops, their abilities, and their loyalty before he can use them effectively. These tasks are made easier if the condition of the enemy - in training, doctrine, morale, and leadership - is known, while at the same time the commander must attempt to deny such knowledge of his own force to the enemy. To a government which seeks to undermine its opponent through other means than the clash of arms, understanding the government and society of an opposing state, and its points of weakness, is even more important. Gathering of information, situational awareness, denial of information, and spreading of disinformation are thus all present in Sun Tzu's model of warfare.

Sun Tzu is also clear about how to control information through means which have typically come to be called "intelligence" and "espionage" in the centuries since he wrote The Art of War. "Now the reason the enlightened prince and the wise general conquer the enemy whenever they move and their achievements surpass those of ordinary men is foreknowledge"¹⁶, he writes. Foreknowledge can only "be obtained from men who know the enemy situation"¹⁷, and such men come in five types. The first are "native agents" – "those of the enemy's country people whom we employ" – they can provide information concerning terrain, troop movements, military and civilian morale, and also spread dissent.¹⁸ Secondly there are "inside agents" – enemy officials who relay state secrets.¹⁹ Third are "doubled agents" – enemy spies who are found out and turned, who can still receive information from their former masters and who can also send disinformation back up the enemy chain of command.²⁰ Double agents are, in Sun Tzu's opinion, also useful for recruiting native and inside agents.²¹ Fourth are "expendable agents" – spies sent into enemy territory with deliberately fabricated information, who will be captured and give up their untruths when interrogated.²² Finally there are "living agents" – those with the skill to enter enemy territory, gain access to information, and return alive.²³

In Sun Tzu's description of warfare, then, both tactical and strategic information is important – with strategic information often focusing on enemy morale and ways to damage it. Information offence and defence are both present, as are intelligence operations as a means to facilitate them. However, Sun Tzu's term moral influence is too vague to be definitively construed as ideology – to clarify the role of ideological offence and ideological defence in information operations, we can move forward in time to a European philosopher of the Enlightenment, Niccolo Machiavelli.

Much analysis in political philosophy suggests that Machiavelli's aim in The Prince is to deflate both classical and Christian concepts of morality and virtue through an examination of the nature of society and warfare.²⁴ This examination concludes that human nature is essentially self-serving, and therefore "the effective motives on which a statesman must rely are egoistic, such as the desire for security in the masses and the desire for power in rulers."²⁵ By comparing Machiavelli's comments in The Prince with the republican ideals he expresses in The Discourses, University of Chicago professor Leo Strauss²⁶ and his students, some of whom are now professors at other universities,²⁷ develop a number of arguments – one of which is that Machiavelli is advocating the importance of ideas as fundamental to the creation and destruction

of societies. To develop this approach The Prince can be divided into three broad layers of interpretation.

At the most superficial layer, which may be called amoral manipulation, Machiavelli is destroying the moral interpretation of virtue for no other reason than to sell his services to Florence's ruler, Lorenzo. This layer is, however, little more than a cover for the deeper meanings written into the book – a cover to prevent Machiavelli from being accused of treachery by Lorenzo or heresy by the Church. In the second layer, Machiavelli deals with the nature of society and the military, suggesting that “good arms and good laws” must be found together. An army must be made up of willing citizens. Thus the only way to have a healthy army is to have a healthy society. Machiavelli writes:

... it now remains for me to discuss in general the various ways in which... principalities can organize themselves for attack or defence. We said above that a prince must build on sound foundations; otherwise he is bound to come to grief. The main foundations of every state, new states as well as ancient or composite ones, are good laws and good arms; and because you cannot have good laws without good arms, and where there are good arms, good laws inevitably follow, I shall not discuss laws but give my attention to arms.²⁸

He also writes that:

A prince, therefore, must have no other object or thought, not acquire skill in anything, except war, its organization, and its discipline. The art of war is all that is expected of a ruler; and it is so useful that besides enabling hereditary princes to maintain their role it frequently enables ordinary citizens to become rulers.²⁹

Thus a leader must always think of war, but in order to be successful at it he must build on a foundation of good laws. Machiavelli makes his point more striking by stating it subtly: the nature of society and the nature of military activity are inextricably linked. Machiavelli avoids discussion of what he means by “good laws” in The Prince, but in The Discourses he makes his republican ideals clear. Given these ideals, Machiavelli's good laws will resemble the laws of the Roman Republic, the essence of which were maintained under many of the Emperors even after the end of the Republic. Such laws make the entire populace politically involved, and if they are involved politically, they will be willing to fight and die for political ends. The Prince cannot be a mere tyrant to achieve this: “Yet it cannot be called prowess to kill fellow-citizens, to betray friends, to be treacherous, pitiless, merciless.”³⁰ Instead he must be a true leader, able to understand and inspire his people:

But if it is a prince who builds his power on the people, one who can command and is a man of courage, who does not fail to take precautions, and who wins general allegiance by his personal qualities and the institutions he establishes, he will never be let down by the people; and he will be found to have established his power securely.³¹

In this context, the concluding chapter of The Prince, the “exhortation to liberate Italy from the barbarians”, makes sense as something more than an incongruous call to proto-nationalism in a manual for tyrants. It follows Machiavelli's logic that the “good laws” of the Roman Republic must be resurrected by the re-emergence of a united Italian peninsula under a leader motivated by this abstract ideal, not merely by the desire for power. He is suggesting that warfare is ideological and psychological.³²

The third layer at which The Prince can be interpreted develops the ideas of the second in a way which is directly applicable to information warfare. Although Machiavelli expresses a

superficial disdain for “unarmed” prophets, he argues that “But to come to those who became princes by their own abilities and not by good fortune, I say that the most outstanding are Moses, Cyrus, Romulus, Theseus, and others like them.”³³ Each of these leaders created a “new mode and order”.³⁴ Yet all these leaders were religious prophets at least as much as military or political leaders, and would thus seem to fall into the category of being “unarmed”. The key is that all these leaders have used religious ideas to change or eliminate older forms of society and to entrench their own. Towards the end of The Prince, in his discussion of taming and controlling fortune and his veiled suggestion to create a new republic in Italy, Machiavelli is suggesting that secular, republican ideals of citizenship can undermine and destroy the strength of the previous religious ideas. His message is therefore that ideas are the most powerful weapons of all; weapons which can animate and control the minds of people as no simple tyranny can.³⁵

Not only the crises of the Florentine republic, but the religious wars throughout Europe of the 16th and 17th centuries, which drove other political philosophers such as Thomas Hobbes and John Locke to produce their own theories of the nature of society, illustrate the growing importance of ideology in warfare in Machiavelli’s time and after. In these conflicts war was not fought just over rivalries between kings and lords, but because beliefs were seen as dangerous. Although the treaty of Westphalia put an end to much of the religious conflict, by providing a basis for the modern nation-state it also provided a new vessel for ideology to develop in.

A great deal has been written on the role of ideology and nationalism in the modern age,³⁶ but to develop the argument concerning information warfare in this paper it is necessary to move ahead in time again – to analysis of British and American counter-insurgency campaigns in the mid-twentieth century. In these campaigns many of the factors discussed by both Sun Tzu and Machiavelli can be seen at work. Conventional military forces which had developed doctrine for the mass engagements of early twentieth century “total war” had two main problems dealing with guerrilla or asymmetric warfare. The first of these was that conventional organizations have difficulty translating what has been called “background” information into usable operational and tactical intelligence which would allow them to achieve advantageous contact with their opponents. The second is that military organizations tend to target something which looks at least vaguely like themselves – another military organization, even if it is hiding in a camp somewhere in a forest – thus missing the clandestine support networks in the population that regenerate military forces which are destroyed by conventional means.

Writing in the mid-1960s, Robert Thompson described well the typical pattern of insurgencies – most of which described themselves as Communist – during that time. Thompson himself took part in the British anti-insurgency campaign in Malaya from 1948 to 1960, and was head of the British Advisory Mission to Vietnam from 1961 to 1965, and has been referred to as one of “the two great practical theorists of counterinsurgency”.³⁷ In his description, initial insurgent attacks are designed not only to capture war materiel, but to disrupt communications and thus throw the government off balance, panic the population and dislocate the economy.³⁸ These moves have strategic ends which are both military and political: “The political aim is to gain control over the population, starting in the rural areas, and to destroy the government’s prestige and authority. The military aim is to neutralize the government’s armed forces...”³⁹ Thompson provides a chart detailing three components in an insurgent force: component A consists of guerrilla or terrorist cells and their supporters in the population; component B constitutes local armed guerrilla units

at platoon and company strength; and component C is made up of regular units at company and battalion strength.⁴⁰ Thompson describes how these components function together:

(The insurgent) political organization within the population at A is responsible, with the help of the armed military units at B and C outside the population, for expanding... control over the population... The political organization at A is also responsible for providing... the armed units at B and C with food, other supplies, recruits and intelligence. Thus traffic runs from A to B and thence to C... By expanding A and gaining control over larger areas and more population, the flow of supplies and recruits to the armed units steadily increases. In this way, such units can then be built up gradually from platoon to company and even battalion strength...⁴¹

Military commanders brought in by a government faced with this situation are:

...inclined to regard the local and regular units at B and C as their main objective because militarily they present the only attractive targets. The net result is that large-scale military operations based on very meagre intelligence are mounted to seek out and destroy these units. Guerrilla units are designed to cope with exactly this form of government reaction. To start with, they are seldom concentrated (except for an action on their own initiative), and are scattered over wide areas of... inaccessible terrain. Even if, as a matter of luck, the government forces make contact, the action is immediately broken off by the guerillas. In the very rare case when a unit is surrounded and caught in the open and suffers heavy casualties as a result, no permanent damage is inflicted. As soon as the government forces withdraw, the whole organization goes to work, and within a short period... the losses have been made good. For example, let us suppose that a regular company at C suffers fifty casualties; these are immediately replaced by promotions from the local units in the neighbourhood at B, and these in turn are reinforced by new recruits from the population, provided by the organization at A. The restoration of strength is not lost on the local population, and any confidence which such a victory might have restored in the government soon begins to wane.

The situation will develop into one in which the insurgents first gain control over the population and villages in the remoter valleys and on the fringes of jungle and swamp. Such areas are selected for reason of their inaccessibility to government forces, and are rendered more inaccessible by the cutting of any access roads and the blowing up of bridges... As soon as such areas are fully under insurgent control, and the political organization has extended its operations into the next stretch of populated territory, it becomes possible for the district platoon to move into the controlled area, where they can live in comparative safety and give the necessary support to the advancing political organization.⁴²

The above pattern is, of course, a generalization. Nonetheless, it illustrates the importance of the use of intelligence and ideology, as well as the frequent absence of front lines and the need for military forces to be able to operate in small, highly mobile groups in mid-twentieth century warfare. The process by which Western military forces began to adapt to such opponents is partially described by Frank Kitson, who took part in counter-insurgency campaigns in Kenya, Malaya, Muscat, Oman and Cyprus as an infantry officer (at times tasked to intelligence sections) in the British army.

Kitson's first experiences in counter-insurgency were in Kenya, where he learned that background information can be turned into usable operational and tactical intelligence, but that

the process by which to do this is not always obvious to the twentieth-century western military mind. As head of intelligence for a number of districts near Nairobi in the early to mid 1950s, his organization gathered a large amount of what he describes as “background” intelligence, such as lists of Mau Mau gang members, details of weapons possessed by the insurgents, and gang policies and long-term plans.⁴³ However, the problems of using this type of intelligence in a conventional mid-twentieth century army is explained by Kitson:

Units expected whatever intelligence organization existed to provide pinpoint information regarding the whereabouts and future intentions of enemy groups so that soldiers could be put into contact with them. The intelligence organizations were seldom capable of doing this regularly, so the army did two things. Firstly it complained about the inefficiency of the intelligence organization and secondly it set about conducting large-scale operations in likely areas on a hit-or-miss basis. Because its staff procedures were effective it was well suited to exploiting such success as it may have had when carrying out random searches for the enemy. For example, if a patrol bumped into a gang the army could concentrate large numbers in the area quickly. But if it was unlucky with its random operations nothing happened... In other words we, in the Special Branch, thought that the... (background information) which we got from our interrogations and contacts would be of great value, but military commanders expressed little interest in such material...⁴⁴

In Kenya Kitson learned to use this background information to manipulate captured gang members as well as to create “pseudo-gangs” made up of local Kikuyu and others loyal to the government. The background intelligence gave these pseudo-gangs enough knowledge of Mau Mau behaviour to appear believable as Mau Mau themselves. Such pseudo-gangs could leverage knowledge of typical Mau Mau contacts in the community to make direct contact with actual groups of terrorists, and then learn their exact short-term dispositions.⁴⁵ Later in the 1950s, commanding infantry forces in Malaya, he used background information – such as personalities of terrorists, locations of their relatives, locations of likely food supplies – to determine the areas in which Communist forces were most likely to be operating. He would then use his own troops, sending them on patrols in relatively small groups and with tactics and equipment adapted to the conditions of jungle warfare, to narrow the field further:

...whereas in Kenya we had used ex-enemy to trick their former supporters into supplying more information, in Malaya we had used our own soldiers to get it by sending out patrols looking for confirmation of our theories... Based on these thoughts, I formulated the theory for operating against terrorists which I have worked on and taught ever since. Briefly, it can be stated this way. Firstly, if the tactical aim is to destroy a group of terrorists operating from some form of cover, then the main problem will be to discover who they are and where they are, so that they can be neutralized. As a commander cannot be given sufficiently detailed information to do this, he must get it for himself because the responsibility for achieving a tactical aim must be that of the commander of the force concerned. In practice he can do this by a chain-reaction process, in which information and deduction lead to action designed to get more information. At some stage in the chain the chance of bringing about a contact arises and if a contact results, then further information automatically becomes available.⁴⁶

The 1950s also saw a revival of “special forces” type organizations in the armed forces of Western states. During the Second World War Britain and the United States had made extensive

use of intelligence and special forces which did not operate by conventional principles, such as the Special Air Service (SAS) and the Office of Strategic Services (OSS). However, most of these organizations were disbanded along with the rest of the Anglo-American wartime armed forces after 1945.⁴⁷ Although France possessed special forces troops in the early 1950s, they were heavily committed in Indochina. In the late 1940s Britain and the U.S. partially revived their intelligence organizations in the forms of the Secret Intelligence Service (SIS) and the Central Intelligence Agency (CIA), which operated primarily against Soviet influence in eastern Europe, the Baltic States and the Balkans. With the beginning of the Malayan Emergency in 1948 and the Korean War in 1952, specialist hunter-killer and intelligence-gathering units were recreated on an ad hoc basis. Following these developments the British re-formed the SAS for operations in Malaya, while the U.S. raised the 10th Special Forces Group (Airborne), elements of which took part in the later stages of the Korean war.⁴⁸

Commenting on the role of the SAS in the Malayan Emergency, Harclerode notes the way in which its role differed from that of regular infantry – even where those infantry adapt to the conditions of non-conventional warfare as Kitson’s troops did:

During the campaign, total CT (Communist Terrorist) casualties totalled 6,398 killed and 1,245 captured, while 1,938 surrendered themselves to the security forces. Of those killed, 108 died at the hands of 22 SAS. While this may seem a very small proportion of the total... a large proportion of those making up that figure were leading terrorists, and their deaths were thus severe blows... Furthermore, the emphasis during a large part of the regiment’s operations was on intelligence gathering, and on the crucial task of winning the hearts and minds of the aborigines, rather than on seeking direct confrontations with the terrorists.⁴⁹

Other aspects of the British campaign in Malaya extended beyond standard military measures. The British observed that the Communists derived most of their support from the largely ethnically Chinese population which lived on the fringes of the jungle, and so they resettled half a million people in new villages – thus depriving the terrorists of a local population to blend into. They also created “liberated” areas where they were psychologically and militarily in control, reversing the typical insurgent approach to gaining control of territory described by Thompson above. They worked politically to establish a stable, multi-ethnic national political party in Malaya which would have the confidence of the country’s population. Nonetheless, an insurgent force which amounted to little over 6000 troops at any one time tied down 300 000 Commonwealth troops for a number of years before it was defeated.⁵⁰

Under these conditions, while at the Camberley Staff College in the mid-1950s, Kitson wrote a fictional critique of conventional twentieth century Western military thought. It is worth quoting in entirety here, since it foreshadowed the arguments of advocates of the “Revolution in Military Affairs” and “Information Warfare” in the mid 1990s and “Transformation” in the early 21st century:

WORLD WAR III

World War III started shortly before the end of World War II. It was fought by both conventional forces and partisans.

The actions of the conventional forces were few and of comparatively little importance.

Even in World War II some people could see that where Communism was involved the action of guerrillas was already taking over to some extent.

Nations had practised partisan war for centuries but the Communists were probably the first people to teach it systematically as an integral part of operations. Certainly the Communists were the first to see that nuclear weapons made the old sort of war impractical and that in the future the best way to wreck their opponents was by a mixture of people's uprisings and economic chicanery. They kept their armies as a threat and as a weapon with which to finish off the work of their partisans when no risk attached to their employment.

The leaders of the West were slower to understand. For many years bemused and bemedalled parties of the hydrogen hierarchy were talking petulantly about private armies. Their natural reluctance to grasp anything new was accentuated by their ability to see that promotion prospects were at best uncertain in a partisan force. Furthermore the whole idea was a little vulgar.

And so for many years the peoples of a hundred tribes fought in hate at the bidding of the Communists' leaders, knowing neither why, nor for whom, they struggled. In the first decade of World War III (1945-1955) the Communists succeeded in actuating partisans in North Africa, East Africa, Indo-China and Malaya, to mention only a few places. In each case the Western Powers countered with conventional forces which were totally unsuited to the task. They called it the 'Cold War' (though they found it so hot in Indo-China that they baled out). A few people realized that it was not the Cold War but the war. A terrific battle raged in the Western camp while these people tried to persuade their countrymen that information was the key to fighting modern war. (Even the elementary difference between intelligence and reconnaissance was unknown at that time.) The Old Guard stamped on the upstarts in a frenzy and ground many of them into paste.

Eventually daylight dawned. What started in 1945 as a collection of odds and ends known as Special Forces, developed into the main offensive and defensive weapon of the Western World. The West was in a position to turn the Communist weapon of popular uprising against its inventor, in the same way that the Communists had turned the tables on the West with nuclear missiles many years before.

CAMBERLEY
1 October 2056

With these comments in mind we can move ahead in time again, to the military literature of the late twentieth and early twenty-first centuries. The main catch-phrase in the 1990s was "revolution in military affairs", and many official pronouncements concerning it were taken almost verbatim from the definition produced by the Office of Net Assessment, US Department of Defense. This definition states that an RMA is "a major change in the nature of warfare brought about by the innovative application of technologies which, combined with dramatic changes in military doctrine, and organizational concepts, alters the character and conduct of operations."⁵¹ In his paper "The Revolution in Military Affairs: A Canadian Perspective", Major J. Craig Stone of the Canadian Forces Command and Staff College also examines the theoretical writing on the RMA, finding that:

The notion of information dominance and the information age is tied to the ability to process information faster and to have situational awareness on the battlefield. It is considered by many as one of the defining characteristics of RMA... Military innovation is generally discussed in the context of types of innovation-peacetime versus wartime, technological versus doctrinal and evolutionary versus revolutionary.⁵²

Stone also discusses the views of Ralph Peters (retired U.S. Army Colonel and author of works concerning grand strategy) and James Stavridis of the U.S. Navy:

Stavridis argues that we are in the first revolution of the information age and the second revolution (the system of systems) is around the corner. Peters argues that the RMA is over and the new paradigm already exists. He argues that true revolutions occur in the minds of men. From that perspective he advocates that the popularity of the subject and the amount of discussion on the subject are irrefutable arguments that the revolutionary activity is over.⁵³

Williamson Murray, Professor Emeritus at Ohio State University, makes the distinction that, at their first appearance, linked technological and doctrinal changes amount to no more than “military revolutions” with a tactical or operational advantage. It is only in the longer-term process, he argues, in which societal, political and organizational changes are linked to the tactical and technological developments that a new “conceptual approach” to war is born. The change in conceptual approach, which can render a once-powerful organization irrelevant is the true RMA. Murray states that the question today is whether improvements in information exchange are creating revolutionary new capabilities for military forces.⁵⁴ Murray’s discussion of conceptual changes provides an important link between the RMA and the concept of Information Warfare, as well as the broader question of whether societies will continue to organize themselves as nation-states in the future.

Other analysts of Information Warfare join Murray in the belief that the impact of Information Technology (IT) is reorganizing entire societies in a revolutionary manner, eliminating the traditional nation-state. Seen in this light, the RMA appears as only one part of the Information Revolution affecting all of society. However, the implications of the broader strategic context do not stop there. Canadian military historian Ronald Haycock has noted that the Information Revolution technologies appeared alongside other major changes in the world’s political and economic structure. These included increased globalization, especially in economic activity, as well as a proliferation of non-governmental organizations. Such events were compounded by the loss of a superficially bi-polar world in which states knew who the enemy was supposed to be and what type of conflict their armed forces were likely to have to fight.⁵⁵

In terms of this broader discussion, John Arquilla and David Ronfeldt, who have worked with RAND and the U.S. Office of the Assistant Secretary of Defense while developing their ideas, are significant in introducing the ideas of “Cyberwar” and “Netwar”. In *Athena’s Camp*, they describe Cyberwar, which can be considered a form of information warfare for conflict between conventional forces. It focuses on the concept that a modern military must blind its opponent in order to win. This approach differs from earlier warfare concepts in that blinding of the enemy by disrupting his communications is supposed to be immediate, rather than achieved by first penetrating the front line and then manoeuvring to disrupt his command and control systems. Arquilla and Ronfeldt assume that the military forces of modern states are already so reliant on technology that disruption of their technologically advanced C4ISR (Command, Control,

Communications, Computing, Intelligence, Surveillance, Reconnaissance) systems will render them blind and incapable of operating in any meaningful sense.⁵⁶

In Networks and Netwars, Arquilla and Ronfeldt discuss their approach to information warfare for low-intensity conflict and asymmetric warfare conditions, which they term “Netwar”. They argue that the emergence of networked communications capabilities will bring with it a change in the organizational mindset of many rogue organizations. Computers allow people to form geographically dispersed groups which discuss and develop ideas often without a central hierarchical command. Such groups may form on the Internet and continue to use it as a prime medium of communication, but they will also transfer this type of organization to the “real world”. Such “cell”-type organizations have existed to some extent in the past (the IRA is one example), but with the “Internetted” mindset they will proliferate. Such groups will be difficult to deal with, since it is usually not possible to eliminate them by terminating a leader or leadership. However, “network” warfare can also be used to advantage:

Some bad actors (e.g., terrorist and criminal groups) may threaten U.S. and other nations’ interests, but other actors (e.g., NGO activists in Burma or Mexico) may not – indeed, some actors who at times turn to netwar strategies and tactics, such as the New York-based Committee to Protect Journalists (CPI), may have salutary liberalizing effects. Some actors may aim at destruction, but more may aim mainly at disruption and disorientation.⁵⁷

Thus the Internet may become a battleground for, among other things, hearts-and-minds campaigns. However, it is not clear where the dividing line between policing and military action may run. The tendency in some of the literature is to treat Information Warfare and Netwar as one type of asymmetric threat for new types of policing forces to deal with, while regular military forces will focus more on fighting more tangible asymmetric threats, such as use of Weapons of Mass Destruction (WMD) by terrorists. However, speedy intelligence sharing through new technologies is a capability discussed extensively in RMA, Information Warfare and Transformation literatures. All approaches suggest that information gathered by one agency or branch of the military will, if relevant, quickly find its way into the decision-making cycles of other military commands and civilian policing agencies, perhaps through an organization responsible for information security.⁵⁸

Michael Erbschloe, an IT consultant, develops a number of these ideas in his book Information Warfare. He points out that the proliferation of information-age technology which enables the RMA has also levelled the playing field between not only small and large powers but between states, criminal and terrorist organizations, and private individuals.⁵⁹ He believes that because of the globalized economy, established states lack major incentives to attack their trading partners, but terrorists, criminals and perhaps rogue states have nothing to lose and so might do so.⁶⁰ Even if military forces adequately protect their own IT systems, they are still susceptible to attack via civilian IT systems, since they rely in part on such activities as financial accounts moving around through the networked IT systems of the financial world. Wipe out accounts, and everything from soldiers’ pay to procurement projects are thrown into disarray. In the future, Erbschloe argues, it could be difficult for a state to discern whether only private corporations or the state itself is under attack, and such confusion could lead to long delays in military response time.⁶¹ In these types of threats a blurring of the traditional borders of the Westphalian state system can be clearly seen.

Is it possible to visualize what concrete implications these discussions have for forces on a real battlefield? Descriptions often provide plenty of technical terms:

New military technologies associated with the RMA include precision-guided munitions for precision force, stealth for greater power projection, advanced intelligence, surveillance and reconnaissance (ISR) systems for enhanced battle-space awareness, and advanced command, control, communications and computing (C4) systems for increased battle-space control.⁶²

These new technologies are supposed to require shifts in the doctrines of all the services of a typical Western military force. Joint doctrine is often treated as a new idea, although arguments for “combined arms operations” have been around since the 19th century, and joint air/naval/ground operations, coordinating their actions based on highly effective signals intelligence (ULTRA), were used in World War II operations such as the Normandy campaign by Allied Forces. Nonetheless, there is to be an enhanced emphasis on army units being in constant communication with air force and navy forces, sharing intelligence and targeting information.

The force structure implied above would mean that army units could be much lighter, and able to deploy and manoeuvre more quickly, because instead of having to transport heavy firepower with them, they would be able to call it in from air and navy units. It is because of this logic that heavy weapons systems like main battle tanks are often described as outdated – the defensive armour of such a vehicle should be unnecessary because opponents would be destroyed by weapons fired from a “stand-off” distance, before one’s own forces move close enough to be within range of anti-armour weapons such as rocket-propelled grenades (RPGs). Naval forces would have to move towards littoral rather than “blue water” doctrine, in order to provide direct assistance to land forces with cruise missiles launched from warships and submarines, as well as air strikes and transportation launched from aircraft carriers. Air forces would provide cover for both ground and sea elements, and also collect intelligence. All of this would be facilitated by massive increases in information bandwidth provided by satellites (which would also be collecting intelligence) and Unmanned Aerial Vehicles (UAVs) which would relay this information between units in what is sometimes called the “battlecube”. Stealth vehicles would also play an increased role in both air and naval power, as would unmanned combat aerial vehicles (UCAVs).

However, one might still be inclined to ask what does all this really mean? Up to the end of the 1990s, the picture was, as often admitted, cloudy.⁶³ The 1991 Gulf War and the 1999 operations in Kosovo were the main examples of extensive use of the developing technology, but it was difficult to use either instance as solid proof of concept for the new approaches, since in both cases RMA or Transformation approaches were exerted in the main through air power.

In the case of Iraq in 1991, the coalition forces used limited numbers of precision bombs - about 10% of those dropped by a number of accounts⁶⁴ - many of which needed to be laser-guided either by ground troops or by the aircraft that fired them. However, the ground assault was launched with heavy armoured forces which had only two or three years earlier still been preparing for massive armoured engagements on the north European plain. Although Iraqi forces were numerically large, they were poorly equipped and much of their heavy equipment, such as Soviet T-64 and T-72 series tanks, had inferior range to the U.S. M1A1-Abrams main battle tanks deployed. Also, many Iraqi soldiers were conscripts with little desire to fight, and large numbers surrendered at the earliest opportunity. In Kosovo and Serbia in 1999, a number

of factors came together to determine the downfall of Slobodan Milosevic. While significant internal opposition to his rule existed, Russia withdrew support for Serbia at about the same time as the NATO bombing campaign began. Then during late May and June of that year, the Kosovo Liberation Army launched ground offensives that forced Serbian units to concentrate in counterattack and defensive positions. Significantly, 80 percent of the armoured vehicles lost by the Serbian forces were destroyed during those last two and a half weeks when by concentration they had become easy targets. NATO warplanes using laser-guided ordnance were also hampered by bad weather in the Kosovo operation.⁶⁵

Responding to these drawbacks, Martin Van Creveld argues that the armies of the present and the states that maintain them could not survive the true upcoming “transformation of war”. In his 1991 book The Transformation of War, he begins with the observation that in low intensity conflict, guerrilla forces have almost always triumphed over sophisticated military forces since World War II, with the most notable exception being the British defeat of the Communist insurrection in Malaysia. His analysis of why this is so concludes that since World War II non-uniformed fighters have been steadily gaining legitimacy as “freedom fighters”. By contrast, during the period of the dominance of European empires over the world, the “Clausewitzian” concept that guerrilla-style resistance was illegitimate, immoral and beyond the rules of warfare was common. At the same time, Van Creveld argues that technological progress has reduced the delta between cheap and small and expensive and large weapons; while a modern jet fighter is more advanced than a World War II fighter, it can be shot down with a shoulder-mounted rocket launcher. By comparison, a flak gun that was expensive, difficult to transport and difficult to conceal was required to shoot down World War II aircraft. Guerrilla armies were the first to learn that they could use such weapons to defeat organized forces, but organized crime and other such entities are quickly learning that they can operate by intermingling with local populations and thus remain virtually undetectable and difficult to confront with modern military forces.

Van Creveld’s argument is far-reaching if one assumes that Western armies intend to use modern technology only to produce more expensive weapons such as Stealth planes:

Often the pilots and crews... cannot see their opponents. Instead, targets are detected by radar and appear as blips on fluorescent screens. They are acquired, tracked and engaged with the aid of technical, read “electronic”, instruments. Thus, modern aircraft, helicopters, ships, tanks, antitank weapons, artillery, and missiles of every kind are all becoming dependent on electronics to the point where this dependence is itself the best possible index of their modernity. They work fairly well in simple media such as air, sea, even open plains and deserts. However, the more complicated the surroundings the greater the problems. Many sensors can distinguish friend from foe only if the target cooperates by sending out an agreed-on signal... the computers that process the information sent by the sensors can only respond to such eventualities as were explicitly foreseen by their programmers. Often the net effect of complex environments is to cause the wrong signals to be picked up and sent out, either sounding false alarms or none at all. What is more, once the principles on which these gadgets operate are understood they are easy to spoof, overload, or jam. Often all that is needed is a similar gadget, modified to do the opposite job.⁶⁶

Therefore,

The visions of long-range, computerized, high-tech warfare so dear to the military-industrial complex will never come to pass. Armed conflict will be waged by men on

earth, not robots in space... Weapons will become less, rather than more, sophisticated... War will not take place in the open field, if only because in many places around the world there no longer is an open field. Its normal mise en scene will be complex environments, either those provided by nature or else the even more complex ones created by man. It will be a war of listening devices and of car-bombs, of men killing each other at close quarters, and of women using their purses to carry explosives and the drugs to pay for them.⁶⁷

The military conventions of those who do not have advanced technology will default to the possible, and the rules of “civilized” warfare will have to follow. This default to the possible is the flip side of the new threats created by information warfare, (as discussed in relation to the work of Arquilla, Ronfeldt and Erbschloe above). Others echo some of Van Creveld’s concerns. Sloan states that there are good reasons to proceed along the RMA path with caution; like Van Creveld she notes that it is difficult for computerized systems to recognize weapons and troops carried in trucks, hiding in buildings or interspersed among civilians, and WMDs buried underground. Optical and infrared sensors cannot see through bad weather or many types of solid objects. Excessive focus on advanced technologies could breed technocratic thinking that does not place enough emphasis on other requirements for winning wars (doctrine, morale, etc.). Such emphasis can also blind one to the emergence of radically different forms of warfare and create a sense of complacency. As a result, promises of short, decisive wars won by precision weapons could lead to crisis if a longer engagement turns out to be necessary.⁶⁸ Others in the mid to late 1990s, such as the American Institute for National Strategic Studies and a number of senior US military officials concluded that technologies associated with the RMA are narrowly focused on high-end warfare and are not applicable to peacekeeping, urban warfare, or asymmetric threats.⁶⁹

Although Sloan echoes some of Van Creveld’s criticisms, she also discusses technological innovations which can overcome them. For instance, she notes that precision guided munitions (PGMs) using the Global Positioning System (GPS) are not impeded by poor weather conditions, since they do not need to “see” where they are going with either on-board video systems or laser guidance from aircraft or ground forces. Such PGMs proved their value during the Kosovo campaign.⁷⁰ Doctrines for jointness and the use of littoral forces are also useful for operations other than war, since they can make “light” peacekeeping forces seem more intimidating to an enemy. Improved intelligence-gathering and -sharing, as well as situational awareness capabilities, allow commanders a better sense of where clandestine activities are taking place and how to deal with them.

Of all the recent theorists, Caleb Carr provides the best counterargument to Van Creveld. He states that the airpower required by the United States today must include guaranteed genuine precision. Some developments are obvious, he argues, such as confining high-altitude bombing to precision weapons which can be fired from a safe distance from enemy ground fire (the “stand-off” distance) and then guided to their targets by coordinates inputted by troops on the ground. Exceptions to this rule are vehicles like the AC-130 which can work well in tactical roles with troops, as “flying artillery”. However, UAVs and UCAVs provide for the greatest improvements in these areas. Vehicles such as the Predator drone, a long-endurance, medium-altitude UAV used extensively in the Afghanistan and 2003 Gulf War campaigns were originally intended for reconnaissance and surveillance, but can now also be fitted with munition payloads. Such modifications will make it a “modern army’s answer to suicide bombers” since it is

“remote-controlled and thus governed by human intelligence rather than strictly by a computer, as is the case with cruise missiles.”⁷¹ He goes on to point out that: “It is also highly effective against the kind of tactical, handheld weapons that terrorists use heavily, such as shoulder-launched missiles, because it is pilotless and its loss involves no casualties.”⁷² He argues that such a weapon is analogous to the relatively simple American mass-produced medium tanks of World War II – a decisive weapon which can be produced in quantity and replaced easily when lost.⁷³

In addition to UCAVs, weapons systems which were originally designed for strategic operations in the Cold War can effectively find new roles in LIC situations. For instance, Stealth Fighter and Stealth Bomber technology began development in the 1970s. The original mission of the B-2 Stealth Bomber was to go unnoticed by Soviet radar and thus penetrate deep into Soviet airspace where it would have first-strike capability at such targets as Soviet nuclear missile silos. However, a B-2 firing a GPS precision-guided munition at stand-off distance is likely to be able to avoid any of the smaller, cheaper weapons that Van Creveld believes can be used to destroy technically complex systems, while its great range also allows it to respond quickly to points around the world, without any requirement for vulnerable forward bases.⁷⁴ In the long run such platforms may be replaced by cheaper, long-range UCAVs, but the point is that adaptability is available with current technology provided that doctrinal changes can be carried out.

Neither are automated systems mere futuristic dreams. As noted from the comments of the theorists mentioned above, dynamism in the civilian sector has come to be seen as a primary driving force for new military capabilities. This is often explained in terms of Common-Off-the-Shelf-Technology, or COTS. COTS technology is that which is commoditized and widely available, such as many types of microelectronics (CPUs, circuit boards, high-resolution digital cameras, and so on, which are typically incorporated in personal computers, digital cameras, optical drives and so on today). Many of the computer systems needed to pilot a UAV such as the Predator drone can be acquired this way. Had the U.S. military attempted to design all the systems required for a Predator in the 1970s, it would likely have been highly expensive, but by waiting until “cheap-off-the-shelf” (COTS) technology was available it is able to integrate a much less expensive system. Thus, continued advances in technology allow the complexity and expense of advanced systems to shrink, even as weapons systems that can be used against them do so.⁷⁵ Thus established states can turn the reduced delta between cheap and small and expensive and large weapons to their advantage, since they can mass-produce cheaper systems like UCAVs which are more expendable than complex, manned systems.

However, some ground forces are necessary in almost any conflict. Only ground forces can occupy territory – but in some cases this role can be fulfilled by a local ally (sometimes called a “proxy”), as it was by the Northern Alliance in Afghanistan in 2001. In such cases Western ground forces will be small while being capable of directing the maximum possible firepower. Special operations forces (SOF) are key in this role, a situation which is summed up succinctly in this comment:

In Afghanistan, these forces were central. They could be parachuted into the country in small numbers, set up airfields, and develop contacts with rebel leaders. The information about Taliban targets, which the Predator drones transmitted back to headquarters, usually came from a special-ops officer riding on horseback with a laptop.⁷⁶

“Usually” is a question of context; as soon as regular troops reached the ground, they normally called in many of the strikes. Nonetheless, SOF operating together with indigenous allies can command respectable firepower while moving much like LIC forces themselves. Modern information technology also allows geographically dispersed forces to be more aware of where they are in relation to each other, and along with fire support and resupply from the air, enables them to move about in “swarms” rather than along traditional fronts. Such forces are not invulnerable – against a determined enemy, SOF troops could be ambushed or simply overwhelmed, and large numbers of UCAVs shot down. However, by applying new concepts in the way described above, a modern military force has a good fighting chance against LIC, where Van Creveld suggests its predecessors would do poorly.⁷⁷

Arquilla and Ronfeldt have called this type of warfare “swarming”, and described it as “engaging an adversary from all directions simultaneously, either with fire or in force.”⁷⁸ They have also placed it within a historical context:

Examples of swarming can be found throughout history, but it is only now able to emerge as a doctrine in its own right. That is largely because swarming depends on a devolution of power to small units and a capacity to interconnect those units that has only recently become feasible, due to the information revolution.⁷⁹

This point concerning historical context is applicable to most of the uses of information in warfare. Considering the different periods of warfare discussed in this paper, it can be seen that modern technology has increased the tempo of operations and multiplied the specific types of information which need to be obtained. However, from Sun Tzu to Machiavelli and on to mid-twentieth century British and American counter-insurgency theorists, it can be seen that the need exists not only for effective tactical intelligence, but also for control of the flow of information and how it is interpreted at the level of entire societies. Some wars could be fought successfully by mass – despite the importance of Allied intelligence and SOF operations in the Second World War, the industrial output of the United States was probably the single most important factor in winning that conflict. Nonetheless, even in that case Allied forces cut the war short and minimized losses through the use of ULTRA and other intelligence operations. There are, however, those who make an opposing argument.

In his recently published work on the role of intelligence in warfare John Keegan identifies a complex of ideas related to intelligence and traces the evolution of these ideas over time. He argues that intelligence can be divided into the strategic, dealing with the geography, political and technological features of an opponent and the regions it operates in, and operational, dealing with the strength, deployments and movements of enemy forces in theatre.⁸⁰ In addition, Keegan notes that intelligence and subversion operations have become interlinked in the English-speaking world. He traces this development from Britain’s use of local allies to extend and police many parts of the Empire during the 18th to 20th centuries, through the operations of the Special Operations Executive against the Axis in World War II, to the creation of joint intelligence gathering and subversion organizations post-war such as the CIA.⁸¹ During the Second World War and the Cold War, signals and electronic intelligence gained predominance over human intelligence. However, he also believes that intelligence has been of secondary influence in war.

He argues that “having admitted the significance of the pre-vision intelligence provides, it still has to be recognised that opposed enemies, if they really seek battle, will succeed in finding each other and that, when they do, it will rarely be intelligence factors that determine the

outcome”.⁸² Elsewhere he states that “foreknowledge is no protection against disaster. Even real-time intelligence is never real enough. Only force finally counts.”⁸³ In the era before electronic communications, he argues, operational intelligence, limited by the speed of the horse or of the runner, could usually not be delivered in time to be of use. Moving into the modern period, he finds that:

...the organisation of intelligence-gathering and subversion within the same body is undesirable. Subversion is a weak way of fighting, differing from conventional warfare by the total unpredictability of its results; moreover, in a democracy, it is always liable to disavowal by legitimate authority and denunciation by authority’s political opponents.⁸⁴

Despite making the above arguments, Keegan states that Western operations against asymmetric threats in the future will likely be very similar to, and overlap with, police work.⁸⁵ He also notes that modern terrorist organizations use techniques pioneered by early Western SOF forces such as the SOE.⁸⁶ He posits that in the “War on Terror” humint will regain predominance, since systems such as satellite imagery cannot provide reliable detailed tactical information. However, he still argues that in this period intelligence can only “sharpen the gaze” of Western soldiers, the “ability to strike sure” remaining the primary factor in battle.⁸⁷

Part of Keegan’s point is somewhat disingenuous; the will to fight and the ability to field an effective force is an obvious prerequisite for a state to engage in conflict. Keegan considers other points which work against his argument as well. He notes continuity in British SOF operations from World War II to the anti-insurgency campaigns in Malaya and elsewhere. Combined with the extensive British tradition of using local allies, such an approach – he believes – historically helped the British to build effective strategic intelligence from humint by forces that were also operating as fighting units in the field. However, he apparently evades the point that combination of humint, sigint and elint in real-time on the battlefield can better enable Western forces against asymmetric and terrorist threats. More importantly, while recognizing that intelligence and subversion operations have become linked, he does not discuss counter-subversion in this equation. The importance of developing alliances and humint networks through hearts-and-minds-campaigns, as well as preventing the ideological disaffection of one’s own population, is central when considering these three factors together, and has been understood by military theorists from the earliest times. Machiavelli’s injunction that only those leaders who develop “secure foundations” - ideological, not just physical ones - are truly safe in warfare is testament to this. Keegan also does not address the flip side of Western antipathy to using subversion against others – a constantly growing dislike for civilian casualties on any side. If a Western leader in war is able to win a local population over to his (or her) side, and thereby demonstrate to his (or her) own population that what he is doing is in the locals’ interests, he is more likely to be able to continue operations successfully. The alternative is that not only a population in theatre, but also his own population at home, will turn against the government – as happened to the American leadership in the Vietnam conflict.

In conclusion, we should not convince ourselves that information warfare is new. However, modern technology, both directly through its influence on armies and indirectly through its influence on public opinion through telecommunications-driven media, is causing the impact of the information element of warfare to grow significantly. The effects of the use of information in war in the past need to be thoroughly understood to gain some sense of the shape an ever more prominent role will take in the future.

NOTES

¹ See, for instance, Roger C. Molander et al. “What is Strategic Information Warfare?” What is Strategic Information Warfare? Santa Monica: Rand, 1998, p. 3.

² See the section on “Strategic Information Warfare and Defense” on the website “The RMA debate” to gain a sense of the use of these terms in the late 1990s and early 2000s: <http://www.comw.org/rma/fulltext/stratinfo.html>

³ See Molander, op.cit., p. 4.

⁴ The most significant of these is military historian John Keegan’s Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda. Toronto: Key Porter Books, 2003.

⁵ Samuel B. Griffith’s introductory essay in Sun Tzu, The Art of War. London: Oxford University Press, first printing 1963, first paperback printing 1971, p. 8.

⁶ See *ibid.*, pp. 35-38.

⁷ *Ibid.*, p. 39.

⁸ *Ibid.*, p. 39.

⁹ *Ibid.*, p. 40.

¹⁰ Albeit the text quoted from here is an English translation of the original Chinese.

¹¹ Sun Tzu, The Art of War. London: Oxford University Press, first printing 1963, first paperback printing 1971, p. 63.

¹² *Ibid.*, p. 64.

¹³ *Ibid.*, p. 66.

¹⁴ *Ibid.*, pp. 66-67.

¹⁵ *Ibid.*, pp. 77-78.

¹⁶ *Ibid.*, p. 144.

¹⁷ *Ibid.*, p. 145.

¹⁸ *Ibid.*, p. 145. ¹⁸ See, for instance, Roger C. Molander et al. “What is Strategic Information Warfare?” What is Strategic Information Warfare? Santa Monica: Rand, 1998, p. 3.

¹⁸ See the section on “Strategic Information Warfare and Defense” on the website “The RMA debate” to gain a sense of the use of these terms in the late 1990s and early 2000s: <http://www.comw.org/rma/fulltext/stratinfo.html>

¹⁸ See Molander, op.cit., p. 4.

¹⁸ The most significant of these is military historian John Keegan’s Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda. Toronto: Key Porter Books, 2003.

¹⁸ Samuel B. Griffith’s introductory essay in Sun Tzu, The Art of War. London: Oxford University Press, first printing 1963, first paperback printing 1971, p. 8.

¹⁸ See *ibid.*, pp. 35-38.

¹⁸ *Ibid.*, p. 39.

¹⁸ *Ibid.*, p. 39.

¹⁸ *Ibid.*, p. 40.

¹⁸ Albeit the text quoted from here is an English translation of the original Chinese.

¹⁸ Sun Tzu, The Art of War. London: Oxford University Press, first printing 1963, first paperback printing 1971, p. 63.

¹⁸ *Ibid.*, p. 64.

¹⁸ *Ibid.*, p. 66.

¹⁸ *Ibid.*, pp. 66-67.

¹⁸ *Ibid.*, pp. 77-78.

¹⁸ *Ibid.*, p. 144.

¹⁸ *Ibid.*, p. 145.

¹⁹ *Ibid.*, p. 145.

²⁰ *Ibid.*, p. 146.

²¹ *Ibid.*, p. 148.

²² *Ibid.*, p. 146.

²³ *Ibid.*, p. 146.

-
- ²⁴ See, for instance, Quentin Skinner, Machiavelli: A Very Short Introduction. Oxford: Oxford University Press; Anthony Grafton in his introductory essay to the 1999 Penguin edition of The Prince; and Giuseppe Prezzolini, Machiavelli. New York: Farrar, Straus & Giroux, 1967.
- ²⁵ George H. Sabine, A History of Political Theory. New York: Henry Holt and Company, 1958.
- ²⁶ See Leo Strauss, Thoughts on Machiavelli. Glencoe, Illinois: The Free Press, 1958.
- ²⁷ Such as Clifford Orwin and Thomas Pangle of the University of Toronto political science department.
- ²⁸ Niccolo Machiavelli, trans. George Bull, The Prince. London: Penguin Books, p. 39.
- ²⁹ *Ibid.*, p. 47.
- ³⁰ *Ibid.*, p. 28.
- ³¹ *Ibid.*, pp. 33-34.
- ³² This combination of war, ideology and psychology foreshadows the structures of modern think-tanks which include political scientists, psychologists, historians and military planners, among others.
- ³³ *Ibid.*, p. 18.
- ³⁴ This phrase is used by Orwin and Pangle.
- ³⁵ The discussion on Machiavelli here is partially based on the Straussian interpretation of Machiavelli's work as taught by Orwin and Pangle in 1998-99 at the University of Toronto, and is a condensed version of the argument presented in the author's paper "The Nature of Society and Warfare in Machiavelli's The Prince". For a more complete description of Machiavelli's aims, as well as the direct relevance of Machiavelli's work to the later concept of "total war", reference is made to that paper.
- ³⁶ Among the leading works are: Ernest Gellner, Nations and Nationalism. Ithaca: Cornell University Press, 1983; and: Philip Bobbit, The Shield of Achilles: War, Peace and the Course of History. New York: Anchor Books, 2003.
- ³⁷ The other is Edward Lansdale, according to: Jeet Heer, "Can Vietnam Tactics work in Iraq?", National Post, Saturday, January 10, 2004, pp. RB1-RB2.
- ³⁸ Robert Thompson, Defeating Communist Insurgency: Experiences from Malaya to Vietnam. London: Chatto & Windus, 1966, p. 29.
- ³⁹ *Ibid.*, p. 29.
- ⁴⁰ *Ibid.*, p. 30.
- ⁴¹ *Ibid.*, pp. 30-32.
- ⁴² *Ibid.*, pp. 30-32.
- ⁴³ Frank Kitson, Bunch of Five. Plymouth: Latimer Trend & Company Ltd., 1977, p. 29.
- ⁴⁴ *Ibid.*, p. 29.
- ⁴⁵ *Ibid.*, pp. 29-56.
- ⁴⁶ *Ibid.*, p. 150.
- ⁴⁷ See, for instance, Peter Harclerode, Fighting Dirty: The Inside Story of Covert Operations from Ho Chi Minh to Osama bin Laden. London: Cassell Military Paperbacks, 2001, p. ix.
- ⁴⁸ The above developments are summarized well in *ibid.*, p. xi, and discussed in detail throughout the book.
- ⁴⁹ *Ibid.*, p. 162.
- ⁵⁰ This summary is based on: John Man, "Jungle War: The Malayan Emergency", History of the Twentieth Century. Purnell, for B.P.C. Publishing Limited, London, England. Editor in Chief A.J.P. Taylor., no. 91., pp. 2539-2540.
- ⁵¹ Compare this definition to that in: Canadian Defence Beyond 2010. Accessed April 11, 2003: http://www.vcds.dnd.ca/dgsp/dda/rma/wayahead/intro_e.asp; and Elinor Sloan, "DCI: Responding to the US-led Revolution in Military Affairs". NATO Review, Web Edition, Vol. 48 - No. 1, Spring-Summer 2000, pp. 4-7.
- ⁵² Major J. Craig Stone, "The Revolution in Military Affairs: A Canadian Perspective". Conference of Defence Associations Institute: First Annual Graduate Student Symposium, 13-14 November, 1998.
- ⁵³ Stone, *op.cit.*, p. 3.
- ⁵⁴ Drawn partly from the overview concerning Murray's arguments in Elinor C. Sloan, The Revolution in Military Affairs. Montreal & Kingston: McGill-Queen's University Press, 2002, pp. 22-23. Also see: Williamson Murray, "Thinking about Revolutions in Military Affairs". Joint Forces Quarterly, summer 1997.
- ⁵⁵ Ronald Haycock, "The Labours of Athena and the Muses: Historical and Contemporary Aspects of Canadian Military Education", Canadian Military Journal, Vol. 2, No. 2. Kingston: Royal Military College of Canada, 2001. Printed by Canadian Forces Training Materiel Production Centre.; pp. 6-7.
- ⁵⁶ See John Arquilla; David Ronfeldt, In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica: RAND, 1997.

⁵⁷ John Arquilla; David Ronfeldt, Networks and Netwars. Santa Monica: RAND, 2001, pp. 6-7.

⁵⁸ See Sloan, The Revolution in Military Affairs, op.cit., pp. 108-122.

⁵⁹ “Before the Internet, information warfare was a war that would be fought among giants. The widespread use of the Internet and readily available access to the global communications systems and an arsenal of software tools has brought information warfare down to levels that all types of warfare eventually fall back to – once again, almost anyone can launch an information warfare attack.” Michael Erbschloe, Information Warfare. Berkeley: Osborne/McGraw-Hill, 2001, pp. xv-xx.

⁶⁰ Erbschloe could well be mistaken. In the years immediately before World War I, respected financial analysts, economists, and others repeatedly stated that major sustained conflict was impossible because the global financial system was so interlinked that, once war cut off trade between different countries, their economies would simply collapse. Yet Erbschloe is not alone in holding similar views today.

⁶¹ Erbschloe, op.cit., pp. 267-282.

⁶² Sloan, “DCI: Responding to the US-led Revolution in Military Affairs”, op.cit., p. 4.

⁶³ Both Sloan’s book and Stone’s paper make this point from time to time.

⁶⁴ See, for instance, Fred Kaplan, “Force Majeure: What Lies Behind the Military’s Victory in Iraq”.

Slate.msn.com, Tuesday April 15: <http://slate.msn.com/id/2081388>

⁶⁵ See Caleb Carr, The Lessons of Terror. New York; Toronto: Random House, 2003, pp. 248-252. See also Sloan, The Revolution in Military Affairs, op.cit., pp. 94-95.

⁶⁶ Van Creveld, op.cit., pp. 30-31.

⁶⁷ Van Creveld, op.cit., p. 212.

⁶⁸ Sloan, The Revolution in Military Affairs, op.cit., pp. 29-31.

⁶⁹ Richter, Andrew. “The Revolution in Military Affairs and its Impact on Canada: The Challenge and the Consequences”. Institute of International Relations – The University of British Columbia, Working Paper No. 28, March 1999, pp. 20-21.

⁷⁰ Sloan, op.cit., p. 94.

⁷¹ Carr, op.cit., pp. 252 - 255.

⁷² *Ibid.*, pp. 252 - 255.

⁷³ *Ibid.*, pp. 252 - 255. Since the late 1990s, popular paperbacks for military hobbyists have also starting delivering a message similar to that of Carr. David Alexander’s book Tomorrow’s Soldier is a good example, discussing how UAVs, UCAVs, and other air assets can cooperate with various types of ground forces to both hunt terrorists and guerillas and fight more conventional HIC battles against rogue states. Writers such as Alexander also pick up on both low-tech and high-tech asymmetric warfare threats such as those discussed by Van Creveld and Arquilla and Ronfeldt. Alexander glibly comments that this means that there will be no traditional front lines and that all citizens will be involved in the conflicts of the future. While being good sources for commentary on technological systems, such popular works by their nature have few real recommendations for future organization, education and training of troops. See: David Alexander, Tomorrow’s Soldier. New York: Avon Books, 1999.

⁷⁴ See Alexander, op.cit., pp. 127-137 for a good commentary on the B-2.

⁷⁵ For additional commentary on UAV operations, demonstrating their accomplishment of typical RMA objectives, see Matthew Brezinski, “The Unmanned Army”, New York Times, April 20, 2003.

⁷⁶ Fred Kaplan, op.cit. Similar comments are made by Ralph Peters, Beyond Terror. Mechanicsburg, PA: Stackpole Books, 2002, p. 13, and by many other sources.

⁷⁷ In addition, Van Creveld’s historical analysis of the failure of conventional forces to defeat LIC has been called into doubt: “...a diverse school of revisionists – including military analyst Lewis Sorley, former CIA director William Colby and maverick liberal journalist Michael Lind – has picked up on the idea that the Viet Cong were in fact defeated as a popular insurrection, although their North Vietnamese ally won a conventional war against exhausted South Vietnamese and American forces. ‘The U.S. military has defeated most guerrilla movements it has faced,’ argues Max Boot, author of Savage Wars of Peace (2002), which chronicles U.S. victories in ‘small wars’ against forces ranging from the American Indians (‘the best irregular warriors in the world’) to the first Sandinista movement in Nicaragua in the 1930s. Jeet Heer, op.cit., p. RB2.

⁷⁸ John Arquilla; David Ronfeldt, Swarming and the Future of Conflict. Santa Monica: RAND, p. vii.

⁷⁹ *Ibid.*, p. vii.

⁸⁰ Keegan, op.cit., p. 359.

⁸¹ See *ibid.*, pp. 389-399.

⁸² Ibid., p. 383.

⁸³ Ibid., p. 399.

⁸⁴ Ibid., p. 398.

⁸⁵ Ibid., p. 362.

⁸⁶ Ibid., p. 361.

⁸⁷ Ibid., p. 399.