CANADIAN FORCES COLLEGE /COLLÈGE DES FORCES CANADIENNES

ADVANCED MILITARY STUDIES COURSE 2

NOVEMBER 1999

# Asymmetrical Warfare: The Counterrevolution in Military Affairs

By/par Commander Thomas Francis Manning

# Asymmetrical Warfare: The Counterrevolution in Military Affairs

**by**

**By Commander Thomas F. Manning**

*"In the future, war will not be waged by armies but by groups whom we call terrorists, guerrillas, bandits, and robbers."*

*Martin Van Creveld - The Transformation of War*

## INTRODUCTION

With the end of the Cold War and the collapse of its accompanying bi-polar framework, the world is entering an era of uncertainty. The 21st century has seen wars fought for hegemony over territory and resources. However, as we enter the next century new threats to global security are emerging. Violence and warfare often accompany demands by minority populations for self-determination and calls for the end of repressive and corrupt regimes. Further, as the "information revolution" and the "global economy" continue to advance rapidly, they will be accompanied by periods of instability, as regional conflicts will increasingly endanger global security. Information will become one of the world's most important resources and the power of "virtual nations" and non-nation states such as large corporations is growing as knowledge rather than borders more and more defines power.[1]

In this new world order, militaries and security forces must be ready for an operational environment where rogue states and amorphous enemies without borders will present much greater danger than nation-state rivalry.[2] In its "Joint Vision 2010", the US military recognises that it must be prepared to face a wider range of threats, emerging unpredictably and challenging the nation at varying levels of intensity. Increasingly,

future conflicts will be asymmetrical, against an enemy consisting of insurgency groups, terrorist organisations, rogue nations, computer hackers, and drug cartels. Asymmetrical warfare is emerging as a counterrevolution to the ongoing "revolution in military affairs that is thought to have started with the Gulf War in 1991."[3] This development will have a significant impact on warfare in the 21st century especially at the operational level of war[a]. The traditional force-on-force operations, which produced results in the past, will be essentially ineffective against this new unconventional threat being executed by fanatics willing to commit suicide for their cause. Operational level commanders must be prepared to plan and conduct warfare on a new plane where there are few if any rules and ethics are based on the Machiavellian principle that "the ends justify the means."

**AIM**

This paper will explore briefly the changing threat to global security as the world enters the 21st century. In particular, it will argue that the technological superiority of Western nations, particularly the United States (US), is driving a counter-revolution in military affairs that will have a direct influence on warfare, especially at the operational level, in the next millennium.

**BACKGROUND**

Throughout history technology has affected the nature and course of warfare profoundly and continuously. The invention of the stirrup enabled mounted warriors to

[a]. The operational level can be defined as the gray area between strategic and tactics. Therefore, "if strategic is the art of war and tactics is the art of battle, then operations is the art of campaigning." (English, 7)

put all the force of the horse behind the spears that they had, up to this point, thrust with only the strength of their arm. The arrival of this technology in Western Europe in the eighth century soon led to the seizure of church lands and the establishment of feudalism among the Franks. Seven centuries later the longbow helped undermine feudalism, which eventually led to the destruction of the power of horse-owning aristocrats. In the twentieth century, developments in technology such as the invention of nuclear weapons have become revolutionary in their impact.[4] With the tremendous advances in computer technology that have taken place in the last quarter century, it is not surprising that the nature and conduct of warfare is undergoing a revolution that is established on and driven by technology. To the American military, especially the US Army, rapid advances in science and technology have ushered in nothing less than a Revolution in Military Affairs (RMA). "A survey of any of the current publications of the US Army supports this conclusion"[5], however, they do not agree on a precise definition of RMA. It would appear that the concept is subject to many interpretations.

Many military experts view it as a fundamental break with all previous methods of waging war, while others emphasise the evolutionary nature of RMA. They claim the origins of RMA stem from a number of separate improvements in intelligence and surveillance sensors, communications and the integration of complex software systems. For example, US Admiral William A. Owen, defines RMA as being essentially a "system of systems" whose main components are intelligence collection, surveillance and reconnaissance. This includes technologies and systems that provide command, control, communications and computer processing, and the integration of complex information systems in real time.[6] In a similar interpretation, the US Secretary of Defence's Office of

Net Assessment defines RMA as a "major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organisational concepts, fundamentally alter the character and conduct of military operations." [7]

While these experts may be generally correct when they assert that emerging information and computer capabilities are producing a RMA, it is something else entirely to assume that this revolution will inevitably favour today's developed nations. As an example of such thinking, a recent issue of *The Economist*, as well as an interesting new book by George and Meredith Friedman*, The Future of War: Power, Technology, and American World*, appear to conclude that this revolution will give the US and its allies a virtually insurmountable advantage in future conflicts. They suggest that this superiority in technology and modern weaponry means the US and its allies would be surprised, indeed shocked, if anyone took up arms against them, as long as the war focused on a conventional battle fought apart from civil society.[8] Thus many will argue that this overwhelming superiority will render major global conflicts obsolete. This assumes, however, that all future adversaries will have similar perspectives as the US and its western allies and will appreciate the importance of technology, would prefer to use brains rather then brawn and would not want to cause too much harm. Other researchers, such as Steven Metz, an associate research professor at the Strategic Studies Institute of the US Army War College, argues that global conflict will not become obsolete but simply that the tactics and the targets of our future adversaries will change. He contends that because the US and its western allies will be unbeatable on the traditional battlefield, the major trends of the next twenty-five years will be increasing heterogeneity among the

world's armed forces. Adversaries will seek structures and methods for their armed forces that are different from those of the technologically superior US and the West. Therefore, it is more likely that the threat of a major conventional global conflict will be replaced by something even more horrific - asymmetric warfare. This will be, according to Madeleine Albright, US Secretary of State, "the war of the future."[9]

**CHANGING NATURE OF CONFLICT**

"Asymmetric threat" is a new term used to describe the weapons and tactics that relatively weak enemies could use to foil or circumvent the technological supremacy of western nations.[10] Their aim is not to claim territory or to even threaten the sovereignty of their opponents. Their primary objective is to weaken their western adversary's resolve and ability to use their superior conventional military capability effectively to intervene in regional conflicts or to thwart the goals of rogue states or other subversive groups. Asymmetric threats embrace the full spectrum of disproportionate intimidation with which the West might be faced, from international civil disobedience and criminality right up to military low intensity conflicts. They range from computer warfare through to terrorism or rogue state nuclear blackmail, and includes the use of weapons of mass destruction as much as national destabilisation arising from mass migration.[11] Thus asymmetrical warfare in the 21st century will be rough and ready and probably completely unpredictable.

> As the second millennium A.D. is coming to an end, the state's attempt to monopolise violence in its own hands is faltering. Brought face to face with the threat of terrorism, the largest and mightiest empires that the world has ever known have suddenly begun falling into each other's arms. Should present trends continue, then the kind of war that is based on the division between

> government, army, and people (the trinity of von Clausewitz) seems to be on the way out. The rise of low-intensity conflict may, unless it can be quickly contained, end up destroying the state. Over the long run, the place of the state will be taken by war making organisations of a different type.

Martin van Creveld made this statement before the onset of the Gulf War, and the demise of the Soviet Union. However his predictions of an increase in low-intensity wars have proven to be correct. Civil wars have proliferated in such places as Afghanistan, Somalia, Bosnia, Sudan, Rwanda, Zaire, Sierra Leone, Angola, Northern Ireland, Kosovo, East Timor and many of the former Soviet Republics. In addition, there was a significant spread of serious terrorism as witnessed by such acts as the destruction of the US military compound in Saudia Arabia and the embassies in East Africa, the World Trade Centre bombing in New York, the Oklahoma City federal building bombing, the poison gas attach in Tokyo, the Basque separatist bombings in Spain, Arab actions in Israel, and many others on a lesser scale, including political assassinations. Hanging over the world as well is the even greater threat of proliferation of weapons of mass destruction and their use by terrorists and rogue states.[12] These so-called low-intensity threats will now be examined in more detail.

**Terrorism**

The literature defines terrorism as the sub-state application of violence or threatened violence intended to create disruption and destabilisation in a society, to undermine or even overthrow the official government of the state, and bring about changes in the political system. Terrorism may even on occasion be used as a substitute for war between states. It is definitely related to guerrilla warfare, although unlike

guerrillas, terrorists are unable or unwilling to take or hold territory. As we approach the 21st century most international and domestic terrorism is neither politically left or right, but ethnic-separatist in inspiration. Unlike ideologically motivated terrorists, ethnic terrorists can normally develop a much larger base of public support and thus normally have more staying power.[13] While this paper will primarily address political terrorism, encompassing both trans-national or sub-national adversaries including rogue and "streetfighter" state sponsored terrorism, it will occasionally draw comparsons to criminal terrorism which enpompasses outlaw syndicates and drug cartels.

The threat of terrorism is not new and in its long history it has appeared in many guises. As the world approached the end of the last century, it appeared that no one was safe from terrorist attack. In 1894 an Italian anarchist assassinated French President Sadi Carnot. In 1897 anarchists fatally stabbed Empress Elizabeth of Austria and killed Antonio Canovas, the Spanish Prime Minister. In 1900 Umberto I, the Italian king, fell in yet another anarchist attack; in 1901 an American anarchist killed William McKinley, President of the United States. Terrorism became a major preoccupation of everyone from politicians to police and security personnel.[14] In this respect things have not changed dramatically as we approach the end of this century as demonstrated by the high priority given to the terrorism issue by US President Bill Clinton and other western leaders at the June 1996 meeting of the Group of Seven. However, since 1900, terrorists' motivation, strategies and weapons have changed dramatically. Today, terrorists, whether international cults like Aum Shinrikyo or individuals like the Unabomber, act on a greater variety of motives than ever before. They also have access to weapons of mass destruction, including nuclear devices, germ dispensers, poison gas weapons, and even

computer viruses. One of the greatest changes in recent decades is that violence is by no means the terrorists' only strategy. "The many-branched Muslin Brotherhood, the Palestinian Hamas, the Irish Republican Army, the Kurdish extremists in Turkey and Iraq, the Tamil Tigers of Sri Lanka, the Basque Homeland and Liberty movement in Spain, and many other groups that have sprung up in this century have political as well as terrorist wings. The political arm provides social services and education, runs businesses, and contests elections, while the "military wing" engages in ambushes and assassinations."[15] This separation of the political wing from its military component permits the political leadership to disassociate itself from the acts of terrorism and continue to seek political resolution to the issue. As a result of this multileveled organisational structure it is often difficult for governments and militaries to develop strategies and plans to effectively address terrorist tactics, as illustrated in places such as Northern Ireland.

The tactics of terrorist organisations have also changed in recent years. There has been a shift away from attacking specific targets such as heads of state and politicians and toward more indiscriminate killing. The difference between urban and other tactics has become less distinct, while the line between politically motivated terrorism and the operation of national and international crime syndicates is often impossible for outsiders to discern especially in places such as the former Soviet Union, Latin America, and other parts of the world.[16] The "gangster state" of Chechyna in the Caucasus is considered by many experts to be a prototype of the post-modern enemy, a warrior enclave alleged to be controlled by criminals, black marketers and drug traffickers.[17] Their tactics were recently demonstrated by the current rash of apartment building bombings in Moscow.

But there is one fundamental difference between international crime and terrorism. Most crime syndicates have no interest in overthrowing the government and decisively weakening society as they have a vested interest in a prosperous economy.[18]

State sponsored terrorism is also still a very real threat. While terrorists cannot count on the Soviet Union for support, state-sponsored terrorism is still thriving with many Middle East and North Africa countries willing to provide support. *The Financial World* magazine recently ran an article that presented the following scenario:

> It is the summer of 2004. The radical Islamic government of Iran, becoming even more aggressive after brutally putting down a challenge by a fledgling democratic opposition, is making increasing demands on its more moderate neighbours -- especially Saudi Arabia. But clearly recalling what happened to Iraq after Saddam Hussein invaded Kuwait, the Iranians have devised a different strategy.
>
> Their plan is to avoid any direct confrontation with the US. Instead they will gradually encroach on the Saudis' independence of action---never blatantly enough to convince the American public that vital US interests are at stake. The Iranians will also try to frighten potential Saudi allies and ultimately seek to take effective control of the Middle East by means of threats.
>
> Those threats will not be idle. With funds from oil sales scarcely affected by Western attempts at embargo, Iran has purchased a modest stockpile of medium-range nuclear missiles from states of the former Soviet Union, with advanced guidance systems brought from China and with sub rosa access to commercial satellite communications networks obtained by bribery. Although not of the latest technology, this makeshift system is capable of causing horrendous damage to targets anywhere in Europe. It is backed by a large inventory of conventional arms: tanks, mines, ships, planes and bombs--including some "dirty" weapons carrying germs and poisonous chemicals. Finally, highly trained and well-equipped terrorist cadres are ready to carry out attacks around the world.
>
> As Saudi Arabia fruitlessly complains to its erstwhile protectors, the country's oil fields are hit by an epidemic of sabotage. Militant Islamic fundamentalists keep the streets of Riyadh in turmoil. But there is not enough evidence to lay any of this conclusively at Iran's door. Moreover, both publicly and even more effectively in private, the Iranians make clear to the Saudis'

> European friends that intervention will bring on devastating retaliation.
> Meanwhile, with a presidential election under way, the American public is vocally isolationist--worried about keeping pace with foreign competitors and repelled by a world full of brushfire wars and nationalistic and ethnic turmoil. As a result, both parties are determined to avoid involvement in any foreign military action that cannot clearly be seen as an inescapable response to a direct threat to US survival. The incumbent President has no stomach for leading a coalition to challenge the Iranians--even if he could recruit partners when his potential allies feel even more imperilled than the US. And the generals and admirals in the Pentagon are adamant that the US must not get into anything but an all-out war.
> As the weeks go by, the will to resist dwindles until--with great fanfare-- the Saudis agree to join a military alliance dominated by Iran and including Iraq and Syria. Control of the Middle East, repository of most of the world's oil and the key to Israel's security has effectively fallen into the hands of the fanatic mullahs in Tehran.

While this scenario may read like a story line for a best selling thriller it is actually a scenario that the Defence Budget Project, a Washington, DC think tanks calls "arguably the most formidable threat the US will face in the first decades of the 21st century". The director of Defence Budget Project, Andrew Krepinevich, claims that the most dangerous future enemy will be what he calls the "streetfighter" state.[19] Raymond Macedonia, co-author of the 1993 book*, Getting It Right: American Military Reforms After Vietnam to the Gulf War and Beyond*, states that the number of countries that could become "streetfighter" nations is expanding each year. "A lot of countries learned from the Gulf War that if you're going to fight the US, you'd better buy mass destruction weapons and the technology to use them. According to Krepinevich, the scenario described above is very plausible, as Iran has already commenced procuring most of the required technology. He stated, "they're buying weapons of mass destruction, ballistic missiles, cruise missiles, strong anti-ship capability and diesel submarines from the

Russians. They're looking to China to buy anti-ship underwater mines far more sophisticated than the ones that gave us fits during the Gulf War. Russia is selling them cruise missiles that the Navy calls Sea Skimmers. Even if you intercept one with a Phalanx, the missile weighs about five tons, so you just turn one projectile into a large shotgun shell."[20]

These "streetfighter" nations will change the face of warfare in the 21st century by waging neo-absolutist war. This is a vicious form of conflict, extending across the spectrum of warfare, waged by unconstrained enemies enfranchised by technology. It would differ from more traditional forms of warfare by the propensity of the enemy to focus not on destroying military forces, but rather on shattering the opponent's will. Rather than playing by the conventional military rules of warfare, they would commit acts of aggression in such a way that they fall beneath the threshold that would trigger a western conventional response.[21] To achieve their objectives, these warrior-society, "streetfighter" nations will also ignore the Western concepts of war, instead viewing those outside their group as not entitled to humane treatment. These warriors would see the moral, political, and cultural values of their opponents as asymmetries to be exploited whenever possible.[22] The emergence of this type of warfare can easily be seen today in places like Chechnya where terrorists are prepared to bomb apartment buildings and kill hundreds or thousands of innocent people.

Samuel Huntington, a Harvard professor, suggests that our future adversaries will likely have moral, political, and cultural norms very different from those of peoples in western nations. With the rise of the co-called "New Warrior Class", which many researchers claim already number in the millions, the western nations will face warriors

who are already accustomed to killing and who are capable of atrocities that challenge normal moral comprehension and who will sacrifice their own kind in order to survive.[23] Professor John Keegan, one of the foremost military historians of our time, has noted the re-emergence of the "warrior" society as observed in such places as Afghanistan, Somalia, and the Balkans. Professor Keegan says that these people are psychologically different from people in western nations; the young are "brought up to fight, think fighting honourable, and to think killing in warfare glorious". A warrior in these societies prefers death to dishonour and kills without pity when he gets the chance. Further, future opponents will not hesitate to use brutality openly to exploit the growing aversion to casualties that more and more shapes the political and military decisions of western democracies. Enemies will seek to manipulate western nations through the media by brazenly displayed barbarism. This strategy worked in the past as seen when Somalis dragged the body of an US serviceman through the streets of Mogadishu, or when Chechens took civilians hostage at a Russian hospital, or when Serbs chained UN personnel to potential targets.[24] James F. Dunnigan noted in his book on future war, "if the opponents are bloody-minded enough, they will always exploit the humanitarian attitudes of their adversaries."[25]

Within the last decade the world has also witnessed the re-birth of dozens of aggressive movements espousing varieties of nationalism, religious fundamentalism, fascism, and apocalyptic millenarianism, from Hindu nationals in India to neo-fascists in Europe and the developing world to the Branch Davidian cult in Waco, Texas. These potential enemies will not have the scientific and technological resources to compare with the western militaries but they will have ready access to a wide array of cheap

unconventional as well as conventional weapons - the poor man's nuclear bombs as they are referred to by Iranian President Ali Akbar Hashemi Rafsanjani.[26] Like guerrilla warfare in such places as Vietnam in the 1960s and 1970s, Afghanistan in the 1980s, and Somalia in the 1990s, these groups, like the "streetfighter" states, will not give their enemies the ability to win on the battlefield but their tactics will allow them to raise the cost of conflict, possibly to the point of paralysing policymakers. This will have significant implications for military forces and operations as future political leaders may be deterred from intervening even in situations where western interests are clearly at stake,[27] thus achieving their victory. This essay will now discuss these weapons and tactics in more detail.

**Weapons and Tactics of Asymmetrical Warfare**

As we enter the 21st century, the threat of the use of weapons of mass destruction is escalating, not on the battlefield by warriors, but among dense population centres by deranged non-nation states.[28] The danger of weapons of mass destruction being used against America and her allies is greater now than at any time since the Cuban missile crisis of 1962.[29] Until recently, most strategists believed that stolen nuclear material constituted the greatest threat in the escalation of terrorist weapons. However, an April 1996 US Defence Department report said that "most terrorist groups do not have the financial and technical resources to acquire nuclear weapons but could gather materials to make radiological dispersion devices and some biological and chemical agents."[30] The manufacture of nuclear weapons is not that simple, nor is delivery to their target. Nuclear material, of which a limited supply exists, is monitored by the U.N. affiliated

International Atomic Energy Agency. Only governments can legally produce it, so that even in this age of proliferation, investigators can trace those assisting terrorists without great difficulty. Chemical agents are much easier to produce but not so easy to keep safely in stable condition and their dispersal depends largely on climatic factors. Biological agents, on the other hand, are far and away the most threatening. They could kill hundreds of thousands of people where chemicals might kill only thousands. While storage and dispersal is trickier than chemical agents, they are easy to produce. [31]

Canadian Department of National Defence document entitled "A Biological Weapon Terrorist Attack on A Major Canadian City" describes a fictional scenario which involves the mass killing of 10,000 Toronto residents. The scenario has a terrorist simply driving along a highway north of the city for 30 minutes, spraying invisible anthrax spores from a hose sticking out of his vehicle. The wind does the rest. If the terrorist took his deadly drive at midnight, thousands of residents of Toronto would be feeling ill by early evening the following day. Initially those people affected will simply believe that they were coming down with an ordinary cold and would not bother to see a doctor. The study suggests that even if the victims chose to seek a doctor their symptoms would likely be misdiagnosed since the symptoms of anthrax are non-specific. After several days of mild symptoms, a high fever would strike and the victims' lungs would fill with fluid. Death would follow within 24 hours with the chest cavity turning to mush. The terrorist would require little more than a technical school diploma in science to execute this scheme. If he had spent any time at all around a laboratory, he would know how to obtain a single anthrax sample, and using potatoes or molasses, grow that sample into a lethal quantity.[32] His sample could be easily ordered through a mail order specimen

company in the U.S; the same way Saddam Hussein brought his original anthrax culture.[33] The procedure would not require specialised equipment or core material; just gardening equipment.

Biological warfare is not a new concept; it has been used as a weapon of war for centuries. In 1346 A.D., Tartars, while holding the walled city of Kaffa under siege, catapulted plague-infested bodies into the city which not only caused the city to surrender, but some medical historians speculate that this event resulted in the bubonic plague epidemic that spread across medieval Europe between 1347 and 1351, killing 25 million people. Biological warfare was introduced to North America during the French and Indian War when the English offered blankets to the Indians that were defending Fort Carillon. The English, suspecting the Indians were loyal to the French, exposed the blankets to the smallpox virus before delivering them to the Indians. The Indians began to fall ill, and after an epidemic spread through the fort, the English attacked and defeated the incapacitated defenders. Through the years there have been many other examples of armies attempting to use natural diseases in war. For example, dumping bodies into water supplies has been a common tactic throughout history. Two thousand years ago, Romans fouled many of their enemies water sources by throwing the corpses of dead animals in the wells. During the American Civil War, Confederate soldiers shot horses and other farm animals in ponds in an effort to contaminate the water supply of the Union forces.[34]

In modern times the 1995 chemical warfare attack in the subway of Tokyo was a glaring example of just how susceptible society could be to these kinds of insidious attacks and how easily these agents are obtained and concealed. To this point, chemical-

biological terrorism was just a theoretical concept for most modern military strategists. Members of Aum Shinri Kyo or the Supreme Truth struck five different subway cars simultaneously carrying a total of 11 plastic packages filled with a Nazi-developed nerve agent called sarin, which was set on the floor and punctured. Despite being a very ineffective way to disperse a nerve agent, 11 people died, mainly those who came into physical contact with the seeping fluid. At least 5,500 others were exposed to the fumes and needed hospital treatment for convulsions, respiratory distress and vision problems. It was two hours after the attack before the Japanese authorities even knew they were dealing with sarin. Had the cult used a contagious biological agent such as smallpox or the plague, where containment and decontamination are crucial, this two-hour delay would have been catastrophic. As it was, the failure to quickly identify the sarin caused the deaths of several emergency workers who went in without protection, and hospital staff themselves became incapacitated from handling tainted clothing.[35]

There is also general agreement among military experts that Iraq had a biological warfare program during the Gulf War that was concentrated on the very toxic botulinum and the very resilient anthrax toxins. This assessment was confirmed by several sources, the most credible being an Iraqi defector who worked as a microbiologist in the Iraqi biological warfare program. The defector said he had personally done research and solved technical problems relating to the weaponisation and deployment of biological warfare agents.[36] There was one unconfirmed news report of several incidents of illness and death among Iraqi guards after the coalition bombed a biological warfare facility in Baghdad.

Some of the other countries suspected in open sources of having or wanting a biological warfare program include the former Soviet Union, Syria, Iran, Libya, North Korea, Israel, Egypt, Cuba, Taiwan, China, Romania, Bulgaria, Pakistan, India and South Africa. There are real concerns with countries like Iraq and those on this list having biological warfare programs or having access to biological weapons. First, many of the countries have been known to support terrorism. Second, many of the counties are geographically located in regions of instability or emerging instability. Finally, the economical distress in the republics of the former Soviet Union may cause biological warfare weapon experts to seek prosperous employment elsewhere.[37] "Consider how much more effective the terrorist bombing of the New York World Trade Centre would have been if the terrorist had placed a fire extinguisher filled with a biological agent at the bottom of each stairwell and rigged them to begin spraying just as the bomb ignited. In the ensuing panic, thousands of occupants of the building would have escaped down the stairs. No one would have considered a fire extinguisher out of the ordinary in a crisis situation after the bombing. Potentially every occupant on the World Trade Centre would have been infected. If the intent of the terrorists were to demonstrate the vulnerability of the population of the US, the addition of biological agents to the conventional attack would really have terrified both the leadership and citizenry of the US, and indeed, all civilised nations."[38]

Despite the moratorium on the development and production of biological and chemical agents, research in this area is anything but stagnant. New biological warfare agents are constantly being developed and old ones genetically reengineered to make them more sophisticated and lethal. The degree of sophistication of a nation's research

program will determine how advanced their biological agents will be. Even the most rudimentary program will likely have very lethal agents that have been a threat for some time. Botulism and anthrax are high-probability candidates that are difficult to reckon with. In addition, the revolution in biotechnology has already, or will in the very near future, produce other agents that are even more toxic and resilient and will give this weapon a great deal more utility on future battlefields whether in the hands of military leaders or terrorists. Relatively minor molecular adjustments may produce a more toxic, fast acting, and stable biological agent. There is also a possibility that genetic engineering may produce a weapon that is unique and can only be protected with a unique vaccine, available only to the attacker. If a commander or terrorist could deploy biological agents against an enemy while friendly troops or supporters remained invulnerable, the biological option would become even more attractive as a weapon. There is also some speculation that a toxic agent could be produced that would target only a specific genetic makeup, giving the attacker the capability to discriminate among age, gender, racial or behaviour groups as targets.[39] After the Aum Shinri Kyo attack on the Tokyo subway, it was determined that the group had ordered sophisticated molecular design software that was capable of reengineering the molecular structure of chemicals and micro-organisms to make them stronger or more dangerous.[40] One can only speculate to what end.

Besides the incredible lethality, another factor that makes biological warfare so dangerous is that the agents are very difficult, if not impossible, to detect while they are in the research, production, transit, or employment phases. Normal biological warfare research facilities are completely similar to legitimate biotechnical and medical research

facilities. The same production facilities that can produce wine, beer, dried milk, food, and agricultural products can produce biological warfare agents. Therefore, it is nearly impossible to identify the locations and facilities that are actually producing biological warfare agents in order to monitor their activities or to take pre-emptive action against them. In addition, if a terrorist wanted to carry a biological agent into any enemy nation in a carry-on bag or checked luggage, there is no mechanism to identify the agent using routine customs, immigration, drug scan, or bomb search procedures. The only way to find it would be a physical search by a very well-trained and very lucky searcher.[41]

Information systems will also become lucrative targets for terrorists. According to the US National Security Agency, the threat posed by potential "cyber attacks" against US military and industry computer systems and information networks is now growing beyond the "computer hacker" stage to the point where foreign governments and groups potentially hostile to the West are developing or trying to acquire such offensive capabilities.[42] For resource limited adversaries, information warfare has become a relatively cheap and practicable alternative to full-scale war. It can be waged from anywhere in the global spectrum and offers anonymity to potential adversaries.[43] In a cap2 T.020tm4tCeere

An attack on a country's military information systems can potentially be a very potent strategy against one's enemies. Just as Japan attempted to annihilate America's Pacific Fleet at Pearl Harbour in 1941, an adversary may use an information attack to hamper an enemy's war effort. Instead of using bombers, the information system itself can be attacked directly using information weapons. Military systems may be complex and expensive but the technology needed to attack information systems is low cost (a computer and modem), widely available (a willing hacker) and just as efficient (one telephone call). Futurist Alvin Toffler argues that an enemy does not have to be big and rich to inflict significant damage through information warfare. "A few smart guys with computer workstations and modems could endanger lives and cause great economic disruption," according to Donald Latham, a former pentagon communication czar.[44]

Terrorist groups or rogue states can easily and quickly learn the technical skills themselves or hire hackers to conduct information warfare. Hackers may be the mercenaries of the 21st century, available to the highest bidder. During the Gulf War, according to Pentagon officials, a group of Dutch hackers offered to disrupt the US military's deployment to the Middle East for one million dollars. Saddam Hussein turned down the offer. However, according to computer-security experts the potential for disruption was great. During the Gulf War, the military made extensive use of the Internet for its communications, and it would have suffered had the Iraqis decided to take it out.[45]

The toughest military computer to crack is the first one. Once inside, nearly 90 percent of the other computers linked to the first computer will recognize the intruder as a legitimate user.[46] In her paper "Information Warfare: Combating the Threat in the 21st

Century," Mary Gillam refers to an article in *SIGNAL* magazine entitled "Defence Organisation Safeguards War Fighters' Information Flow". This article notes that the Defence Information Systems Agency Centre for Information Systems Security (CISS) countermeasures department had launched 12,000 attacks against the Defence Department computer systems in 28 command vulnerability assessments. According to Michael Higgins, the CISS countermeasures department head, more than 88 percent of those systems were successfully compromised. Only about 500 users detected the intrusions, and only two dozen users reported the intrusions. The tools used to conduct the intrusions are readily available commercially.[47] Higgins further stated:

> The information security problem is worsening, as the number of computers in the US government continue to rise. The United States is the world's most interconnected country, and the operational reliance on computers also is increasing, along with the complexity of the computing environment. While active information security is being used, hackers who are motivated by money are turning professional.

All of this has great significance for global security in the 21st century. As the year 2000 approaches, a very large percentage of the governments' and the private sector's transactions are on-line. Societies at large are becoming more dependent on the electronic storage, retrieval, analysis, and transmission of information. The National Security Agency is concerned that computers controlling banking, stock exchanges, air-traffic control, phones and electric power could be crippled by terrorists or a determined hacker. Western nations are now totally reliant on computers making them very vulnerable. A terrorist group or wired adversary could take down these computers without ever entering the affected countries.

"An unnamed US intelligence official has boasted that with one billion dollars and 20 capable hackers, he could shut down America."[48] The terrorist group could easily achieve the same end. The potential to create chaos is almost unlimited. Therefore, with such soft targets readily available to them, many terrorist groups will almost certainly switch from assassinations and indiscriminate killings to information warfare. Attacks on electronic switching will produce far more dramatic and lasting results. Imagine the devastating effects if a terrorist group hit on the computers at the US Federal Reserve Headquarters at Culpepper, Virginia which handles all federal funds and transactions.[49] Indeed, in some respects, information warfare may only refine the way modern warfare has shifted toward civilian targets, from the fire-bombings of Dresden and Tokyo during World War II to the "ethnic cleansing" in Balkans to electronically disabling a country's financial and social infrastructure. Attacking a country's banking, stock exchanges, air-traffic control, phones and electric power might be accomplished cleanly by computers—but it is still an attack on civilians. As we have seen with the embargoes against Iraq, economic warfare can be as dire as other forms of warfare, especially on civilians. Information warfare may be able to avoid some of traditional warfare's lethal, bloody and dirty traditions, but in the words of William Tecumseh Sherman "War is cruel, and you cannot refine it."[50]

**COUNTERING THE ASYMMETRICAL THREAT**

Currently, there are disagreements amongst many nations and within nations on how to deal with the asymmetrical threat. Retribution is advocated by many hard-liners particularly the US as was demonstrated by their retaliation on terrorist camps in

Afghanistan and chemical weapons facilities in Sudan following the bombings of their embassies in Kenya and Tanzania. Other countries, including Canada, would argue that it is easier and cheaper to let the US take the lead, but the hard-line US approach may be difficult to sell at home. On the other hand, rehabilitation is advocated by those more tolerant of violent means, like the members of European Union, although appeasement and compromise have historically been poor responses to international threats. Those who assume that there may be reasons for the violence and who wish to know what that might be before condemning the violent, advocate a mixed strategy.[51] They would suggest that giving a terrorist or an insurgency group political recognition would add creditability to their cause and may pave the way for a negotiated peace settlement. However, this approach also has its dangers, as many of the legitimate factions involved in the conflict may be reluctant to sit at the same negotiating table as terrorists.

To date, the deceptively small scale of the asymmetric threats has effectively concealed the potency of the danger which, in turn, has misdirected planning efforts and thereby confounded nations' ability to respond adequately. This has resulted in western nations becoming increasingly vulnerable to these growing threats as a result of their militaries' capabilities being too heavily reliant on war-fighting skills designed for conventional engagements.[52] If military leaders continue their slavish belief in high-tech combat, there will likely be a recurrence of the attitude that affected the US military in Vietnam: an enemy, through strategies and tactics, successfully made itself seem militarily unimportant to the US soldier. Some will claim this attitude is already present in the US military and that many "uniformed elites" believe themselves too good now to engage this kind of enemy, partly because they feel "real soldiers" do not treat terrorists

as worthy foes and partly because their "techno worship" blinds them to the fact that the battle will be against adversaries trying to "mess" with their heads, rather than capture their territory. But Socrates stated that the "guardians" should protect a nation's culture. This will mean that in the 21st century our militaries must fight those who seek through various forms of asymmetrical warfare to undermine public confidence."[53]

The asymmetrical threat will have an effect on warfare at all three levels (strategic, operational, and tactical) but it will be most dramatic at the operational level. The strategic level leaders must continue to be concerned with the entire spectrum of national and international security issues, regardless of the source, and must operate within the political arena to seek solutions and to develop strategies to address the problems. They will also design the policies and guidance which will set the framework by which operational level commanders and their civilian counter-parts in other government and non-government agencies will operate to address the perceived threats. While the tactical level commanders must acquire new skills and learn to employ their forces in different operational arenas, their leadership role will not change appreciably. However, as the world enters the 21st century, the challenge for operational level leaders will change drastically. It will be the operational level commanders who will have the responsibility for the defence of the country and their military forces involved in operations in other parts of the world who will be especially susceptible to terrorist attacks. In addition, it will be the responsibility of the operational level leaders to co-ordinate defence activities with the many other agencies which could become involved whether they are police forces, intelligence agencies, or emergency response organisations.

According to British and US Defence Doctrine, the "manoeuvrist" theory of warfare which has replaced the "attritionist" theory is equally applicable to all types of military operations, and so out-manoeuvring one's enemy by thought or by deed can have as much utility in asymmetrical warfare as it can in conventional warfare.[54] In other words, operational leaders must intellectually out-manoeuvre their adversaries. As stated by Lieutenant-General Romeo Dallaire, operational leaders of the 21st century must be educated and have an in-depth understanding of the human side of war. They must understand their own culture and be a part of it if they are to win the trust of the people and that of their troops. They will also have to understand the civilian population that supports their adversaries. In any warfare, knowing one's enemy is fundamental to success and this is no less true in the case of an asymmetrical threat.[55] And finally they will have to understand the power of the media and have the courage to say no to politicians and strategic military leaders who would make promises based on technological wizardry.

To be effective in addressing the asymmetrical threat, military policies, doctrines, strategies, and readiness of western nations must reflect effects-based warfare strategies and pre-emptive actions rather than retaliatory reactions. Traditional force-on-force strategies, which produced successes on the battlefield during past conflicts, will be undermined by the new unconventional threats. Precision weapons will not necessarily be the solution as "streetfighter" states will not hesitate to hide their communication centres and other vital facilities beneath POW camps, schools, hospitals, and similar facilities. Combating this threat will require a joint effort on the part of a number of organisations. However, nations must first implement systems of decision-making that

will combine civil, military, and intelligence expertise throughout their respective chains of command. This decision-making system must integrate planning and operational activities, build up institutional capabilities, and highlight defensive needs before an incident happens. This strategy should include four elements: intelligence and warning, prevention and deterrence, crisis and consequence management, and co-ordinated acquisition of equipment and technology.[56]

The challenge for military leaders will be to train and equip their forces to respond to biological, radiological, or chemical threats and to develop the capability to defend against information warfare. If an attack occurs against a civilian target, the military must respond immediately to mitigate casualties and damage. This would require emergency medical care; distribution of protective clothing, medications and vaccines; and evacuations and area quarantines.[57] To respond effectively to these attacks, militaries must procure effective, comfortable, and long-wearing protective clothing for their soldiers to replace the existing ensemble. A self-contained, air conditioned unit would be ideal. The military must also procure and deploy improved sensors to detect and identify contaminants, including low-level exposure to chemical nerve agents, which have cumulative toxic effects.[58] The military must also be capable of eliminating biological, radiological, or chemical production facilities and stored munitions. To achieve this, they must work with the technology community to develop a capability to destroy these facilities and wipe out the agents before they can be used on friendly forces or the general population and without causing unacceptable level of collateral damage.[59] Winning over the local populations must also be an objective of the

military because if the civilians belong to the enemy, the terrorists can blend-in with the local population and no sophisticated technology will be able to find them.[60]

To mitigate the consequences of an attack against troops, units should be reduced in size and dispersed throughout the threatened areas or battle zone. Since the threats will often be terrorists acting without the support of massive forces, to defeat them will require soldiers with fighting skills, toughness, discipline, and lots of field training with infantry weapons. Infantry will rise in importance in the next century because of its ability to hide from and sneak though high-tech barriers. [61]

To protect defence information systems from attack, the military must integrate all information warfare activities and bring all individual efforts together to produce an overall balanced strategy. All members of the Defence Department, both military and civilian, must be educated to the vulnerabilities inherent in the conduct of information transmission and reception and must be taught to report all intrusions. Protective countermeasures such as automated intrusion detection capabilities, hacker intrusion alarms, double-password protection, software firewalls, virus scan software, and other protection devices currently under development, must be implemented as they would eliminate many of the simple invasions that occur. Finally, information warfare should be included in all major exercises to permit member to practice their counter-measure procedures.[62]

Finally, it is important to stress the fact that the emergence of a new threat in one area of military affairs does not mean that all other threats are suddenly obsolete. These new threats will not displace the existing ones but merely add to them. There is little doubt that while the West struggles to counter the new asymmetrical threats, the need to

e able to con entional warfa conventional nilarly equippe

e US and its llies will exis the next mill There are still

me 28 coun over 1000 tar experts wou rongly, howeve

at nations m their milita ties in order the increasing

reat from " " states or th less enemy e terrorist,

litical or c ture, or a h hree.[64]

NCLUS

A appro este ew types of

sari ectro logi ly physically

will l ba rrito tories in the

ntic TT0 1 haern a .999631 570ies in

few and relatively unsophisticated terrorists can tie down the combined capability of regular forces equipped with the latest technology, as the Afghan rebels did so effectively to the Soviet Union during the Afghanistan War.[66]

In conclusion, many analysts agree that the western militaries are ill prepared for asymmetrical warfare that now seem to be more of a probability than a possibility. The threat of catastrophic terrorism spans the globe, defying ready classification as solely foreign or domestic. The fundamentalist, the revolutionary, terrorist, and the rouge state all can advance their cause in the face of the apparently overwhelming odds of western governments who continue to deploy organised military forces in the mistaken belief that they are superior and will not be militarily challenged. To effectively address the counter-revolution in military affair and the increased threat from asymmetrical warfare, militaries must develop strategies and plans for applying armed force to frustrate the violent actions of their foes at the least possible cost in time, resources, and above all blood.[67]

[redacted]

[redacted] Journal June 1999: 56

[redacted] Asymmetrical Threats New Military Watchword," Aviation W[redacted] Technology; 27 Apr., 1998: 55

[11] Anthony Stone, "Future imperfect", RUSI Journal June 1999: 56

[12] Conference of Defence Association Institute, A Strategic [redacted] Canada's Response to the New Challenges of International Sec[redacted] Defence Association Institute (Ottawa, Conference of Def[redacted] 15

[redacted] Terrorism," Foreign Affairs Sep/Oct 1996: 25

[14] Walter Laqueur, "Post-modern terrorism," Foreign Affairs Sep/Oct 1996: 24

[15] Walter Laqueur, "Post-modern terrorism," Foreign Affairs Sep/Oct 1996: 25

[16] Walter Laqueur, "Post-modern terrorism," Foreign Affairs Sep/Oct 1996: 25

[17] Paul Mann, "Pentagon Called Unprepared For 'Post-Modern" Conflict," Aviation Week and Space Technology; 27 Apr., 1998: 55

[18] Walter Laqueur, "Post-modern terrorism," Foreign Affairs Sep/Oct 1996: 25

[19] Dan Cordtz, "War in the 21st century: The streetfighter state," Financial World 29 Aug, 1995: 43

[20] Dan Cordtz, "War in the 21st century: The streetfighter state," Financial World 29 Aug, 1995: 43

[21] Dan Cordtz, "War in the 21st century: The streetfighter state," Financial World 29 Aug, 1995: 43

[22] Charles J. Dunlap Jr, "21st Century Land Warfare: Four Dangerous Myths," Parameters: Journal of the US Army War College Autumn 1997: 28

[23] Charles J. Dunlap Jr, "21st Century Land Warfare: Four Dangerous Myths," Parameters: Journal of the US Army War College Autumn 1997: 27

[24] Charles J. Dunlap Jr, "21st Century Land Warfare: Four Dangerous Myths," Parameters: Journal of the US Army War College Autumn 1997: 28

[25] James F.Dunnigan, Digital Soldiers: The Evolution of High-Tech Weaponry and Tomorrow's Brave New Battlefield, (New York: St Martin's Press, 1996) 219.

[26] Walter Laqueur, "Post-modern terrorism," Foreign Affairs Sep/Oct 1996: 28

[27] Zalmay Khalilzad and Ian O. Lesser, The Sources of Conflict in the 21st Century, (Washington, RAND, 1998) 23

[28] Terry Mayer, "Biological Weapons: The Poor Man's Nuke," Air University, Maxwell Air Force Base, April 1995: 21

[29] Ashton Carter, "Catastrophic Terrorism," Foreign Affairs, Nov/Dec 1998: 81

[30] Walter Laqueur, "Post-modern terrorism," Foreign Affairs Sep/Oct 1996: 27

[31] Walter Laqueur, "Post-modern terrorism," Foreign Affairs Sep/Oct 1996: 27-28

[32] Leonard Stern, "In the Battle Against Bio-terrorism, Canadian Researchers Are On the Front Line," Ottawa Citizen 19 Sept 1999: C3

[33] Terry Mayer, "Biological Weapons: The Poor Man's Nuke," Air University, Maxwell Air Force Base, April 1995: 20

[34] Terry Mayer, "Biological Weapons: The Poor Man's Nuke," Air University, Maxwell Air Force Base, April 1995: 5

[35] Leonard Stern, "In the Battle Against Bio-terrorism, Canadian Researchers Are On the Front Line," Ottawa Citizen 19 Sept 1999: C3

[36] Terry Mayer, "Biological Weapons: The Poor Man's Nuke," Air University, Maxwell Air Force Base, April 1995: 12

[37] Terry Mayer, "Biological Weapons: The Poor Man's Nuke," Air University, Maxwell Air Force Base, April 1995: 15

[38] Terry Mayer, "Biological Weapons: The Poor Man's Nuke," Air University, Maxwell Air Force Base, April 1995: 21

[39] Terry Mayer, "Biological Weapons: The Poor Man's Nuke," Air University, Maxwell Air Force Base, April 1995: 16

[40] Terry Mayer, "Biological Weapons: The Poor Man's Nuke," Air University, Maxwell Air Force Base, April 1995: 17

[41] Terry Mayer, "Biological Weapons: The Poor Man's Nuke," Air University, Maxwell Air Force Base, April 1995: 17

[42] Craig Covault, "Cyber Threat Challenge Intelligence Capability," Aviation Week & Space Technology 10 Feb 1997: 20

[43] Mary M. Gillam, Information Warfare: Combating the Threat in the 21st Century, Air University, Maxwell Air Force Base 1998: 15

[44] Douglas Waller, “Onward Cyber Soldiers,” Time 21Aug 1996: 41

[45] Douglas Waller, “Onward Cyber Soldiers,” Time 21Aug 1996: 41

[46] Douglas Waller, “Onward Cyber Soldiers,” Time 21Aug 1996: 42

[47]Mary M. Gillam, Information Warfare: Combating the Threat in the 21st Century, Air University, Maxwell Air Force Base 1998: 18

[48] Walter Laqueur, "Post-modern terrorism," Foreign Affairs Sep/Oct 1996: 30

[49] Walter Laqueur, "Post-modern terrorism," Foreign Affairs Sep/Oct 1996: 30

[50] Douglas Waller, "Onward Cyber Soldiers," Time 21Aug 1996: 42

[51] Willian L Waugh Jr., "Rogue Regimes: Terrorism and Proliferation," Perspectives on Political Science, Winter 1999: 51

[52] Anthony Stone, "Future imperfect", RUSI Journal June 1999: 59

[53] Michael Duncan Wyly, "Combat in the 21st Century," US News and World Report, 16 Mar1998: 82

[54] Anthony Stone, "Future imperfect", RUSI Journal June 1999: 58

[55] Anthony Stone, "Future imperfect", RUSI Journal June 1999: 57

[56] Michael Duncan Wyly, "Combat in the 21st Century," US News and World Report 16 Mar1998: 82

[57] Anthony Stone, "Future imperfect", RUSI Journal June 1999: 56

[58] Jonathan Tucker, "Asymmetric Warfare", Forum for Applied Research and Public Policy Summer 1999: 38

[59] Terry Mayer, "Biological Weapons: The Poor Man's Nuke," Air University, Maxwell Air Force Base, April 1995: 23

[60] Ashton Cater et al, Catastrophic Terrorism: Tackling the New Danger," Foreign Affairs November/December 1998: 85

[61] Michael Duncan Wyly, "Combat in the 21st Century," US News and World Report, 16 Mar1998: 81

[62] Mary M. Gillam, Information Warfare: Combating the Threat in the 21st Century, Air University, Maxwell Air Force Base 1998: 32

[63] Anthony Stone, "Future imperfect", RUSI Journal June 1999: 56

[64] Paul Mann, "Asymmetrical Threats New Military Watchword," 27 Apr 1998: 56

[65] Paul Mann, "Pentagon Called Unprepared For 'Post-Modern Conflict," 27 Apr 1998: 54

[66] Anthony Stone, "Future imperfect", RUSI Journal June 1999: 56

[67] Anthony Stone, "Future imperfect", RUSI Journal June 1999: 56

## Bibliography

### Books

Dunnigan, James F., Digital Soldiers: The Evolution of High-Tech Weaponry and Tomorrow's Brave New Battlefield. New York: St Martin's Press, 1996.

Fried, George and Meredith. The Future of War: Power, Technology and American World Dominance in the 21st Century. New York: Crown Publishers, 1996.

Huntington, Samual P. A Clash of Civilians and the Remaking of World Order. New York: Simon & Schuster, 1996.

Kennedy, Paul. Preparing for the Twenty-First Century. London: Harper Collins, 1993.

Khalilzad, Zalmmay and Lesser, Ian. Sources of Conflict in the 21st Century. Washington: RAND, 1998.

O'Brien, Connor Cruise. On the Eve of the Millennium. Concord ON: Anansi, 1994.

Van Creveld, Martin. The Transformation of War. New York: The Free Press, 1991.

### Monographs, Proceedings, Academic Papers and Reference Books

Conference of Defence Association Institute. A Strategic Assessment: Canada's Response to the New Challenges of International Security. Conference of Defence Association Institute, Ottawa, 1999.

Department of National Defence. Shaping the Future of Canadian Defence: A strategy for 2020. June 1999

Dewer, J.S. "Revolution in Military Affairs: The Divergence Between the Most Dangerous and the Most Likely." Advanced Military Studies Course * AMSC 1.

Gillam, Mary M. "Information Warfare: Combating the Threat in the 21st Century." Thesis. Air University, Maxwell Air Force Base, 1998.

Mayer, Terry N. "Biological Weapons: The Poor Man's Nuke." Diss. Air University, Maxwell Air Force Base, 1995.

Semiamow, W. "The Revolution in Military Affairs: All That Glitters is not Gold," Advanced Military Studies Course * AMSC 1.

**Articles**

Burton, Daniel F. Jr. " The Brave New Wired World." Foreign Policy Spring 1997: 22 -27

Carter, Ashton, et al. "Catastrophic Terrorism: Tackling the New Danger." Foreign Affairs Nov./Dec. 1998: 80 - 94

Cohen, Eliot A. "A Revolution in Warfare." Foreign Affairs, Mar./Apr. 1996: 37 - 48

Cordtz, Dan. "War in the 21st century: The streetfighter state." Financial World 29 Aug. 1995: 42 - 47

Cordtz, Dan. "War in the 21st century: The digitized battlefield." Financial World 29 Aug. 1995: 47 - 50

Covault, Craig. "Cyber Threat Challenge Intelligence Capability." Aviation Week & Space Technology 10 Feb. 1997: 20 - 21

Dunlap, Charles J. Jr. "21st-century Land Warfare: Four Dangerous Myths." Parameters: Journal of the US Army War College Autumn 1997: 27 - 37

Editorial. "Not quite a new world order, more a three way split." The Economist, December 20, 1997.

Editorial. "The future of warfare." The Economist 8 Mar 1997: 15 -16.

English, John. The Operational Art - Developments in the Theories of War. Westport, CT: Praeger Publishers, 1996.

Freedman, Lawrence. "The Changing Forms of Military Conflict." Survival Winter

Keegan, John.  "The Warrior's Cose of No Surrender." US News and W