CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
AMSC 6 / CSEM 6

WAR IN THE 21st CENTURY

THE GOOD, THE BAD, AND THE UGLY: KNOWING AND FINDING THE ADVERSARY IN THE "THREE BLOCK WAR"

By /par …
Commander Martin Adamson

25 October 2003

THE GOOD, THE BAD, AND THE UGLY: KNOWING AND FINDING THE ADVERSARY IN THE "THREE BLOCK WAR"

Many people think it is impossible for guerrillas to exist for long in the enemy's rear. Such a belief reveals lack of comprehension of the relationship that should exist between the people and the troops. The former may be likened to water and the latter to the fish who inhabit it.

- Mao Tse-tung: On Guerrilla Warfare, 1937.

I. INTRODUCTION

Recent newspaper headlines may well characterize the future of war as we enter the 21st century. On one hand, the rapid buildup of an overwhelming US (United States) led coalition military force resulted in a seemingly decisive campaign against conventional Iraqi forces. On the other hand, today, those same coalition forces are undergoing a regular cycle of ambushes, rocket attacks and suicide bombings. Despite superiority in both conventional forces and technology, insurgents and terrorists continue to hide within "plain site" and emerge from the shadows of Iraqi cities to unleash their attacks. The US is not the only dominant military power to face this type of asymmetric[1] threat; history has many examples and modern Israel is striving to confront combatants who include young women ready to detonate suicide bombs within crowded restaurants.

The Revolution in Military Affairs (RMA)[2] and the resulting disproportionate US gains in intelligence, command and control, and precision will likely maintain the current US military dominance; however, human nature has not changed and both the will to win and aggression still flourish. As such, in any conflict involving a US led coalition, the adversary will likely seek to exploit asymmetric warfare rather than venturing into the conventional arena. Thus, the future of warfare will probably have a greater resemblance to the streets of Mogadishu than to the Kursk pocket. Adversaries to a US coalition will hide amongst non-combatants and strike, where and when they can, with terror and surprise. This type of war will demand new technologies and capabilities as the challenges inherent

in identifying individuals and small groups differ significantly from those required to track major combat units.

This paper will assert that modern land-based conflict is evolving to encompass the model of the "three block war," [3] one in which the full spectrum of conflict will arise within a few hours and within a few city blocks. Enhanced surveillance as well as a deep understanding of the adversary's motivation and culture will be key factors in determining a coalition's success in defeating an asymmetric opponent. To chart this course, an initial review of the changing nature of war will be conducted. Evolving technologies and techniques necessary for both knowing and identifying asymmetric adversaries will then be assessed. Finally, conclusions relevant to Canada's ability to operate within the "three block war" will be rendered.

II THE SHAPE OF WAR IN THE 21ST CENTURY

The magnitude and extent of the RMA provides considerable scope for debate amongst military theoreticians and historians. Some contend that it is more evolutionary than revolutionary; however, most agree that the nature of warfare is changing given enhancements in precision, information management, and battlespace awareness. These technologies, which focus on the ability to collect, analyze, disseminate and act upon information, have enabled militaries, especially the US, to enhance combat power, ease friction, and be more adept at peering through the fog of war.[4] Whether or not this particular RMA will have the same impact on warfare as the development of the stirrup will likely be the focus of scholarly attention for many years to come.

What is irrefutable is the growth of military power that resides in the United States. Harnessing existing and emerging technologies, the US military has evolved into a force for which there is no symmetric, or conventional, peer competitor either now or in the foreseeable future. The Quadrennial Defence Review

of 2001 indicates that there is no clear competitor in the near term; however, it raises the specter of terrorist attacks as a risk to the US.[5] Other sources indicate the potential for a peer competitor to arise in 2015 or thereabouts;[6] however, this is a questionable assertion. The US technical and economic dominance that has propelled military power will continue to extend the qualitative gap between the US and any likely rivals.[7] This is demonstrated by the magnitude of US defense spending. The US commits 3% of its GDP to defence expenditures; however, this expenditure accounts for 37% of the combined world defense budget.[8] With respect to RDT&E (Research, Development, Test, and Evaluation), the US budget for 1996, $37 Billion, was twice that of the combined RDT&E budgets of China, France, Germany, Great Britain, Japan, and Russia.[9] In 2004, the budget for US RDT&E will exceed $61 Billion,[10] and will support the development of numerous RMA-type technologies employed in precision weaponry, command and control, and surveillance. US forces can deliver overwhelming power from, and on, the sea, the land, and the air; the qualitative and quantitative force overmatch is such that no country can engage the US in symmetrical conflict with any realistic hope of victory.[11]

The US and its allies, while possessing overwhelming military force, do have vulnerabilities which some opponents may seek to exploit – to whit, an aversion to casualties and sensitivity to world and, more importantly, domestic opinion.[12] Domestic opinion, in turn, can be swayed by a perceived lack of progress, growing duration of the conflict, the infliction of collateral damage during operations and resultant domestic concerns with respect to the necessity, legality, and legitimacy of military operations. In confronting a US led coalition, these vulnerabilities are normally unassailable through symmetrical conflict; however, they can be attacked asymmetrically.[13] Asymmetric warfare may be a comparatively recent addition to the military argot; however, the concept is not. Indeed, Sun Tzu exhorted his successors by stating “All warfare is based on deception … If he is in superior strength,

evade him … If he is taking his ease, give him no rest … Attack him where he is unprepared."[14] Thus, future adversaries to a US led coalition, who will undoubtedly be inferior in conventional military strength, will be far more likely to seek resolution by exploiting time, will, and the inherent power of the defense.[15] Therefore, asymmetric approaches including insurgency, terrorism, and employment of Weapons of Mass Destruction may well be employed against future US led coalitions.[16] As stated by General Charles Krulak (Commandant USMC), "a symmetrical and overwhelming approach by a dominant power . . . always … invites an asymmetrical response."[17]

Furthermore, a sound opponent, wishing to attack the vulnerabilities of a US led coalition will stand the best chance of success by forcing the coalition to conduct Military Operations in Urban Terrain (MOUT) [18] as it reduces technological advantage while dramatically increasing the opportunity to inflict casualties on coalition forces.[19] In addition, the natural forces of demographics and global urbanization will, by necessity, tend to draw forces into urban areas either in combat or peace support operations; projections indicate that 85% of the world's population will be located in urban centers by 2015.[20] Conventional militaries, like Canada's, try to avoid urban conflict; Canada's land forces doctrine states "if a built up area is defended…[it is]…preferable for the attacker to bypass or encircle it" rather than take it, as it is "costly both in time and manpower."[21] Sun-Tzu is more succinct "The worst policy is to attack cities. Attack cities only when there is no alternative."[22] This reluctance to undertake urban combat was illustrated in Chechnya. After terrible losses and the erosion of public support in 1994-96, the Russians were determined that they would need to avoid urban conflict and would bypass cities, relying on either negotiation or shelling. This doctrinal decision, which resulted in a decision to not train for urban warfare, resulted in significant casualties when the Russians were once again forced to attack Grozny five years later.[23] Chechen guerillas recognized their vulnerability in the open and their comparative strength in urban terrain; hence, they forced the Russians to come into

the cities.

An illustration of the comparative vulnerability of Western powers to asymmetric threat and the complexities of urban terrain is provided by a review of the US engagement in Somalia. While clearly outmatched militarily, Aideed, the most powerful warlord in Somalia correctly identified the US center of gravity as public opinion, which had already been weakened by limited US public commitment to the mission. Thus, he sought to attack this vulnerability by inflicting US casualties in an urban battle.[24] The US led coalition, compromised by an extremely poor command and control framework and not appreciating the Somali culture, entered into a bloody firefight in the Bakara Market in Mogadishu. The US suffered 91 casualties of whom eighteen were killed; the Somali fatalities numbered in excess of three thousand, of whom many were non-combatants. After seeing dead American soldiers being dragged through the streets of Mogadishu, the US Congress, reflecting the views of the American public, pressured the President to withdraw forces.[25] In this case, a poorly equipped third-world militia prevailed over the US led coalition through a ruthless urban-based campaign focused on eroding US public support for the mission. Aideed lost the tactical engagements; however, he prevailed in the conflict and the US withdrew.

In response to the growing likelihood of confronting asymmetric combatants in unfamiliar and unforgiving urban terrain, General Krulak developed a model for future warfare known as the “three block war.” This model captures the unpredictability and broad spectrum of conflict that will be the centerpiece of modern asymmetric conflicts.

> In one moment in time, our service members will be feeding and clothing displaced refugees, providing humanitarian assistance. In the next moment, they will be holding two warring tribes apart – conducting peacekeeping operations – and, finally, they will be a fighting a highly lethal mid-intensity battle – all on the same day … all within three city blocks.[26]

Canada, in keeping with its foreign policy objectives of the promotion of peace as the key to protecting Canadian security and the projection of Canadian values, has, since the end of World War II, participated in coalitions across the continuum of conflict, with particular emphasis on peace support operations. This country has traditionally been aligned with the US, and while there have been exceptions such as Vietnam and the 2003 invasion of Iraq, shared values and security objectives will tend to prevail. While the US will reserve the right for unilateral action, it will normally seek to align itself with like-minded coalition partners.[27] Henceforth, it is most likely that Canada, though not exclusively, will participate in US led coalitions and will need to be ready to confront asymmetric adversaries in the "three block war." In addition, to the "three block war," Canada will potentially operate in non-US led coalitions focused on peacekeeping and nation building.

Van Creveld paints a disturbing view of a future in which asymmetric warfare is rife and conventional forces are rendered irrelevant.

> Armed conflict will … have more in common with the struggles of primitive tribes than with large scale conventional war…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. It will be protracted, bloody and horrible.[28]

To prevent van Creveld's vision from being a reality, coalition commanders will need to be able to address the challenges of asymmetry. Predictability will be one of the first casualties of war and combatants, who will be indistinguishable from the civilian populace, will surround the modern soldier. Success may hinge on locating and tracking small groups, or perhaps just one man or woman, within a teeming third-world market. Rugged border areas will have to be scoured to find a few men concealed within the movement of refugees. The risks to be confronted in the "three block war" will demand different surveillance technologies than have heretofore been developed for the planned armored battles of the cold war. Not only will individuals and groups have to be identified, but there will also have to be a strong understanding of motivations and culture. In the next section of this paper, a number of the

relevant surveillance techniques and technologies that will be necessary for 21st century warfare will be discussed.

III. SURVEILLANCE IN 21ST CENTURY WARFARE

The problems inherent in understanding and identifying adversaries within a population are not new and history provides a number of relevant lessons that are instructive. Further, in keeping with the theme of "war in the 21st century" a survey of relevant technology is warranted, as this will provide a sense of the capabilities that will be available to the future operational commander. An emphasis will be placed on US technology and development programmes as they, for the most part, are state of the art. As a means of organizing this review, use will be made of Mao's analogy of insurgent fish swimming in the sea of the people.

Understand the Sea

Very few fishermen will make it to comfortable retirement unless they have a solid understanding of the sea, including its inherent dangers and opportunities. Likewise, a critical element for the operational commander is to fully understand the adversary – and hence the need for human factors analysis – an understanding of the mindset and psychology of one's opponent.[29] While important across the spectrum of conflict, this element becomes vital in asymmetric warfare. Somalia highlighted the criticality of understanding cultural factors when undertaking a campaign in an asymmetric environment. While a desperately poor third world nation, Somalia is noteworthy in many respects. Specifically, the importance given to the stature of the 'clans', the warlike nature of the populace, the willingness to accept casualties, and the inclusion of women and children in the clan's order of battle. [30] The decision that transitioned the campaign to counter insurgency operations directed against the principal clan inflamed the population in a manner that would not be understandable to most

Westerners. Further, few Westerners would countenance an operational plan that was predicated on accepting disproportionate casualties amongst one's own women and children. Major General Zinni observed that the principal failure of US intelligence was the inability to "penetrate the faction leaders and … understand the culture, the clan association affiliation, [and] the power of the faction leaders."[31] At the tactical level in the Bakara market, the Rules of Engagement were also highly constrained and did not account for the Somali willingness to place non-combatants in the line of fire; in one instance a gunman opened fire between the legs of a woman with four children sitting on him for cover.[32]

The recent conflicts in Chechnya also highlighted the need to understand the cultural and military heritage of the adversary. As Russian troops approached Grozny in 1994, operational commanders considered that their overwhelming military force would intimidate the population.[33] They ignored the militant tradition of Chechnya, the two centuries of conflict with Russians and, most importantly, Stalin's mass deportation of the Chechens in 1944. To Chechens, the deportations and attendant privations, which led to a 50% death rate, had the same visceral impact as the Holocaust had on the Jews, and ingrained a staunch and steadfast resistance to being part of the Russian state. These cultural factors were paramount in the brutality and vehemence that defined the bloody defence of Grozny and Chechnya.[34]

In understanding the culture of the adversary in asymmetric warfare, the operational commander will likely be at a natural disadvantage as his adversary may have a far better personal understanding of the Western psyche than we will have of theirs. Aideed, as a member of a third world elite, was educated in Italy and Russia and understood Western weaknesses and strengths. On the other hand, Western commanders and their forces will often only be physically exposed to the culture of their adversary when they commence operations. Britain was able to maintain India within the Empire for approximately 200 years despite being dramatically outnumbered and confronting intrigue, subterfuge,

and nascent revolt. There were many issues at play; however, one of the enablers was the understanding developed by military and political officers who made their careers in India. Those that survived disease knew the languages, knew the culture and most importantly knew their opponents. When the sub-continent erupted in the mutiny of 1857, a contributing factor was the arrival of a new generation of administrators and leaders who were aloof and no longer understood India and its complexities.[35] To offset the lack of familiarity that today's operational commander will have of his adversary, he must be able to draw upon the expertise of skilled analysts and have access to linguists[36] to develop a full understanding of the motivations and limitation of the enemy.[37]

Achieving the greatest possible understanding of both the environment and the adversaries will be key to achieving operational success. To this end, the US has initiated the concept of Operational Net Assessment (ONA), a comprehensive intelligence picture developed by fusing information from military sources, government agencies and non-governmental organizations. The objective is to have a holistic understanding of the enemy and identify the most appropriate actions that may be taken across the diplomatic, information, military and economic (DIME) spectrum of operations.[38] While not a new concept, ONA uses highly complex data fusion and dissemination systems to generate a comprehensive picture of the adversary gained from these numerous, and far reaching, sources of intelligence: this picture is the so-called Common Relevant Operating Picture (CROP). ONA is currently under development within USJFCOM[39] and is still in an experimental stage.

Finding the Fish

The dynamics of locating combatants engaged in asymmetric operations has been, and continues to be, a challenge. However, technology has ameliorated many of the problems faced when the range of surveillance was restricted to that that could be seen by a man on a horse. In the Boer war, even though outnumbered by five to one, the Commandos, who were supported by friendly farmers, were able to

roam the *veldt* and sweep down to conduct raids. Lacking sufficient intelligence, the British could not locate the Commandos and bring them to decisive battle. This frustration led to the adoption of extreme measures including widespread brutality, a scorched earth policy, the deportation of numerous women and children to concentration camps, and the establishment of blockhouses across the countryside to restrict the movement of the Commandos. In Mao's parlance, the fish could not be found, so the sea was attacked. The Boers sued for peace, but not before thousands of non-combatants had died of disease in the camps and the country had suffered extensively.[40] The inability to find and engage the asymmetric adversary can lead to increasing brutality and, ultimately, a descent into van Creveld's vision of war.

With the introduction of air and, subsequently, space based reconnaissance, the challenge of identifying combatants in the field has been significantly improved; Predator drones and satellites would have located the Boer Commandoes more quickly than was accomplished in 1901. However, air/space reconnaissance has not been a panacea in locating insurgents and combatants.[41] Summarizing developments in Afghanistan, the US Secretary of Defence stated, "The new and the high-tech have not totally replaced the old and conventional. In Afghanistan, precision-guided bombs from the sky did not achieve optimal effectiveness until the United States placed old-fashioned boots on the ground"[42] The "old-fashioned boots" were highly trained Special Forces troops who located and provided information necessary for reconnaissance, communications and targeting.

There are a host of intelligence sources available to the operational commander including, inter alia, Signals Intelligence (SIGINT)[43], Imagery Intelligence (IMINT), and Human Intelligence (HUMINT).[44] These tools can provide key information with respect to the location and intentions of asymmetric adversaries. For example, while there is only limited information on SIGINT that creeps into the public domain, technologies such as ECHELON[45] and voice recognition software can pinpoint momentary

use of a cell phone by a targeted insurgent and provide cueing information to identify his location. It can only be assumed that the capabilities ascribed to the rather venerable ECHELON system have been exceeded significantly by its successors. There is much greater availability of information with respect to other surveillance systems and some of the technologies with application to asymmetric warfare and urban combat will now be reviewed.

Unmanned Sensors. Unmanned sensors will continue to provide a key surveillance capability across the spectrum of conflict. In peace support operations, they are critical in both supervising and interposing activities,[46] and compensate for lower friendly troop densities. For warfighting applications, especially asymmetric conflicts, they offer enhanced force protection and the ability to detect and track the activity of small groups and individuals. Current unmanned sensors are diverse in their means of operation, and encompass acoustic detection, pressure sensors, video and infrared cameras, radar and other mechanisms.[47] However, the current complaint is that they lack data fusion capabilities and often act as simple "trip wires," lacking the ability to discriminate between enemy, friendly, or non-combatants. There are a number of initiatives underway to enhance sensor performance. An example of evolving technology is the UGS (Unattended Ground Sensors) project[48] that is developing a fused and integrated sensor net that will permit dramatically enhanced detection, tracking, classification and identification of time critical targets.[49] The capabilities of video surveillance are being dramatically exploited through Artificial Intelligence. Systems currently being developed have the potential to automatically analyze video data and identify suspicious behavior by individuals or vehicles. This technology will address some of the problems confronting current video surveillance; too much data and boredom and inattentiveness on the part of personnel monitoring camera feeds.[50] The future of video surveillance is exemplified by the Combat Zones That See (CTS) project,[51] which is developing a network of, potentially, thousands of interconnected video cameras that will provide detailed

and close-in surveillance. Encompassed within this project is sophisticated, and automated, artificial intelligence technology that will permit management of the tremendous quantity of video data. The technological enhancements in data fusion and information management will dramatically enhance the ability of coalitions to undertake asymmetric warfare in the close confines of urban terrain where the ability to see around corners is pivotal.

Unmanned Aerial Vehicles (UAV). Clearly, one of the most promising areas of technology for future military surveillance lies with UAVs. US systems, such as Global Hawk and Predator have demonstrated outstanding surveillance capabilities in recent military operations in Iraq and Afghanistan through employment of their sophisticated suite of optical, infrared and radar sensors. Other nations, including Israel and Germany, have also developed sophisticated and effective UAV systems. UAV surveillance capabilities continue to be enhanced including the introduction of ground penetrating radar to locate mines[52] and enhanced radar capable of detecting personnel at long range in foliage.[53] However current UAVs experience inherent limitations in urban terrain and this has prompted the development of a family of Micro-Air Vehicles (MAVs), such as the USMC Dragon Eye – a five-pound man portable miniature aircraft capable of providing troops a view beyond the next building.[54] Considerable effort is being extended to reduce the size of MAVs to make them more suitable for urban terrain; exemplifying this development is the Black Widow, which is six inches long and weighs two ounces.[55] Yet more revolutionary is current research that is striving to develop autonomous insect like MAVs with flapping wings that will be able to negotiate stairwells and provide surveillance within buildings and tight urban confines.[56] [57]

Unmanned Ground Vehicles (UGVs). As a means of enhancing surveillance within urban terrain, extensive development effort is being committed to UGVs. Recent USMC exercises have fielded

Dragon Runner, a small remotely controlled UGV that includes a host of miniaturized sensors. [58] Dragon Runner is a conventional wheeled machine; however, future development, exemplified by the Tactical Mobile Robotics (TMR) programme,[59] will field beyond line-of-site communications and extremely compact UGVs that will be capable of insect-like crawling and wall climbing. This new generation of UGVs will serve to push the commanders field of vision into closely packed urban terrain.

Other technologies. A number of other technologies are also being developed to enhance surveillance on the modern battlefield. Ground based radar, like its airborne counterpart is being dramatically enhanced to permit identification of small groups of personnel concealed within foliage.[60] To achieve some degree of visibility as to what is going on within buildings, a man-portable through wall surveillance radar set has also been developed for urban operations; currently it can identify the presence of personnel up to a range of 10 meters through walls. Further development is underway to permit this device to identify the presence of weapons inside a building.[61] Other developments will see systems fitted to soldiers that will instantly analyze acoustic data to accurately provide information regarding the elevation and range of a sniper.[62]

While the technical gadgetry discussed above will undoubtedly enhance battlefield awareness and remove some of the cover enjoyed by adversaries engaged in asymmetric conflict, the importance of HUMINT cannot be overstated, especially for peace support operations and operations in urban terrain. Irrespective of the number of cameras in play, there will be occlusions and blind spots that can be exploited. SIGINT can be rendered far less effective by the enemy's adoption of simpler communication tools. In the comparative close confines of a city, adversaries may well adopt runners for communications, or, as in Somalia, use burning tires.[63] In this type of environment, HUMINT, which gains information from friendly forces, friendly and neutral civilians and captured adversaries,

becomes increasingly valuable. In addition to providing essential military information, HUMINT also reveals important insights into local attitudes, emotions, and the identities of key players.[64] It is of note that HUMINT is not a panacea and there are inherent risks in its employment. As exemplified in the US experience in Somalia, the use of bribery to solicit information led to highly questionable results.[65] Further, intelligence provided by informants was often distorted by the ulterior motives of Somalis who sought to gain advantage over other clans or groups.[66] However, an excellent source of HUMINT is the mutual trust engendered by the physical presence of experienced troops.[67]

Only the big fish please…..

In asymmetric warfare, there may be a small cell of insurgents in an otherwise peaceful population or the insurgency may be endemic. In the latter case, a level of surveillance granularity sufficient to identify a single individual may be necessary to isolate and identify leadership targets. Indiscriminate or excessive force could well inflame the population and impact on operational and strategic goals. "In Somalia all the gunmen could not be killed because all Somali men had guns… destroying the village to save it cannot be general policy."[68] Furthermore, accidental targeting of non-combatants or "friendlies" can have strategic consequence.[69] To illustrate the complexities of this problem, it is of note that the population of Mogadishu in 1992, nominally 500,000, had grown to as many as 1.5M due to refugees and thus the city was completely overcrowded. Infrastructure and institutions such as telecommunications and the police force had collapsed. Areas such as the Bakara market had become completely lawless and UN forces considered them too dangerous to enter.[70] The complexities inherent in locating one man, or a small group, in this urban maze are self-evident. The problems are further evidenced as one considers the long search, the resources applied, and the lack of success in finding Osama bin Laden and Saddam Hussein.

In isolating and identifying the location of specific individuals, HUMINT is a tool of tremendous

importance. Other sources may aid in this identification, especially if the target is unwise enough to use electronic communications. However, HUMINT, despite its limitations, provides a vital means in locating targets of interest. Anecdotally, most police officers explain that it is rare to solve a case solely through reliance on the modern miracles of forensics; most cases are broken when someone talks. However, one technological development that holds considerable promise in recognizing specific individuals is biometric identification.

Biometrics may be defined as "any specific and uniquely identifiable physical human characteristic, e.g., of the retina, iris, acoustic spectrum of the voice, fingerprint, handwriting, pattern of finger lengths, facial characteristics, etc., that may be used to validate the identity of an individual."[71] Encompassing a broad range of disciplines, biometrics has considerable application in domestic security, military, and commercial domains and it is developing rapidly. Given the nature of asymmetric warfare where insurgents are intermingled with non-combatants, biometric recognition provides an opportunity to definitively identify an individual at a distance through physical characteristics. DARPA, the US Defence Advanced Research Projects Agency, has initiated the Human Identification at a Distance (HID) [72] project that endeavors to provide automated human recognition through a multi-modal approach exploiting biometric face, gait, and iris characteristics. Requiring extensive video capture and data processing capability, this ambitious programme ultimately is intended to permit definitive individual recognition out to 150 meters. Biometrics has already been employed by casinos (to identify undesirables such as card counters) and its use stirs controversy. This was highlighted during Super Bowl XXXV where digital cameras scanned the crowd and 'faceprints'[73] of attendees were compared to those of known felons; nineteen offenders were identified and significant privacy concerns were voiced.[74] [75] Both the technology and legal standing[76] of biometric recognition within Canada are still evolving; however, biometrics has been recognized as one of the "top ten emerging technologies that will change the world."[77] The US Department of Defense recognizes the potential of biometrics

and has established the Biometrics Management Office within the Department of the Army; its mission is to "… coordinate the development and the institutionalization of biometric technologies for combatant commander, Services, and Agencies, to enhance Joint Service interoperability and warfighter operational effectiveness…."[78] Exploitation of biometric technology for the military could provide an opportunity to automatically identify individuals and strip away the anonymity they gain by mingling with non-combatants.

Technical innovation has become an integral component of war and is one of the key driving forces behind the enhancement of military surveillance. However, new technology will not be the panacea in confronting the challenges of asymmetric warfare. Biometrics, artificial intelligence, and UAVs may well catch "some of the fish" and restrict their activities. However, technology alone will not stop a 27-year-old woman from walking into a crowded restaurant and exploding a bomb that will kill herself and the women and children around her.[79] The operational commander will never be able to distinguish every single combatant and neutralize him or her. But, he must understand his adversary's motivations and their culture if he is to effectively wage asymmetric warfare.

IV THE "THREE BLOCK WAR"

The previous section has discussed surveillance requirements and techniques relevant to asymmetric warfare. It is now appropriate to consider the applicability of these technologies and techniques to Krulak's model of a "three block war." Again, this model depicts a situation where humanitarian, peace support, and mid-intensity conflict could all occur within a few hours and within three city blocks. Inherent in the model is the inchoate nature of urban asymmetric warfare and the inability to predict with certainty where, in the spectrum of conflict, forces will operate at any given point in time. Hence, forces deployed in the "three block war" will need to be highly reactive and flexible to function effectively throughout the continuum of operations.

Humanitarian and Peace Support Operations

The high technology RMA-type surveillance techniques explored in the previous section are not absolutely essential in all "blocks" of the "three block war." In conceptualizing a spectrum of conflict ranging from peacekeeping, through peace enforcement, to mid-intensity conflict, it is clear that the high-end RMA-type surveillance mechanisms are most relevant at the higher end of the continuum with somewhat less applicability in low intensity conflict. While peacekeeping and peace support operations will exploit high technology equipment, an excessive reliance on technology may, in fact, be counterproductive. [80] Physical presence, visibility, and HUMINT collection lie at the heart of peacekeeping missions.[81] In low intensity operations purely technical surveillance means tend to supplement HUMINT collection, as "they are no substitute for eyes and ears."[82]

However, there is technology that clearly can, and will, be exploited to support low intensity conflict. The unpredictability of the "three block war" will stress the importance of force protection. Improved capabilities arising from video surveillance and artificial intelligence based threat recognition could protect facilities and access routes from terrorism and mining. Sensor technology continues to evolve and will provide increased capability in the hands of peacekeepers. One of the most promising technologies available to support low intensity conflict is biometrics. As has been demonstrated in other areas of military intelligence, the digitization of information has been an enabler in data fusion and rapid dissemination. In the case of biometrics, the digitization of human identity will permit threats and opportunities posed by specific individuals to be identified more swiftly, with greater precision, and to be shared with coalition partners. In this manner, biometrics could effectively complement the HUMINT activities that are key to the success of these operations. While not inexpensive, these technologies are maturing rapidly in both the military and civilian domains and they are within the reach of a middle power. Finally, exploitation of ONA (Operational Net Assessment) will be necessary to provide the operational commander with the most comprehensive understanding of potential adversaries

and the environment as a whole. The necessary information and analysis generated by ONA could be provided from other coalition partners or national sources.

Mid-Intensity Conflict

As Krulak suggests, the tempo may radically shift and coalition troops theretofore performing humanitarian operations may suddenly be embroiled in bitter urban street fighting. The shift to mid-intensity conflict would result in a dramatic increase in the requirement for, and availability of, high-RMA surveillance technologies. In urban mid-intensity conflict, the US is planning to saturate the area with advanced surveillance technology to optimize situational awareness. The Center for Emerging Threats and Opportunities (CETO), which supports the US Marine Corps, articulates a vision of such surveillance employment through the so-called Reconnaissance, Surveillance and Target Acquisition (RSTA) "cloud concept." The "cloud concept" includes extremely small UGVs that would scurry into a "hide" position and link to an integrated surveillance system. Working in concert with UAVs, and potentially MAVs, this concept would give commanders a dramatically enhanced battlespace awareness extending to the interior of buildings. Technologies fielded as part of the VIVID (Video Verification of Identity) project,[83] will search predicted weapon impact areas for the presence of non-combatants to minimize collateral damage. The Affordable Moving Surface Target Engagement (AMTE) would fuse ground and air based radar systems to identify and locate vehicles flushed out of hiding.[84] Fusing this tremendous volume of data and disseminating it in a useful form would be the function of the Advanced ISR Management (AIM) project, which will incorporate next-generation information processing and data collection architecture.[85] [86] Overlaying this system-of-systems is ONA that will provide continuous, and fused, knowledge generated by multiple agencies, both military and civilian. The overall intent of all these technologies and processes is to gain information dominance, a rapid decision cycle, and clarity on the battlefield, thereby conducting urban combat with minimal own losses and collateral damage.

As can be seen, this vision of urban conflict dramatically pushes the technological envelope and, in the near future, can only be the domain of the US. No other nation has the economic and military clout to realize it. However, the consequences of engaging in mid-intensity urban conflict without information dominance are not welcoming. While, admittedly, there were systemic problems in the Russian forces, the battles in Chechnya and Grozny clearly revealed the costs of battling a militarily inferior, but determined, enemy in urban terrain. The tactics employed by both Russians and Chechens in Grozny would have been familiar to a Stalingrad veteran and the heavy Russian losses led to increasing brutality and an ever-shrinking regard for collateral damage and civilian casualties. In 2000, the Russians entered Komsomolskoye; by the end of the battle, which saw widespread, and indiscriminate, shelling and bombing there was little of the village left standing.[87] The bitterness engendered by military action in Chechnya has led to terrorist attacks in Moscow, suicide bombers, and a campaign that seemingly has no end. Russian forces clearly had a strong material advantage; however, they could not “find and fix” the Chechens who would melt away after each ambush.

V. THE ROAD AHEAD – CANADA AND SURVEILLANCE

With respect to the RMA, technology, and surveillance capabilities, Canada is at a crossroads. While this country has demonstrated the ability to work in coalition and has shown excellence in peacekeeping and peace support missions, there is clearly a gap developing between ourselves and the US with respect to information and surveillance technology. Given the interrelationship between levels of conflict, the unpredictability of asymmetric warfare, and the requirement for RMA-type surveillance capability discussed above, this “information gap” could have considerable impact on military capability in a US led coalition. To whit, Canada could become incapable of participating in mid intensity combat operations because of the lack of RMA-type technology and infrastructure required to fit into the operational decision cycle that is being put in play by the US.

Prior to addressing options for the future, it is relevant to assess Canada's current capabilities applicable to asymmetric warfare and the "three block war."

- Canadian soldiers are extremely well trained, and by dint of a high operational-tempo, they are very experienced in deployed operations and low-intensity conflict. As such, there is a tremendous degree of expertise in the collection and management of overt HUMINT gained within theatre.

- For the collection of covert HUMINT, Canada is significantly constrained. The CSIS (Canadians Security Intelligence Service) Act gives CSIS the power to collect covert "security intelligence" (relating to direct threats to Canada) abroad; however, collection of "foreign intelligence" (broader intelligence that may not relate to a direct threat to Canada) can only be obtained within Canada.[88] As such, most covert intelligence has to be obtained from allies. This restriction has often been assessed as a weakness and has prompted periodic calls for the establishment of a foreign intelligence service. This debate may well be revisited in light of CSIS's recent announcement that they have been conducting extensive foreign covert intelligence gathering operations.[89]

- Canada has existing capabilities with respect to advanced surveillance. Canadian troops employ the HERMES system of remote sensors,[90] they have recently introduced the French Sperwer UAV for operations in Afghanistan,[91] and they operate the state of the art COYOTE vehicle. Further, the ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) project will focus on integration of current sensors, fusion of geomatic and weather information, and procurement of new systems such as counter-battery radar and UAVs. While this will not represent the wholesale enhancements sought

through the US RMA surveillance programmes, ISTAR will enhance data fusion and improve the understanding of the battlespace.

- The conduct of R&D (Research and Development) faces significant limitations in this country. Specifically, government spending on R&D is comparatively low, fifteenth amongst the countries of the OECD[92] and, as a percentage of GDP, the US spends twice as much as Canada on R&D.[93] Furthermore, due to a number of factors, Canadian industry tends to devote less funding to R&D than most of our foreign competitors. On a positive note, Canadian companies demonstrate strength in telecommunications, a key enabler to the RMA, and the Canadian Forces has a coordinated research strategy.[94] However, increased spending in R&D will be required to develop significant organic RMA-type surveillance capabilities.

- In regard to the employment of Operational Net Assessment (ONA), Canada is working closely with the US through current experimentation and participation in USJFCOM[95] Multinational Limited Objective Experiment two (MN-LOE2) wherein the concepts of ONA are being tested on a multinational basis with participation by the US, Canada, and a number of Western allies. This development will test procedures and technology necessary to share and contribute to the CROP.

- Finally, Canada's remarkable cultural diversity provides an outstanding resource that could be tapped to support ONA within this country. The "Canadian mosaic" includes a tremendous number of cultures and languages, and this diversity could be capitalized upon to provide an essential understanding of the background and motivation of future adversaries.

In consideration of the way ahead for the development of surveillance capabilities in Canada, the following options are available.

- First, maintain the status quo and continue with upgrades to existing systems and the planned introduction of ISTAR. Given the cost of these capabilities, this is not an insubstantial undertaking and it is clear that investment must be made or the question of engagement in other than benign environments will become moot.[96]

- Second, develop organic RMA-type technology that provides the tools necessary for mid intensity conflict. While posed as an alternative, Canada's limited defence budget and constraints in R&D preclude this from being feasible in the near term.[97]

- Third, develop technologies and doctrine that will enable Canada to "plug in" to a US led coalition and work off a US generated Common Relevant Operating Picture (CROP). Achieving interoperability is not an insignificant complexity; however, this approach avoids the cost of developing organic high-level RMA-type information collection and data fusion technology. The technology requirements needed to "plug in" to a US led coalition are far more achievable and are within the reach of Canada. It is of note that the Canadian Navy has achieved a substantial degree of interoperability with the US Navy through employment of commercial equipment and innovation.

The consequences arising from a decision to simply maintain the status quo will be telling and may determine relevance. Fighting the "three block war" against asymmetric opponents means that one's forces must be capable of rapidly shifting missions across the spectrum of conflict with limited warning.

A rapid shift to mid-intensity conflict in the "three block war" has a concomitant demand for immediate access to high-level RMA-surveillance technology. Without this technology, forces will be confronted with urban combat and a highly constrained awareness of the battlespace. This will inexorably result in increased casualties and a high risk of inflicting collateral damage. As such, Canada will be restricted in its ability to function effectively in the "three block war"; forces will not have the intrinsic battlespace awareness, and nor will they have the ability to "plug in" and operate within the reduced decision cycle that will be employed by a US led coalition. As such, Canadian troops would not be able to assume all combat roles within the coalition, but rather, they would potentially be relegated to roles with less risk and could well be marginalized.

Developing the technology to "plug in" to a US led coalition, at first blush, provides substantial benefits; most notably, it makes it possible to operate across the spectrum of conflict. However, there are clearly some limitations. Simply "plugging in" will mean that Canadian troops would receive the fused US ONA reflecting US diplomatic, military, and political objectives and values. Our two nations share great commonality; however, we have differing security objectives and national values that result in differences in the way that the two nations engage the world. We are signatories to different treaties, our interpretation of aspects of the Law of Armed Conflict varies, and our perceptions of national threats differ. This can lead to substantial variance in fundamental concepts such as who, or what, constitutes a legal combatant. US leaders assert, "Prevention and sometimes even pre-emption are necessary to effectively defend the United States… [and] … for a persuasive deterrent, the United States must lean forward, not back."[98] Thus, the fused CROP would reflect US strategic objectives that could vary from those of Canada. These strategic objectives will be transformed into tactical missions through an extremely rapid RMA-driven decision cycle. Therefore, without sufficient and suitable national input, Canada may lose a certain degree of freedom of action and could be constrained to the degree to which it can serve distinct Canadian objectives.[99]

The 1994 White Paper articulates that Canadians will be able to fight "alongside the best, against the best" and indicates that it would be misguided to invest in low-end capabilities such as forces only capable of undertaking low-risk peacekeeping activities.[100] Strategy 2020, is more guarded in its direction however, it provides for "modernization … particularly in the areas of information and sensing … global deployability… and ensuring Canadian and US forces are inter-operable and capable of combined operations in key selected areas."[101] The CDS Annual Report for 2003 reinforces the need to be able to address asymmetric threats, enhance C4ISR[102] capabilities, and generate "lethal forces that are relatively easy to deploy, [and] can operate in the most hostile and demanding operational theatres…"[103] Given this guidance, and considering the substantial difference in surveillance requirements between low and mid intensity conflict, it is now relevant to render recommendations with respect to the way ahead for surveillance capabilities in Canada.

- Canada requires a coherent overarching strategy with respect to the future of the RMA in this country. This strategy would provide clear R&D objectives as well as intended procurement and experimentation. While recent strategic direction has addressed the issue to some extent, the strategy is not depicted as clearly as it is in other allied countries.[104]

- Development of doctrine and the technical capability necessary to maintain interoperability with the US for mid-intensity conflict must be developed. In doing so, the constraints arising from the decision to "plug in" to the US picture must be fully understood; specifically, the fact that Canadian troops will be operating under extremely short decision cycles and working off a US generated CROP. This CROP, given the nature by which it is generated will largely represent US strategic objectives and analysis. Doctrine or organizational constructs may be able to ensure that Canadian strategic goals are represented; however, when the conflict suddenly changes to mid-intensity conflict and weapons are in the

air, there will be little time for discussion or proffering of the "national red card." As such, Canada may have to become far more selective in the missions to which Canadian Forces are dispatched.

- In the development of national RMA-type surveillance capabilities, Canada should play to its strengths and focus on the requirements necessary to support peacekeeping and peace support operations.

- From a technical programme perspective, investment in surveillance capabilities should be focused on those suitable for interoperability with the US as well as systems supporting force protection and low-intensity conflict. Such technology will enhance Canada's ability to function unilaterally or in non-US led coalitions within low-intensity conflict environments. Interoperability will permit Canada to contribute effectively to a US-led coalition engaged in mid-intensity and urban conflict. Some relevant technologies suggested for development include UAVs, unmanned sensors, video surveillance and biometrics. Further, technology to support effective dissemination of information must be employed, as information overflow and under use can be highly detrimental.

- A durable Canadian ONA process is required to ensure that Canadian commanders will have the best possible understanding of their adversary, and incorporate relevant political, military, and cultural factors into decision making. The Canadian ONA process would need to span different coalition requirements and levels of conflict. Specifically, in non-US led coalitions (focused on low-intensity operations) there may be limited input from allies and the Canadian net assessment process would have to provide considerable independent analysis. In a US-led coalition engaged in mid-intensity and urban conflict, the process would have to be "plugged in" to the US system to contribute to analysis and also reflect Canadian values and

objectives. The need for interoperability of these processes underlines the importance of experimentation such has been conducted as part of the USJFCOM MN-LOE2 trials. The key requirement for the Canadian ONA process will be to fuse input from military planners, federal departments, civilian agencies, non-governmental organizations, and other nations; the process will also have to achieve stronger inter-departmental cooperation than has heretofore been the case.[105] Of note, this expertise clearly does not have to reside in the operational headquarters given the reach-back capabilities that have been fielded.

Technological advances will certainly aid in surveillance; however, cameras and computers will never be able to definitively identify every threat; there are too many fish and the sea is too big. Asymmetric war is about will, patience, and perseverance, not necessarily assets or military strength; one man with a rocket launcher can achieve strategic effects.[106] As surveillance and technology will not be a panacea, it is absolutely essential that the operational commander understand the will, motivation, and cultural heritage of the enemy. Failure to do so, and the employment of ill-judged or ineffective countermeasures can lead rapidly to a bloody and endless conflict in which classical military strength is meaningless. The genius sought in the operational art may well be the commander who realizes that there is no military solution.

VI. CONCLUSION

While conventional warfare will still occur, it is clear that any US led coalition must be prepared to confront asymmetric threats and operate effectively within the “three block war.” Most adversaries will clearly recognize US conventional military dominance and will likely seek the protection of urban terrain while attacking coalition weaknesses using insurgency and terror. Furthermore, coalitions will need to be capable of performing peacekeeping and humanitarian support to renew order. To confront the challenges inherent in the “three block war,” new technology and practices are being optimized to

find and track small groups and individuals who mingle with non-combatants.

The spectrum of conflict encompassed by the “three block war” will demand varying degrees of surveillance. Mid-intensity urban conflict will require an extremely robust capability to avoid the high casualties and extensive collateral damage that is typical for this type of combat. The comprehensive suite of RMA-type surveillance technologies needed to undertake mid-intensity urban conflict is beyond the reach of Canada to develop unilaterally. The surveillance requirements for low-intensity conflict and peacekeeping are not insignificant, but are less demanding than those required for mid-intensity conflict. As such, Canada should focus its attention on developing interoperability with the US as well as developing organic surveillance capabilities focused on peacekeeping and low-intensity conflict. Thereby, while Canada will be able to operate with a variety of allies in peacekeeping operations and low-intensity conflict, this country will engage at the higher end of the conflict continuum when “plugged in” to a US led coalition.

An overarching consideration; however, is that technology alone will never provide the complete solution. Asymmetric conflict is about will and is fought by individuals. Every adversary cannot be definitively identified and they cannot all be found. Thus, the need to understand the cultural, military, and political motivations of the asymmetric adversary will be critical. Leveraging the knowledge and information of allies, other federal departments, non-governmental organizations, and other agencies through a process of Operational Net Assessment will be a key factor in gaining the advantage and avoiding a Hobbesian descent into terrorism and insurgency.

Bibliography

Altamann, Jurgen, Horest Fischer, and Henny van der Graf. *Sensors for Peace.* New York and Geneva: United Nations, 1998.

Bell, J. Bowyer. *Dragonwars: Armed Struggle &the Conventions of Modern War.* New Bunswick (USA): Transaction Publishers, 1999.

Bell, Stewart. “CSIS admits to spying abroad,” *The National Post.* 21 October 2003: available

from http://www.nationalpost.com/utilities/story.html?id=F4A8E979-0CDC-40E1-B416-AEB0DC995FE0; accessed 22 October 2003.

Canada, Office of the Privacy Commissioner of Canada. *The 2002-2003 Annual Report to Parliament by the Privacy Commissioner of Canada. Ottawa; available from* http://www.privcom.gc.ca/information/ar/02_04_11_e.asp; accessed 7 Oct 03.

Canada, Department of National Defence, *1994 Defence White Paper.* Ottawa: Canadian Communications Group, 1994; available from http://www.forces.gc.ca/site/Minister/eng/94wpaper/three_e.html; accessed 16 October 2003.

Canada, Department of National Defence. *Strategy 2020.* Ottawa: Chief of Defence Staff, 1999; available from http://www.cds.forces.gc.ca/pubs/strategy2k/s2k06_e.asp#1; accessed 6 Oct 03.

Canada, Department of National Defence. *Chief of the Defence Staff Annual Report 2002-2003.* Ottawa: Chief of the Defence Staff, 2003; available from http://www.cds.forces.gc.ca/pubs/anrpt2003/capabilities_e.asp; accessed 20 Oct 03.

Canada, Department of National Defence. B-GL-357-001/FP-001 *Land Forces Information Operations Field Manual Intelligence.* Ottawa: DND Canada, 2001.

Canada, Department of National Defence. *Dispatches Vol. 8 No. 1 HUMINT During Peace Support Operations.* Ottawa: DND Canada, 2001.

Charters, Dr. David. "The Future of Military Intelligence within the Canadian Forces," *Canadian Military Journal.,* Winter 2001-2002: 46 – 52.

Collins, Richard. *The sound and the fury: an account of the Indian mutiny.* London: Collins, 1965.

Cooling, Norman. "Operation RESTORE HOPE in Somalia: A tactical action turned strategic defeat," *Marine Corps Gazette.*, Vol. 85 Iss. 9: 92-107.

Czerwinski, T.J. "Asymmetrical Threats," *Marine Corps Gazette.* Vol 3 Iss. 4 (1999): 88 - 90.

Dupont, Alan. "Transformation or stagnation? Rethinking Australia's defence." *Australian Journal of International Affairs,* Vol. 57, No. 1 (2003): 55 – 76.

Fahey, Jonathan. "We See You," *Forbes.com;* available from www.forbes.com/free_forbes/2001/1015/052.html ; accessed 7 Oct 03.

Fulghum, David A. "Conflict's New Phase Exposes Old Problems," *Aviation Week & Space Technology.* Vol. 155 Issue 21: 41-44.

Garfield, Andrew. "Information Operations as an Integrating Strategy: the Ongoing Debate," *Cyberwar 3.0.* Fairfax Virginia: AFCEA International Press, 2000.

Gongora, Thierry and von Riekhoff editors. *Towards a Revolution in Military Affairs,* Contributions in Military Studies, Number 197. Westport, Connecticut: Greenwood Press, 2000.

Henrichon, Patrick. "Protecting the Canadian Forces against asymmetric threats," *Canadian Military Journal.* Winter 2002-2003: 9-14.

Hibbert, Lee. "Researchers get into a flap," *Professional Engineering.* Vol .14, Iss. 10: 24-25.

Huber, Thomas. "Napoleon in Spain and Naples – Fortified Compound Warfare," *Combat Studies Institute- Fort Leavenworth Kansas;* available from www-cgsc.army.mil/csi/research/ComWar/ comwarhuber.asp; accessed 25 Sep 03.

Krulak, General Charles. "The Three Block War – Fighting in Urban Areas," *Vital Speeches of the Day.* Vol. LXIV, No. 5 (1997): 139 – 141.

Lambakis, Steven, James Kiras and Kristin Kolet. "Understanding "Asymmetric" Threats to the United States." *Comparative Strategy*, Vol. 21 (2002): 241 – 277.

Metz, Steven. *Armed Conflict in the 21st Century: The information revolution and Post-Modern Warfare.* Carlisle Barracks, Penn: Strategic Studies Institute, April 2000.

Mooney, Paul. "Army acquires first in fleet of drones," *The Canadian Army* [journal on-line].September 2003; available from http://www.army.dnd.ca/LF/English/6_1_1.asp?id=54; accessed 14 October 2003.

Oliker, Olga. *Russia's Chechen Wars.* Arroyo Center: RAND, 2001.

"Reforging the Sword: Forces for a 21st Century Security Strategy," CDI Military Reform Project; available from http://www.cdi.org/; accessed 24 Sep 03.

Richelson, Jeffrey. "Desperately Seeking Signals," *The Bulletin of the Atomic Scientists.* Mar/Apr 2000: 47 – 51.

Richter, Andrew. *The Revolution in Military Affairs and its Impact on Canada: The Challenge and the Consequences.* Working Paper No. 28. Vancouver: Institute of International Relations, The University of British Columbia, March 1999.

Richter, Andrew. *Canadian Research and Development (R&D.* Vancouver B.C.: Institute of International Relations, University of British Columbia; available from http://www.ccs21.org/ccspapers/papers/richter-r_d.htm; accessed 21 October 2003.

Roos, John. “WarBots,” *Armed Forces Journal International.* Vol. 139 Iss. 4: 3 p.

Russell, Peter. “CSIS: Only in Canada?” *The Ottawa Citizen*, November 12 1989: A-8.

Scales, Major-General Robert H. Jr. *Future Warfare*. Carlisle Barracks, Penn: US Army War College, 1999.

Seely, Robert. *Russo-Chechen Conflict 1800-2000 – A deadly embrace.* London: Frank Cass, 2001.

Stanton, Martin. ”Task Force 2-87: Lessons from RESTORE HOPE,” *Military Review.* September 1994 Volume 74 Issue 9: 35- 42.

Stix, Gary. “Sounding out Snipers,” *Scientific American.* Vol. 285, Iss. 1 (2001): 33.

Sun Tzu - translated by Lionel Giles (1910); accessed from www.chinapage.com/sunzi-e; 3 Oct 03.

Sun-Tzu. *The Art of War,* trans.and ed. Samuel Griffith. London: Oxford University Press, 1963.

Thompson, Robert. *Defeating Communist Insurgency*. London: Chatto & Windus, 1974.

“Time Domain through-wall surveillance radar aids in counter-terrorism and urban warfare.” *Military and Aerospace Electronics.* Vol. 12 Iss. 12 (2001): 1-3.

Tiron, Roxana. “Urban exercise tests new technology,” *National Defense.* Vol 87, Iss. 588: 62-65.

United States, Department of Defense. *Fiscal 2004 Department of Defense Budget Release;* available from http://www.defenselink.mil/news/Feb2003/b02032003_bt044-03.html; accessed 2 Oct 03.

United States. Department of Defense. *Quadrennial Defense Review Report.* Washington, D.C.: U.S. Government Printing Office, September 30, 2001; available from www.defenselink.mil/pubs/qdr2001.pdf; accessed 3 October 2003.

United States, Department of Defense, “Annual Report to the President and Congress – 2002”; available from www.defenselink.mil/execsec/adr2002; accessed 1 Oct 03.

United States, Department of Defense. *Biometric Management Office, BMO Mission Statement;* available from http://www.defenselink.mil/nii/biometrics/; accessed 7 Oct 03.

United States, DARPA Defence Advanced Research Projects Agency – Information Awareness Office; available from http://www.darpa.mil/; accessed 19 Sep 03.

United States, DARPA Defence Advanced Research Projects Agency – Information Exploitation

Office; available from http://www.darpa.mil/; accessed 1 Oct 03.

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

Van Creveld, Martin. *Technology and War*. New York: The Free Press, 1989.

Vest, Jason. "The Army's Empire Skeptics," *Nation.* Vol. 276 Issue 8: 27 – 30.

Woodward, John D. Jr. *Super Bowl Surveillance – Facing up to Biometrics.* Arroyo Center: RAND Arroyo Center, 2001.

---

[1] Asymmetric warfare may be defined as "means or tactics employed by states, terrorist groups or individuals to carry out attacks on a superior opponent while trying to avoid direct confrontation. The attacks will seek to circumvent the adversary's advantages or exploit its weaknesses." From - Patrick Henrichon, "Protecting the Canadian Forces against asymmetric threats," *Canadian Military Journal*, Winter 2002-2003: 9.

[2] RMA – defined by Andrew Marshall, Director of the Office of Net Assessment "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 organizational concepts, fundamentally alters the character and conduct of military operations" from Thierry Gongora and Harald von Riekhoff, *Toward a Revolution in Military Affairs?* (Westport, Conn.: Greenwood Press, 2000), 2.

[3] General Charles Krulak, "The Three Block War – Fighting in Urban Areas," *Vital Speeches of the Day.* Vol. LXIV, No. 5 (1997), 140.

[4] Andrew Richter. *The Revolution in Military Affairs and its Impact on Canada: The Challenge and the Consequences*. Working Paper No. 28 (Vancouver: Institute of International Relations, The University of British Columbia, March 1999), 3.

[5] United States. Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C.:U.S. Government Printing Office, September 30, 2001); available from www.defenselink.mil/pubs/qdr2001.pdf. Accessed 3 October 2003, p. 4.

[6] Steven Lambakis, James Kiras, and Kristin Kolet, "Understanding "Asymmetric" Threats to the United States," *Comparative Strategy* 21 (2002): 243.

[7] Andrew Richter, *The Revolution in Military Affairs…, 71.*

[8] Lambakis, Kiras, and Kolet, *Understanding "Asymmetric" Threats. . . ,* 245.

[9] Thierry Gongora and Harald von Riekhoff, *Toward a Revolution in Military Affairs?* (Westport, Conn.: Greenwood Press, 2000), 15.

[10] United States, Department of Defense, *Fiscal 2004 Department of Defense Budget Release;* available from http://www.defenselink.mil/news/Feb2003/b02032003_bt044-03.html; accessed 2 Oct 03.

[11] Steven Metz, *Armed Conflict in the 21st Century: The information revolution and post-modern warfare,* (Carlisle Barracks, Penn.: U.S. Army War College Strategic Studies Institute, 2000), 21.

[12] MG Robert H. Scales Jr., *Future Warfare* (Carlisle Barracks, Penn.: U.S. Army War College Strategic Studies Institute, 1999), 47.

[13] Steven Metz *Armed Conflict in the 21st Century…,* 22

[14] Sun Tzu - translated by Lionel Giles (1910); accessed from www.chinapage.com/sunzi-e; 6 Oct 03.

[15] MG Robert H. Scales Jr., *Future Warfare…,* 48.

[16] Lambakis, Kiras, and Kolet, *Understanding "Asymmetric" Threats. . . ,* 244-246.

[17] T.J. Czerwinski, "Asymmetrical Threats," *Marine Corps Gazette* 83 Iss. 4 (1999): 88.

[18] The Canadian doctrinal equivalent to MOUT is FIBUA (Fighting In Built Up Areas)

[19] T.J. Czerwinski, "Asymmetrical Threats," *Marine Corps Gazette* 83 Iss. 4 (1999): 100.

[20] General Charles Krulak, "The Three Block War – Fighting in Urban Areas," *Vital Speeches of the Day.* Vol. LXIV, No. 5 (1997), 140.

[21] Department of National Defence, B-Gl-300-002/FP-000 *Land Forces Tactical Doctrine Volume 2* (Ottawa: DND Canada, 1997) 8-7.

[22] Sun-Tzu, *The Art of War*, trans.and ed. Samuel Griffith (London: Oxford University Press, 1963), 78.

[23] Olga Oliker, *Russia's Chechen Wars 1994-2000: Lessons from Urban Conflict* (Arroyo Center: RAND, 2001), 86.

[24] Norman Cooling, "Operation RESTORE HOPE in Somalia: A tactical action turned strategic defeat." *Marine Corps Gazette*, 85 Iss. 9 (Sep 2001); accessed from Proquest p. 2/19

[25] Ibid, p.9/19

[26] Krulak, General Charles. "The Three Block War – Fighting in Urban Areas", *Vital Speeches of the Day*. Vol. LXIV, No. 5 (1997) p 139

[27] MG Robert H. Scales, Jr. *Future Warfare*, 203.

[28] Martin van Creveld, *The Transformation of War* (New York: The Free Press, 1991) 212.

[29] Andrew Garfield "Information Operations as an Integrating Strategy: the Ongoing Debate," *Cyberwar 3.0,* (Fairfax Virginia AFCEA International Press 2000) 270.

[30] A Somali proverb is illustrative – Me and Somalia against the World, me and my clan against Somalia, me and my family against the clan, me and my brother against my family, me against my brother.

[31] Norman Cooling, *Operation Restore Hope in Somalia* …, p. 14/19

[32] Ibid p. 8/19

[33] Olga Oliker, *Russia's Chechen Wars 1994-2000…,* 8.

[34] Robert Seely, *Russo-Chechen Conflict 1800-2000 – A deadly embrace* (London: Frank Cass, 2001) 9.

[35] Richard Collins, *The sound and the fury: an account of the Indian mutiny* (London: Collins, 1965), 86..

[36] Computerized and automated translation tools are being developed under both commercial and military auspices.

[37] Dr. David A. Charters, "The Future of Military Intelligence within the Canadian Forces," *Canadian Military Journal,* Winter 2001-2002, p. 52.

[38] "Joint experiment will test information linkage concept"; accessed from http://www.jfcom.mil/; 2 Oct 03.

[39] US Joint Forces Command

[40] F. Pretorius. "The Experience of the Bitter-ender Boer in the Guerilla Phase of the South African War" *The Boer War*,. ed. John Gooch (London: Frank Cass, 2000), 179.

[41] It is of note that a wealth of aerial and space-based platforms was unable to locate Iraq's SCUD missile launchers during the first Gulf war. However, as observed in the referenced article, considerable capability enhancement has been achieved in the intervening years. Jonathan Fahey, "We See You," *Forbes.com;* accessed from www.forbes.com/free_forbes/2001/1015/052.html ; 7 Oct 03.

[42] United States, Department of Defense, "Annual Report to the President and Congress – 2002" Chapter 3; accessed from www.defenselink.mil/execsec/adr2002; 1 Oct 03.

[43] SIGINT is comprised of Communications Intelligence (COMINT) and Electronic Intelligence (ELINT)

[44] Department of National Defence, B-GL-357-001/FP-001 *Land Forces Information Operations Field Manual Intelligence* (Ottawa: DND Canada, 2001), 8.

[45] ECHELON in a telecommunications intercept system that searches public telecommunications networks for specified keywords. Jeffrey Richelson, "Desperately Seeking Signals" *The Bulletin of the Atomic Scientists,* Mar/Apr 2000: 47 – 51.

[46] Jurgen Altmann, Horst Fischer and Henny van der Graaf, *Sensors for Peace: Applications, Systems and Legal Requirements for Monitoring in Peace Operations,* (New York and Geneva: United Nations, 1998), 20.

[47] Ibid, p. 71

[48] United States, Defense Advanced Research Projects Agency, Information Exploitation Office, *Unattended Ground Sensors;* accessed by http://dtsn.darpa.mil/; 1 Oct 03.

[49] Programme objectives are to provide for a 70% detection rate out to 3000 yards and, within 500 yards, achieve a classification rate of 85% with targeting precision of 20 meters – significantly in excess of current capability.

[50] Martin van Creveld, *The transformation of war…,* 211.

[51] United States, Defense Advanced Research Projects Agency, Information Exploitation Office, *Combat Zones that See;* accessed by http://dtsn.darpa.mil/; 1 Oct 03.

[52] Jonathan Fahey, "We See You," *Forbes.com;* accessed from www.forbes.com/free_forbes/2001/1015/052.html ; 7 Oct 03.

[53] For, example, the FORESTER project is developing FOPEN (Foliage Penetrating) radar capable of detecting dismounted personnel and vehicles out to 30 kilometers in foliage. United States, Defense Advanced Research Projects Agency, Information Exploitation Office, *FORESTER project;* accessed by http://dtsn.darpa.mil/; 1 Oct 03

[54] John G. Roos, "WarBots," *Armed Forces Journal International,* 139 Iss. 4: 3.

[55] "30 Minute Black Widow Flight", DARPA TTO office; available from www.darpa.mil/dso/thrust/matdev/palmpower/presentations/wilson_part2.pdf; accessed 20 October 2003.

[56] Lee Hibbert, "Researchers get into a flap," *Professional Engineering,* 14, Iss. 10: 24-25

[57] Necessary supporting technology is the development of miniaturized power sources – current developments in microelectromechanical systems (Mems) have yielded thrusters a quarter of the size of a penny and MIT is developing Mems based gas turbine engines measuring 1 cm in diameter and 3 mm thick

[58] Roxana Tiron, "Urban exercise tests new technology," *National Defense,* 87, Iss. 588: 62-65.

[59] United States, Defense Advanced Research Projects Agency, Information Exploitation Office, *Tactical Mobile Robotics;* accessed by http://dtsn.darpa.mil/; 1 Oct 03.

[60] One such system under development is the Organic GMTI Radar, which will support Force Protection, and other missions, through detection and tracking of moving vehicles and personnel at long range in complex terrain. United States, Defense Advanced Research Projects Agency, Information Exploitation Office, *Organic GMTI Radar;* accessed by http://dtsn.darpa.mil/; 1 Oct 03.

[61] "Time Domain through-wall surveillance radar aids in counter-terrorism and urban warfare." *Military and Aerospace Electronics.* 12 Iss. 12 (2001): 1-3.

[62] Gary Stix, "Sounding out Snipers," *Scientific American,*.285, Iss. 1 (2001): 33.

[63] Norman Cooling, *Operation Restore Hope in Somalia …,* p. 14/19

[64] Department of National Defence, *Dispatches Vol. 8 No. 1 HUMINT During Peace Support Operations,* (Ottawa: DND Canada, 2001), 3.

[65] Norman Cooling, *Operation Restore Hope…,* p 13/19.

[66] Martin Stanton, ""Task Force 2-87: Lessons from RESTORE HOPE," *Military Review,* September 1994 Volume 74 Issue 9, 41.

[67] Department of National Defence, *Dispatches Vol. 8 No. 1 HUMINT During Peace Support Operations,* (Ottawa: DND Canada, 2001).

[68] J. Bowyer Bell, *Dragonwars: Armed Struggle &the Conventions of Modern War,* (New Bunswick (USA): Transaction Publishers, 1999), 422-423.

[69] In Somalia poorly planned US operations that resulted in the capture of UN workers and the arrest of Somali Genera Ahmen Jilao, a close UN ally being groomed to lead the Somali police force were high profile errors that had significant impact on the operation. From Norman Cooling, *Operation Restore Hope in Somalia …,* p. 7/19.

[70] Norman Cooling, *Operation Restore Hope in Somalia …,* p 8/19.

[71] http://www.atis.org/tg2k/_biometric.html; accessed 7 Oct 03.

[72] United States, Defense Advanced Research Projects Agency, Information Awareness Office, *Human Identification at a Distance;* accessed by http://dtsn.darpa.mil/; accessed 19 Sep 03 – since removed.

[73] A "faceprint" is generated through scanning the individual's face and using algorithms to measure distances and angles separating geometric points on the face – for example mouth extremities, nostrils, corners of the eye, etc. From John D. Woodward, *Superbowl Surveillance – Facing up to Biometrics*, (Arroyo Center: RAND, 2001), 3.

[74] John D. Woodward, *Superbowl Surveillance – Facing up to Biometrics*, (Arroyo Center: RAND, 2001), 3 – 15.

[75] It is of note that the entire DARPA IAO web page has recently been removed from the public domain and is no longer readily accessible. .

[76] The Privacy Commissioner of Canada has expressed concern with respect to the widespread implementation of this technology. Further information may be found at http://www.privcom.gc.ca/information/ar/02_04_11_e.asp - the 2002-2003 Annual Report to Parliament by the Privacy Commissioner of Canada.

[77] Stated in the 2001 MIT Technology Review per John D. Woodward, *Superbowl Surveillance… ,* p. 4.

[78] United States, Department of Defense, *Biometric Management Office. BMO Mission Statement;* available from http://www.defenselink.mil/nii/biometrics/; accessed 7 Oct 03.

[79] 27-year-old Hanadi Tayseer Jaradat, a lawyer from Jenin, entered the Maxim restaurant in Haifa and exploded a shrapnel laden bomb that was wrapped around her waist; she was not a known terrorist, however, she was avenging the deaths of relatives killed by Israeli troops. The attack killed 19 civilians and has had strategic consequence in the Middle East, prompting an air attack on a training camp within Syria.

[80] Dr. David A. Charters, *The Future of Military Intelligence within the Canadian Forces…,* 51.

[81] Andrew Richter, *The Revolution in Military Affairs…, 42.*

[82] Dr. David A. Charters, *The Future of Military Intelligence within the Canadian Forces*, 51.

[83] United States, Defense Advanced Research Projects Agency, Information Exploitation Office, *VIVID;* accessed by http://dtsn.darpa.mil/; 1 Oct 03.

[84] United States, Defense Advanced Research Projects Agency, Information Exploitation Office, *ASTE;* accessed by http://dtsn.darpa.mil/; 1 Oct 03.

[85] United States, Defense Advanced Research Projects Agency, Information Exploitation Office, *AIM;* accessed by http://dtsn.darpa.mil/; 1 Oct 03.

[86] A flood of information can potentially overwhelm even the best decision maker. It is of note that during the Three Mile Island nuclear disaster, the highly knowledgeable and skilled operator was confronted with hundreds of alarms and reams of information – so much so that he could not deduce the root cause of the problem and take necessary action.

[87] Olga Oliker, *Russia's Chechen Wars …,* 79.

[88] Peter H. Russell, "CSIS: Only in Canada?" *The Ottawa Citizen,* November 12 1989: A-8.

[89] Stewart Bell, "CSIS admits to spying abroad," *The National Post,* 21 October 2003: available from http://www.nationalpost.com/utilities/story.html?id=F4A8E979-0CDC-40E1-B416-AEB0DC995FE0; accessed 22 October 2003.

[90] Jurgen Altmann, Horst Fischer and Henny van der Graaf, *Sensors for Peace…*, 10.

[91] Paul Mooney, "Army acquires first in fleet of drones," *The Canadian Army* [journal on-line], Septermber 2003; available from http://www.army.dnd.ca/LF/English/6_1_1.asp?id=54; accessed 14 October 2003.

[92] Organization for Economic Cooperation and Development

[93] Andrew Richter, *Canadian Research and Development (R&D)* (Vancouver B.C.: Institute of International Relations, University of British Columbia); available from http://www.ccs21.org/ccspapers/papers/richter-r_d.htm; accessed 21 October 2003.

[94] Ibid.

[95] US Joint Forces Command

[96] Andrew Richter, *The Revolution in Military Affairs.. ,* 49.

[97] Ibid p. 71

[98] United States, Department of Defense, "Annual Report to the President and Congress – 2002" Chapter 1; accessed from www.defenselink.mil/execsec/adr2002; 6 Oct 03.

[99] Dr. David A Charters, *The Future of Military Intelligence within the Canadian Forces,* p. 49

[100] Department of National Defence, *1994 Defence White Paper* (Ottawa: Canadian Communications Group, 1994) Chapter 3; available from http://www.forces.gc.ca/site/Minister/eng/94wpaper/three_e.html; accessed 16 October 2003.

[101] Department of National Defence, *Strategy 2020* (Ottawa: Chief of Defence Staff, 1999); available from http://www.cds.forces.gc.ca/pubs/strategy2k/s2k06_e.asp#1; accessed 6 Oct 03.

[102] Command, control, communications, computers, intelligence, surveillance, and reconnaissance

[103] Department of National Defence, *Chief of the Defence Staff Annual Report 2002-2003* (Ottawa: Chief of the Defence Staff, 2003); available from http://www.cds.forces.gc.ca/pubs/anrpt2003/capabilities_e.asp; accessed 20 Oct 03.

[104] Andrew Richter, *The Revolution in Military Affairs.. , 71.*

[105] Andrew Richter, *The Revolution in Military Affairs.. , 71.*

[106] J. Bowyer Bell, *Dragonwars: Armed Struggle &the Conventions of Modern War…*, 207.