

DND photo AR2005-A01-137a by Sergeant Jerry Kean



Sergeant Reginald Obas oversees a translator talking to a local resident before giving him a short-wave radio and a newspaper outside the town of Spin Bulduk in Afghanistan. The distribution of the items are part of an effort by the Provincial Reconstruction Team (PRT) in Kandahar (LFWA).

FROM KOSOVO TO AFGHANISTAN: CANADA AND INFORMATION OPERATIONS

by Second Lieutenant Jessica M. Davis

Introduction

From the Peloponnesian wars to Iraq, psychological operations, information campaigns and intelligence gathering have played a crucial role in developing and maintaining an advantage on the battlefield. The information challenge facing armed forces is one of gathering and disseminating information. In an age when battles are fought in real time, with members of the public and the enemy able to 'log on' and view the conflict, dissemination of information is essential for gaining an advantage. Information Operations (IO)¹ are a vital facet of exploiting information superiority and a key aspect to warfighting in the modern era.

This article will focus on how Canada's armed forces are adapting to the changing infosphere² and how they are conducting Information Operations. The specific examples of IO usage in Kosovo and Afghanistan will demonstrate that Canada has not actually stepped full thrust into the information battle space. In fact, Canada's continued refusal to devote the necessary resources and develop the necessary capabilities is severely hampering its effective use of IO, and, indeed, the safety and effectiveness of Canadian soldiers deployed on the front lines. Despite this, Canadian soldiers are still generally able to accomplish the mission in true Canadian style – that is, without the proper equipment or

training. Unfortunately, this will not always be possible as Canadian equipment and skill sets become outdated, and technological advances become increasingly complex.

Background

The American armed forces often refer to this form of battle as the 'hearts and minds' campaign. Indeed, influencing public opinion, both at home and abroad, is one of the most important aspects of modern warfare. Information Operations are thus a critical aspect of any operation or war. The media reaches not only the homes of citizens, but also their minds. The ability to control the message being presented may result in the ability to influence the thoughts, and, possibly, even the behaviour of the recipient of the message.³ Many of the humanitarian disasters of the 20th century were spawned or exacerbated through the dissemination of information. Radio was used to propagate Nazi ideology in Germany and to spur genocide in Rwanda.⁴ Following these examples, one of the key strategies in the war on terror currently

Jessica Davis is a Master's candidate in the War Studies Programme at the Royal Military College of Canada, and is currently employed in the Canadian Forces Joint Headquarters J2 (Intelligence) section as an analyst.



An historically significant manipulator of public opinion, Nazi Germany's Minister of Propaganda, Joseph Goebbels.

being waged by the United States of America deals with defeating enemies by addressing the causes of discontent upon which extremism feeds.⁵

Elements of Information Operations

During the wars in the Former Yugoslavia, a strongly entrenched Western press corps made restrictions to information access nearly impossible. The British military sought to manage the media message, but this proved to be increasingly difficult, due to the sophisticated nature of the existing media establishment it faced.⁶ In recent years, the American military has taken to generating its own message. In Kosovo, a sophisticated media management machine generated daily messages, and then distributed them to reporters. The US military has thus attempted to shape the ideas of journalists by allowing them access only to certain information or areas. The media is difficult to control, but it can be key in winning (or losing) an information war.

While managing the media is one aspect of IO, controlling the information flow is yet another. This can involve shutting down satellites, cable links and microwave towers that are being employed by enemy forces.⁷ One of the most effective ways to attack an opponent is to attack its civilian infrastructure, such as commercial communications and broadcasting networks, financial data systems and transportation control systems.⁸ None of these attacks would likely result in heavy casualties, but they can cause a massive disruption of civilian infrastructure and frustrate the local population. For example, the

destruction of the Internet infrastructure in a single country would limit both the civilian public and their armed force's ability to access information, and this in turn would likely result in significantly reduced response times available to counter other emergencies. While this would prove extremely difficult to facilitate, and it would be unlikely to result in extensive enemy casualties, the Internet provides open source information, and connects key aspects of the military communications network. Therefore, by attacking the Internet, the intelligence-gathering capabilities of any military, and its ability to communicate, could be significantly compromised. The United States possesses a huge conventional military superiority, and, therefore, attacks against this type of 'soft' target are likely to be an attractive strategy for any potential assailant.

One of the most effective uses of communication systems in wartime is to spread disinformation. Planting false or misleading information is often more valuable than shutting down enemy communications.⁹ Indeed, as a result of spreading disinformation, one's enemy is often forced to follow false leads, which, in turn, sows further confusion and strains resources.

Even Canada's most technologically advanced allies, such as the United States, are currently facing difficulties with respect to Information Operations. American troops face a bandwidth shortage that dictates where ships are sent, when drones can fly, and what type and form of messages sailors and soldiers can receive. Bandwidth considerations kept the US from flying more than two Predator unmanned aerial vehicles (UAVs) at a time in Afghanistan – the live video monopolized the entire network.¹⁰ By flying only two Predators simultaneously, the information thus made available was significantly limited. The Pentagon has four military satellites designed and equipped for secure communications that are reserved for the highest priorities, as well as for simple data communications. To transmit additional information, time must be leased from commercial satellites. During the Kosovo conflict, US forces used all the time available on those satellites.¹¹ Therefore, it follows that without the ability to transmit secure communications, forces on the ground can be deprived of crucial information that could make their tasks much more effective and less dangerous.

Information Operations is a complex form of warfare that involves many aspects of information and intelligence management. According to James F. Dunnigan, a US military consultant and author, IO is managing how and what information is available to the public, as well as to your enemy.¹² It involves compromising enemy communications systems, Electronic Warfare (EW), Psychological Operations (PSYOPS), public relations initiatives, Human Intelligence gathering (HUMINT) and Cyber Warfare, as well as various combinations or mutations of these activities.

“Many of the humanitarian disasters of the 20th century were spawned or exacerbated through the dissemination of information.”

The Kosovo Experience

During the winter of 1999, the Yugoslavian government escalated its use of violence against the Albanian population of Kosovo. The resulting humanitarian disaster threatened to destabilize the Balkans and prompted Western intervention in the area.¹³ At the outset of the conflict, there was strong opposition to sending in Allied ground troops because of the likelihood of incurring significant casualties. However, action had to be taken as Slobodan Milosevic, the President of the Serbian Republic, continued his campaign against the Kosovar Albanians.¹⁴ The ensuing war for Kosovo was telecast around the world, with millions of people watching the conflict in real time.

Information Operations played a key role in the Kosovo crisis, since, as a precondition, the entire Balkan region was plagued by religious and ethnic turmoil. The intense emotions that were systemic there created new challenges for the forces that were attempting to develop peace and stability. The key messages that emerged in the subsequent IO campaign suggested that the only way to a better future for the inhabitants of the region was through tolerance and cooperation, and that the combined strength of the community was greater than its parts. Information Operations themes aimed to reinforce the idea that tolerance and cooperation meant a better standard of living and a safer future for everyone.¹⁵ A British PSYOPS team was responsible for the dissemination of this information via radio stations, magazines, posters, pamphlets and television commercials.¹⁶

NATO forces encountered several groups that were resistant to the messages of their Coalition. First, the Serbians had a vested interest in maintaining the status quo in terms of local and global perceptions of their position. The Serbian protection organizations were dedicated to the protection of the Serbian people and their interests, and they wanted to use the banner of legitimacy provided by the United Nations Mission in Kosovo (UNMIK) and NATO to achieve their aims. Their overall message was close to that of NATO, but the Serbian leaders were mostly religious, and their rhetoric tended to polarize the antagonistic camps by references to either “us” or “them.”¹⁷

Second, leaders of organized crime were also opposed to the IO campaign. In fact, they had a vested interest in seeing NATO fail. They wanted to undermine the security environment, and they largely used word of mouth to achieve this aim. Specifically, they spread rumours about NATO operations causing civilian casualties and greatly exaggerated local conflicts in order to undercut the feeling of safety in the region.

“Information Operations themes aimed to reinforce the idea that tolerance and cooperation meant a better standard of living and a safer future for everyone.”

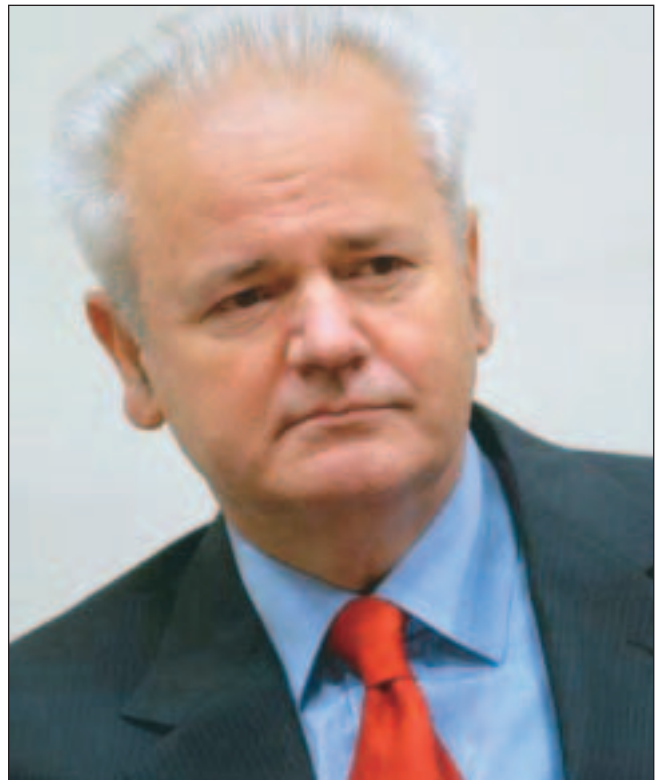
Finally, the Pan Albanian organizations formed the third group opposed to the IO campaign. They supported the creation of a sovereign, separate state of Kosovo, and tried to further this idea through the use of printed media.¹⁸

Qualified Effectiveness

Media management played a large role in Information Operations in Kosovo. Open Internet access was allowed to continue in Yugoslavia, as the allies believed that their message could be delivered most effectively in this manner,

and that access to independent media might undermine President Milosevic’s authority. However, to qualify the effect of these endeavours, it was reported that some Yugoslav Internet users did not even bother to access Western news stations, since they simply did not believe the information they imparted.¹⁹

Critical reporting was curtailed, and this policy was used to great effect during the war. Citing security concerns, senior commanders restricted journalistic coverage, and thus erected a barrier between those serving in the combat zone and those following the war from their living rooms.²⁰ ‘Spin doctors’ in Washington and London agreed on the desired message, then so informed the media through a series of briefings.²¹ Nonetheless, some journalists continued to report human-interest stories, such as what it was like for an ordinary Serbian family to be bombed.



Yet another skilled conjurer of propaganda, Serbia’s Slobodan Milosevic.

Maintaining popular support for the humanitarian intervention required unrelenting media management by NATO and the political leadership of the Alliance nations.²² The IO campaign was crucial in Kosovo in order to prevent the inhabitants from allying themselves with the opposing groups and fractionalizing the region even further.

“The lack of secure communications amongst the allies was another challenge faced by the NATO Alliance.”

The NATO allies certainly sought to manipulate information on the Internet to their advantage. NATO actively denied, via the Internet, that civilians had been accidentally bombed and killed. However, this information was effectively challenged in the same medium, and Alliance statements had to be reversed in the face of incontrovertible evidence.²³ Those opposing the war also used the Internet very effectively. Organizations and individuals throughout the world used their web sites to publish information relating to the conflict and to solicit support.²⁴ Various news groups were used to propagate negative or blatantly untrue stories of allied attacks against civilians. Live footage of the bombings was also distributed via the Internet and was often used in conjunction with scathing editorials that were disruptive to the conduct of the NATO mission.

The British government used web sites to counter Serbian propaganda.²⁵ They were concerned that the Yugoslav public was getting a highly distorted view of the war. Specifically, Foreign Secretary Robin Cook posted a message on the governmental web site that was intended for the Serbians, saying that Britain had nothing against the Serbians but that it was forced into action by the scale of Yugoslav President Slobodan Milosevic’s brutality.²⁶

The Americans and their NATO allies were not only waging an information campaign against their enemies, but directing it towards their own citizens. They were extremely concerned about public opinion at home, and made a very concerted effort to highlight the positive aspects of the campaign in order to maintain a continuous flow of public support for the NATO position.

During the war for Kosovo, NATO also employed Cyber Warfare in a very limited fashion. The Alliance carried out attacks against air defence computers from dedicated jamming aircraft.²⁷ These attacks marked the first combat use of the specific medium of computer network attack tools by the US military’s Information Operations cell.²⁸ The main thrust of their activities involved manufacturing false radar images and generating signal intelligence intercepts and inserting them into the Serbian air-defence system. Specifically, according to James F. Dunnigan, the US Air Force tapped into Serbian communications networks using satellites and EC 130 *Compass Call* aircraft in an effort to insert false messages into Serbian systems with respect to non-existent air raids and other attacks.²⁹

While the Serbian computer systems were extensively interconnected, NATO did not carry out hacking activities.³⁰ However, this interconnectedness could have led to

extremely effective hacking and Cyber Warfare operations. The main reason for not acting more aggressively on this front was that NATO lawyers were worried about concomitant war crimes charges if computers caused major damage to the civilian infrastructure. The relatively rudimentary state of American Cyber Warfare capabilities at the time was also a factor in this decision.³¹

The Serbians possessed a sophisticated deception capability that posed a considerable challenge to NATO forces. Despite American electronic sensors, the Serbians managed to employ an effective array of low-technology tools. Their troops knew how to hide themselves and their vehicles while still maintaining their mobility. They employed decoy vehicles that NATO forces routinely spotted and bombed. Fake bridges were built and heat reflecting camouflage paint was applied to the real bridges, so as to throw off the Alliance’s sensors.³² The Serbians also capitalized upon the few times that ‘smart’ bombs hit civilian targets.³³ And they circulated rumours, which had the effect of causing elements of confusion and dissension amongst various NATO member countries.³⁴

The lack of secure communications amongst the allies was another challenge faced by the NATO Alliance. This forced some air traffic control to be done on open lines, which meant that the Serbians could listen in on discussions of when and where NATO combat aircraft were operating.³⁵ Thus, unsecured communications clearly created a significant problem for the allies in terms of being able to deny the Serb fighters access to the NATO information and decision-making loop.

NATO generated a robust propaganda effort in Kosovo that targeted the local leaders of the villages and encouraged them to propagate the themes of the NATO mission. This was deemed somewhat successful in that the local leaders were occasionally heard to be repeating the main messages of the NATO KFOR (Kosovo Force).³⁶ Additionally, one of the main IO campaigns undertaken by the US military was called *Operation Matrix*. It was a covert operation that included harassing and pressuring Milosevic insiders by faxing and calling them on their cell phones.³⁷ While there is no known unclassified analysis of the results of this campaign available for public consumption, it certainly demonstrates that the allies were aware of the potential impact of yet another element of Information Operations on individuals.

Operation Kinetic

Operation Kinetic was Canada’s specific contribution to the war in Kosovo. Components of a stripped infantry battalion were responsible for the Canadian element of Information Operations generated in theatre, under the supervision of KFOR.³⁸ The main thrust of this Canadian contribution involved indirect media operations.³⁹ Press releases, interviews, newspaper and journal articles, the

Internet and e-mail were all used to advantage in propagating the themes of the mission in Kosovo.⁴⁰ The British command authorities had overall responsibility for the direct media operations and PSYOPS involving posters, loudspeakers, handbills, radio and television spots.⁴¹ Canada's role in the IO campaign in Kosovo, however, was very limited and modest. According to a Canadian intelligence officer who served in Kosovo, Canada's IO capabilities were virtually non-existent. There was only one public affairs officer who dealt with Canadian issues.

“Cyber War was employed to a limited extent during the Afghan conflict.”

Operation Kinetic endured several setbacks to its IO capabilities. Canada's secure communications system in Kosovo was the TITAN (secret) system. A serious virus affected this system in February 2000 and actually shut it down for approximately seven days. This situation persisted sporadically as new mutations of the virus were passed to the system. It created serious difficulties for the intelligence detachment since the system's fundamental database became unavailable during the virus attack.⁴² This left the Canadian contingent with only open sources of information, leaving them vulnerable to enemy disinformation efforts and unable to communicate secure intelligence to their own troops involved in operations.

One of the main challenges Canada faced was the lack of over-arching national and brigade level Information Operations doctrine, policy and structure. Canada needed its own IO capabilities in order to transmit Canadian themes, as well as to reinforce the NATO themes. However, other generalized problems beset the Alliance's IO efforts in Kosovo. For example, KFOR selected some particular local leaders to spread positive information about the KFOR mission. Nonetheless, the majority of the resident population disliked the leaders selected. Consequently, the initial IO campaign that was meant to prepare the population for the arrival of the Alliance troops was a complete failure.⁴³

The major difficulty facing NATO leaders was that they could not reassure their home nations that there would be no requirement to send in ground troops while still sending a convincing message to Belgrade that there would be ground troops committed if the situation did not resolve itself. As an exercise in IO, Kosovo was largely a failure because President Milosevic knew from the Western media that NATO's resolve was not absolute and that they were not prepared to risk the lives of NATO troops in a wholesale manner.⁴⁴ According to one senior US commander, a more robust, focused IO campaign could have halved the length of the conflict. All the tools were in place, but only a few of them were actually employed.⁴⁵



DND photo ISD00-1376a by Master Corporal Ken Allan, DGPA/J5FA Combat Camera

On the Kosovo-Serbia border, Federal Republic of Yugoslavia Soldiers of The Royal Canadian Dragoons use the surveillance equipment in their Coyote reconnaissance vehicles to overlook the Serbian border town of Prešovo from high ground in the American sector of Kosovo.



Trooper Eric Bennett of Lord Strathcona's Horse (Royal Canadians) sets up the surveillance system of a Coyote armoured reconnaissance vehicle in Pristina, Kosovo. Trooper Bennet is serving with the Reconnaissance Squadron of *Operation Kinetic*, Canada's contribution to KFOR, the NATO peacekeeping force in Kosovo.

The Afghanistan Experience

The war in Afghanistan posed a new set of challenges in terms of Information Operations. While the main strategy in Afghanistan has been to seek out and eliminate the Taliban/insurgent threat, little effort has been made to address the root causes of the discontent. Brigadier-General Peter J. Devlin, Commander of the Kabul Multinational Brigade (KMNB) in Afghanistan during 2003 and 2004, identified the importance of employing IO to protect the mission's centre of gravity, as well as international and local support for the resident International Security Assistance Force (ISAF), and to support the lines of operations associated with maintaining a secure environment and developing transitional administration security forces.⁴⁶

When American forces arrived in Afghanistan, a huge IO campaign was conducted to inform the entire country that the Americans had conventional forces on the ground.⁴⁷ However, the insurgent AQ group and the Taliban were also adept at IO, and they encouraged Afghans to join a new jihad or holy war against the Americans and their allies. This was

accomplished by covertly circulating night letters, a skill that, ironically, had been taught to the Afghans by the CIA in the 1980s.⁴⁸ AQ also offered rewards for special operators and foreigners who were killed, and that included humanitarian aid workers and foreign journalists.⁴⁹ Not only did this motivate the economically deprived people of Afghanistan to resist the foreign forces, but it also, understandably, had a negative effect on the morale of foreign workers, both military and civilian.

Independent television networks, such as al-Jazeera and a more sophisticated Internet, are making information more difficult to control than has been the case in previous conflicts.⁵⁰ The Bush administration asked American networks to censor themselves in an effort to reduce the amount of sensitive information released.⁵¹ However, other news agencies were neither susceptible nor amenable to the same influence. In effect, news agencies essentially provided sensitive information to the designated enemy in this case, simply by transmitting their news.

Cyber War was employed to a limited extent during the Afghan conflict. In late 2001, financial institutions were hacked, as well as pro-Taliban servers, as a pre-emptive move in order to gain more information about the enemy.⁵²

At the outset of the war, HUMINT usage in Afghanistan was virtually non-existent.⁵³ The majority of the assets developed during the Soviet-Afghan conflict no longer existed, or they had not been contacted for several years due to budget cuts within the CIA. Reliable HUMINT assets would have provided a significant intelligence capability and could have served as a force multiplier.

Operation Athena and Operation Apollo

These two operations constituted the Canadian contribution to the war in Afghanistan. Members of 3 Princess Patricia's Canadian Light Infantry (PPCLI) Battle Group, together with an augmentation from 2 PPCLI, deployed to Kandahar, Afghanistan, as part of a US Army task force during *Operation Apollo*. *Operation Athena* was Canada's contribution to the International Security Assistance Force.

ISAF Headquarters personnel carried out the majority of IO conducted in Afghanistan. During the first troop rotation, Romanian officers with limited English skills were given overall responsibility for Information Operations. Their limited English skills hampered their overall ability, particularly since they were dealing with Psychological Operations.⁵⁴ When engaged in this form of warfare, a cardinal rule is that the message sent out needs to be crystal clear and that there is no room for misinterpretation. However, during the first five months of the tour, ISAF refused to print any PSYOPS material in any language other than English and Dari. The subtleties of language meant that the effectiveness of the material was hampered, as most of the Romanian officers did not read English and most Afghans are illiterate.⁵⁵

According to General Devlin, the IO campaign in the Kabul Multinational Brigade (KMNB) was extremely dependent upon the ISAF Headquarters, with no integral PSYOPS assets and only a limited IO capability at the brigade level. Despite several Canadian officers being capable of carrying out this tasking, other contributing nations with dedicated psyops occupations were tasked to provide this expertise.⁵⁶ At the KMNB Headquarters, there was some frustration because the ISAF rates a corps level headquarters, and it is focused on strategic and operational level Information Operations, while the KMNB aimed to target the tactical level of operations.⁵⁷ This created a discontinuity between the forces, since they each had different IO needs and perspectives. ISAF Headquarters produced soldier's cards, which every member of the KMNB kept on their person in order to remind themselves of the main themes and messages that ISAF hoped to communicate to the people of the region. The KMNB then worked hard to improve the value of these cards by convincing ISAF to print them in English, German and French, so they could be read by all the soldiers in the brigade.⁵⁸ Even for an individual who reads English well, it is important that they be able to read a message in their primary language, since the subtleties of IO and psyops can often be lost in translation.

In theatre, there was no military television broadcasting capability. Television was not exploited as a means of transmitting messages at all, despite the surprising numbers of televisions in Kabul and the fact that they only had one local television station for competition. However, because of the low literacy rates in Afghanistan, television was eventually identified in the mounting process as a key way to get information to people. Exploited in a timely manner, television would have been a key medium for passing on the themes of the mission.

Operation Athena was the second Canadian Forces mission to deploy an integrated HUMINT capability.⁵⁹ However, key deficiencies still existed in the HUMINT collection, analysis and dissemination capabilities demonstrated in Afghanistan. Most notable was the lack of HUMINT collection assets, little available specific analytical capability, and the reluctance of national agencies to share information with the rest of the force.⁶⁰ Better integral HUMINT and covert surveillance capabilities for KMNB would have given an improved collection capability, and, therefore, more accurate intelligence collection.⁶¹ All KMNB operations that resulted in the capture of Afghani Extremist Resistance Group members were accomplished using HUMINT sources.⁶² The main failure in this realm was the lack of HUMINT development earlier in the mission. As it materialized, very few, if any, substantive HUMINT contacts were passed from nations that had formerly operated in West Kabul.⁶³

“Available communications equipment proved to be a consistently limiting factor with respect to reconnaissance operations during *Operation Apollo*.”

Decades of war and changing alliances have made Afghans extremely sensitive to any form of questioning. Any unusual presence by an officer or specialist team was quickly judged to be some form of intelligence-gathering mission.⁶⁴ This created a situation of distrust and apprehension with the local population, making it more difficult to judge their attitudes and responses to ISAF. Passive collection from Canadian personnel in the area was a very useful aspect of HUMINT. However, Canadian HUMINT only became useful to the brigade in the last month of the deployment of Rotation 0. Until that time, the KMNB was reliant on whatever HUMINT other allies chose to provide to it.⁶⁵

A significant communications problem existed for Canadians in Afghanistan. The reserve members of the Canadian Mechanized Brigade Group had no TITAN access, and this greatly slowed the passage of information. Regular mail or secure fax was used, but these were not optimal from a time management perspective.⁶⁶ The main communication system designated to be used in theatre, TETRAPOL, was slow to be procured, although funding for it had been approved in July 2003. Therefore, the commander was forced to assume the additional risk of using cell phones that were unsecured.⁶⁷ A request for a TITAN server with four workstations was not approved by National Defence Headquarters, due to the high costs involved. As a result, the Canadian military Departmental Wide Area Network (DWAN) system was used to transmit information, which, although unclassified, was frequently of a sensitive nature and would have been best transmitted via TITAN.⁶⁸ Once TITAN eventually arrived in theatre for *Operation Athena*, it suffered a prolonged outage that seriously affected operations for over a month, despite attempts to energize the chain of command to the importance of an immediate solution.⁶⁹ All company intelligence sources were linked via TITAN. And when TITAN collapsed, so did a company's intelligence picture.⁷⁰

The reconnaissance platoon did not have the means to transmit imagery remotely. Follow-on forces did not have the ability to learn the results of the initial area reconnaissance during combat operations. This sort of information is invaluable to a follow-on force commander during the planning process.⁷¹ Available communications equipment proved to be a consistently limiting factor with respect to reconnaissance operations during *Operation Apollo*.⁷²

For *Operation Athena*, Rotation 1, the brigade lacked personnel qualified to analyze incoming information. Few individuals in the brigade had an intelligence background, and none of them knew what area they would be focusing on prior to their arrival in theatre.⁷³ Regardless of these shortfalls, Canada's all-source intelligence cell proved to be outstanding in its analytical capability, but analysis was based upon non-ISAF sources and therefore it could not be shared with the KMNB as an entire entity, due to security limitations with respect to disclosure.⁷⁴



Canadian soldiers stand guard by their G Wagons while on patrol in Kandahar, Afghanistan. The soldiers are deployed as members of the Provincial Reconstruction Team (PRT) in support of *Operation Archer*. Approximately 1000 Canadian Forces personnel are deployed to Kabul and Kandahar as part of Joint Task Force Afghanistan (JTF-A).

Conclusions

Looking at the successes and failures of these missions, several major themes can be extracted. Deploying troops need to be better prepared from an intelligence standpoint to undertake their missions. Full, comprehensive briefings covering all likely eventualities anticipated should always be provided, and intelligence personnel should be made available for the work-up training. All personnel should arrive in theatre with a solid understanding of the cultural differences likely to be encountered.⁷⁵

Canada's IO capabilities are spread wide throughout the forces, and they should be consolidated.⁷⁶ Proper HUMINT training, such as the five-day interview, debrief and elicitation programme offered by the Director General of Intelligence, could go a long way in helping key military leaders become more efficient pieces of the intelligence gathering puzzle.⁷⁷ Number 3 PPCLI reported that their soldiers established an excellent rapport with indigenous

forces and local citizens, and a vast quantity of HUMINT was gathered by this means.⁷⁸ Section commanders, up to, at the very least, company commanders, need more formal information-gathering courses.⁷⁹

While HUMINT assets were developed and used on both these missions, they could have been employed much more extensively. The experience of *Operation Athena*, in which all the insurgents captured resulted from HUMINT inputs, clearly demonstrates the value of this asset.

The lack of proper communications equipment on both these missions is distressing. Not only did Canadian forces lack the methods by which to communicate with their allies, at times they could not even communicate amongst themselves. The resultant lack of secure communications was a very dangerous precedent. Despite these shortcomings, ISAF still managed to positively influence the vast majority of the local population, and this was verified by subsequent polling activities.⁸⁰

The Way Ahead

The information war is no mere sideshow. Possessing an ability to affect the attitudes and perceptions of local citizens in a zone of operations will be critical in helping to create a secure environment. The ability to communicate effectively with the local population, other military forces and people at home will be critical to providing intelligence and maintaining support for operations. In order to achieve positive results, the military must be on the cutting edge of these technologies.

Projections of future CF requirements will call for a paradigm shift in defence intelligence towards what may be described as a quest for information superiority.⁸¹ The operational backbone for information superiority is an

advanced technological architecture. Information superiority is predicated upon a defence intelligence capability to generate and integrate offensive and defensive information from a variety of intelligence sources, including surveillance, reconnaissance, and other information-gathering operations.⁸² Canada is currently following a disturbing path, given the realities of the new global environment, of not taking its IO capabilities, or lack thereof, seriously enough. We are in the unique position of having an incredible wealth of intelligent, educated, technologically competent people who can be used to great advantage. Were the Canadian military to leverage this natural capability, a significant force multiplier would be created that would greatly enhance the efficiency and success of the Canadian Forces.



NOTES

1. The term 'Information Operations' will be used throughout the article. The term 'Information Warfare' is prevalent in academic articles. However, Canadian doctrine uses the term information operations, and in order to be consistent throughout the text, the Canadian term has been applied.
2. The 'infosphere' is the fusion of the world's communication networks, databases and other sources of information into a vast connection collection of electronic interchanges. Alan D. Campen and Douglas H. Dearth (eds.), *Cyberwar 2.0* (Fairfax, Virginia: International Press, 1998), p. 77.
3. James F. Dunnigan, *The Next War Zone* (New York: Citadel Books, 2003), p. 148.
4. *Ibid.*
5. Campen and Dearth, p. 79.
6. James F. Metz, *Information Intervention, Foreign Affairs*, November/December 1997, p. 16.
7. *Ibid.*, pp. 17-18. In Bosnia, NATO was aggressive in responding to negative messages. The Pale-based Serb Radio Television that was loyal to Bosnian Serb leader and indicted war crimes suspect Radovan Karadzic was prevented from broadcasting its anti-NATO message. 300 US troops seized one of the station's relay towers and held it until the station agreed not to air 'inflammatory' broadcasts.
8. Thomas R. Mockaitis, *Winning Hearts and Minds in the War on Terrorism, Grand Strategy in the War Against Terrorism* (London: Frank Cass, 2003), p. 31.
9. Maud S. Beelman, *The Dangers of Disinformation in the War on Terrorism*, Harvard University's *Nieman Reports*, Winter 2001, Vol. 55, No. 4, p. 17.
10. Dunnigan, p.149.
11. *Ibid.*, p.109.
12. *Ibid.*, p.72.
13. Noah Shachtman, *Military Faces Bandwidth Crunch* <www.wired.com>, accessed 31 January 2003.
14. *Ibid.*
15. Sean Maloney and L.A. Willner, *Canadian Forces Operations 1970-2000*. Department of National Defence. Directorate of Operational Research (Joint). ORD Project Report PR 2002/01.
16. Sean Maloney, *Are We Just Peacekeepers? The Perception Versus the Reality of Canadian Involvement in the Iraq War*. Working Papers, IRPP. November 2003.
17. KFOR/MNB(C) *Operation Agricola VII* Presentation, 1999.
18. Interview with a senior intelligence officer requesting anonymity.
19. *Ibid.*
20. *Ibid.*
21. John Arquilla and David Ronfeldt. *Networks and Netwars*. (Santa Monica: Rand Corporation, 2001), p. 245.
22. Andrew J. Bacevich and Eliot A. Cohen (eds), *War Over Kosovo* (New York: Columbia University, 2003), p.158.
23. Beelman, p. 18.
24. Michael Ignatieff, *Virtual War* (Middlesex: Penguin Books, 2000), p.72.
25. Chris Cobb, *Governments losing control of information, The Edmonton Journal*, 16 October 2001.
26. Arquilla and Ronfeldt, p.246.
27. *Ibid.*, p.247.
28. *Ibid.*
29. Ivo Daalder and Michael E. O'Hanlon, *Winning Ugly: NATO's War to Save Kosovo*. (Washington D.C.: Brookings Institution Press, 2000), p.146.
30. Bacevich and Cohen, p.196.
31. *Ibid.*
32. Daalder and O' Hanlon, p.147.
33. *Ibid.*
34. Ignatieff, p.105.
35. Dunnigan, p.73.
36. *Ibid.*
37. Daalder and O'Hanlon, p.149.
38. Interview with a senior intelligence officer requesting anonymity.
39. Bacevich and Cohen, p.17.
40. Maloney and Willner.
41. All the information for this article was obtained from open sources. The author acknowledges that this is a limiting factor in assessing the information operations capabilities of *Operation Kinetic*, *Operation Athena* and *Operation Apollo*.
42. *Operation Kinetic* Rotation 0 Post Operation Report, December 1999. The post-operation reports were obtained through the Army Lessons Learned Centre's online resources, the Lessons Learned Knowledge Warehouse.
43. Interview with a senior intelligence officer requesting anonymity.
44. Rhiannon Vickers, *The Kosovo Campaign Political Communications, the Battle for Public Opinion and Foreign Policy*, International Studies Association, 14 March 2000.
45. Bacevich and Cohen, p.196.
46. Specifically, Brigadier-General Devlin was the commander of the KMNB during *Operation Athena*, Rotation 0, from July 2003 until February 2004. He was awarded a Meritorious Service Cross for his accomplishments while so commanding.
47. Robin Moore, *The Hunt for Bin Laden* (New York: Random House, 2003), p. 267.
48. *Ibid.*, p.272.
49. *Ibid.*
50. *Ibid.*
51. Victor Malarek, Investigative Editor, Thalia Assuras, Anchor, CBS News, *War on Terrorism Spawns an Information War*. On Canada AM, CTV Television, 15 October 2001.
52. Dunnigan, p.2.
53. Moore, p.54.
54. *Operation Athena* Rotation 0 Post Operation Report, December 2003.
55. *Ibid.*
56. *KMNB Information Operations: A Case Study*. Captain N. Packer, G3 ISTAR 2 and Colonel K.D. McQuillan, COS KMNB HQ *Operation Athena*, Rotation 0. In *Army Lessons Learned Centre: Bulletin*, Vol. 10, No. 2, June 2004.
57. Brigadier-General P.J. Devlin, *Operation Athena* Rotation 0 Phase 4 Commander Kabul Multi-national Brigade Update, January 2004. *Devlin Letters*. Published in the Army Lessons Learned Centre Bulletin, Vol. 10, No. 2, June 2004.
58. *Ibid.*
59. Bulletin: Army Lessons Learned Centre: HUMINT bulletin, Vol. 10, No. 4.
60. *Ibid.*
61. *Ibid.*
62. *Ibid.*

63. Army Lessons Learned Centre: Battalion Group Intelligence Section bulletin, *Operation Athena* Rotation 0, Vol. 10, No. 4.
64. *Ibid.*
65. Army Lessons Learned Centre: Intelligence bulletin. Vol. 10, No. 4.
66. Army Lessons Learned Centre: *Operation Athena* First Impressions, August 2003. The ALLC First Impressions was a special tasking that the ALLC received to capture the initial lessons from the deployment ahead of the POR being completed by the units.
67. See Note 56.
68. *Operation Apollo* Rotation 0 Post Operation Report, December 2003.
69. *Ibid.*
70. *Ibid.*
71. *Ibid.*
72. *Ibid.*
73. *Ibid.*
74. Moore, p. 54.
75. Army Lessons Learned Centre: Intelligence Section dispatches, *Operation Athena* Rotation 0, Vol. 10, No. 4.
76. Interview with a senior intelligence officer requesting anonymity.
77. See Note 56.
78. Moore, p. 54.
79. See Note 56.
80. Army Lessons Learned Centre: Information Operations dispatches, Vol. 10, No. 4.
81. Martin Rudner, *Intelligence and Information Superiority in the Future of Canadian Defence Policy*. Norman Paterson School of International Affairs. Occasional Paper No. 24, 2001.
82. *Ibid.*

