CF Combat Camera Photo IS2002-6764a by MCpl Paul MacGregor

A Lord Strathcona's Horse officer paying a visit to a school in Sanski Most, part of a 'winning the hearts and minds' programme in the Canadian area of responsibility in Bosnia.

PROTECTING THE CANADIAN FORCES AGAINST ASYMMETRIC THREATS

by Patrick Henrichon

It has become commonplace for commentators to note that, over the past dozen or so years, the international security environment has undergone a momentous transformation. The fall of the Soviet Union, the decline in the number of inter-state conflicts, the accelerated integration of the international economic systems, the growing influence of non-state actors, as well as revolutions in military affairs and information technology, have all contributed to the creation of new threats to states, military forces and civilian populations.

Among these new dangers are what analysts have labelled "asymmetric threats". The expression refers to 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. These non-traditional threats pose particular challenges to the defence communities of Western nations, especially with regard to force protection. The question of how to protect deployed personnel against asymmetric factors has become central in the minds of military thinkers as they strive to prepare their forces to operate on the battlefield of the future.

The problem of force protection against asymmetric threats is of particular importance for Canada and the Department of National Defence (DND). The Canadian Forces (CF) is often called upon to deploy as part of peace support operations, humanitarian missions or other actions undertaken alongside Canada's allies. As these activities take place in environments that are by definition tense or unstable, Canadian troops will undoubtedly be exposed to a variety of threats — including those of an asymmetrical

Patrick Henrichon *is a policy officer with the Assistant Deputy Minister (Policy) Group. He is currently working in the Ministerial Speechwriting Section.*

nature. This article will highlight the most significant issues in force protection against non-traditional threats in the context of peace support operations, and will explore ways by which the CF might counter them.

THEORETICAL CONSIDERATIONS

Generally speaking, asymmetric warfare occurs when a party employs unexpected or unusual tactics or weapons to defeat, reduce or neutralize the superiority of its opponent. In this regard, the terrorist attacks perpetrated against the United States on 11 September 2001 are a perfect example of an asymmetric action: civilian airliners were used in a way previously unimagined, directed as missiles against the heart of a large city and causing tremendous material damage and human casualties. For their part, the terrorists suffered only a minimum loss of resources.

"It is important for the CF to further develop its psychological operations, public affairs and civil-military cooperation capabilities, since these activities can be used to protect forces from asymmetric threats by 'winning over' the local population...."

The Canadian Forces defines an asymmetric threat as "attempts to circumvent or undermine an opponent's strengths while exploiting his weaknesses, using methods that differ significantly from the opponent's usual mode of operations."[1] Asymmetric threats can be grouped in three broad categories: information operations (IO), weapons of mass destruction (WMD) and non-conventional operations.

- **Information Operations.** Like other Western countries, Canada is highly dependent on information systems. Computers are now used in every field of life, from the simplest activities to critical sectors such as communications, energy and finance. Electronic systems are also crucial elements in the information-gathering process necessary for decision making. This dependence leaves Canada vulnerable to information operations conducted by hostile parties. These factions might infiltrate military or civilian information technology systems (including those used for C^4ISR^2 and logistics) to modify or manipulate data, attack the national strategic infrastructure, or disrupt decision-making processes or information collection and management capability. Information operations can take three forms:

  - strikes against infrastructures (e.g., computer network attacks, electronic warfare and physical destruction);
  - deception (e.g., propaganda operations through public communication channels, misinformation, hoaxes, etc.); and
  - psychological operations (e.g., hostage taking and the distribution of leaflets, radio or television broadcasts, and other means of transmitting information that promote fear or dissension).

"Regardless of the type of threat, better intelligence is needed to anticipate and counter asymmetric warfare."

- **Weapons of Mass Destruction.** The last decade has seen a proliferation of weapons of mass destruction (WMD), so labelled because they can cause indiscriminate suffering and death to a large number of people over a wide physical area. Despite international treaties, several countries are actively looking to develop these weapons or to acquire their means of delivery.[3] The fact that some of these weapons can be produced by individuals (thereby making them easily available to whoever is willing to pay for them) only increases the threat. The risks from WMD fall into the following broad categories:

  - ***Nuclear.*** Even if the possibility of a full-scale nuclear war has all but disappeared, threats involving nuclear weapons remain. There are grave uncertainties about the physical security of Russia's nuclear arsenal, and fissile material could be smuggled out of civilian or military facilities and acquired by hostile individuals or organizations. Proliferation is also a problem at the state level, where India and Pakistan have become the latest countries to develop nuclear weapons and where other countries, such as North Korea, are believed to have nuclear weapon programmes.

  - ***Biological.*** Biological agents are relatively cheap to produce, are within the capabilities of civilian biotechnologists, and have the potential to cause large-scale casualties or commotion (e.g., the anthrax incidents of the fall of 2001 in the United States and other countries). Conscious of the serious threat posed by biological agents, states have developed the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (BTWC).[4] However, a number of states have yet to sign or ratify this document, non-state actors are out of its reach, and the Convention lacks any verification mechanisms.

  - ***Chemical.*** Chemical weapons are also relatively easy and inexpensive to produce. As in the case of biological weapons, an international convention prohibiting the use of these types of weapons exists (the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC)),[5] but some states remain outside its regime. The CWC requires States Parties to prevent people under their jurisdiction from engaging in prohibited activities involving chemical weapons, but the nature of terrorist groups (combined with the ease with which certain chemical agents can be purchased or manufactured) makes

the implementation of national laws designed to support these measures nearly impossible.[6] The international community was reminded of the threat posed by chemical weapons in June 1995, when members of the Japanese Aum Shinrikyo religious cult launched a terrorist attack on the Tokyo subway. The sarin gas used in the attack killed 12 people and injured 3,800 others.[7]

- ***Radiological.*** Any country with civilian nuclear technology can produce radiological weapons. Such devices, which use the hazardous effects of radioactive material (such as plutonium or radium) to cause casualties or illnesses, are relatively easy and inexpensive to manufacture, though their distribution may be problematic. Terrorist organizations could notably use radioactive material in conjunction with conventional explosives to create a 'dirty bomb'. For these reasons, the destructive potential of radiological weapons should not be minimized.

- **Non-conventional Operations.** These types of operations include the use of non-orthodox tactics or terrain, civil disobedience and terror to circumvent an adversary's numerical, tactical or technological advantage:

  - ***Use of novel tactics and terrain.*** The use of non-traditional tactics (e.g., hit and run) and terrain (e.g., urban areas) [8] by an asymmetric opponent can facilitate a direct attack on military assets and operations, maximize the physical and psychological impact of the attack, and hinder military and police responses. The conduct of belligerent reprisals in built up areas poses particular problems, as large numbers of civilian bystanders can hamper a clear identification of the attackers. Furthermore, a counter-attack carries the risk of further civilian casualties.[9]

  - ***Civil disobedience.*** Asymmetric opponents can pose a threat by fomenting strikes and riots, demonstrations, boycotts and illegal occupations of facilities in order to destabilize, discredit or inflict damages to those they view as their adversaries. This type of non-conventional action is increasingly common in failed states (e.g. Somalia) or countries with tenuous political controls, and can be directed at both military and non-military personnel.

  - ***Use of terror.*** Actions such as the intentional targeting of civilians in locations distant from the main stage of the conflict, hostage taking, kidnapping, maiming, murder and other criminal activities can cause terror among a population without the asymmetric attacker being exposed to too much risk. As examples, we can cite the almost routine abduction of journalists or law officials by non-governmental factions in Colombia or of humanitarian aid personnel in Chechnya. Chechen rebels have also gained international media attention on 23 October 2002, when they took several hundred people hostage in a Moscow theater.

CF OPERATIONS AND ASYMMETRIC THREATS

The majority of CF personnel currently deployed abroad are engaged in peace support operations. These operations are often conducted in environments which are unstable (sometimes volatile) and which can lack political and judicial structures. Parties hostile to the presence of the peacekeeping force might take advantage of these conditions and strike against it using asymmetric means.

"Asymmetric threat: attempts to circumvent or undermine an opponent's strengths while exploiting his weaknesses, using methods that differ significantly from the opponent's usual mode of operations."

While it is expected that front-line peacekeeping troops will be well armed, well trained and well protected from most asymmetric threats, support structures such as base camps, logistics installations and lines of communications will likely be more vul-

DND Photo IS2002-1765a by MCpl Brian Walsh

A seaman aboard HMCS *Winnipeg* standing by to operate a signal lamp during operations in the Arabian Sea as part of Operation "Apollo", the international campaign against terrorism, November 2002.

nerable. Since their primary role is to support the mission, the people manning the logistics elements will probably not be as well armed and trained or have as much protective equipment as the deployed soldiers. Furthermore, because of personnel and budgetary reductions in several Western armed forces, an increasing numbers of civilian contractors are deployed in theatres of operation.[10] All these factors could present tempting opportunities for an opponent prepared to use asymmetric means.

DND Photo IS2002-2779a by MCpl Frank Hudec

A Canadian corporal applying chemical agent detector paper to a colleague's chemical defence suit during an exercise at Camp Ziouani in the Golan Heights, November 2002.

Threats to a peacekeeping force could materialize in several ways. In the domain of information operations, potential opponents could perpetrate attacks against C[4]ISR systems. These attacks could take the form of physical destruction of systems, denials of service or data tampering, and could be perpetrated with a view to disrupt command and control or interrupt communications. Adversaries could also engage in media manipulations or propaganda operations through public communication channels with a view to discredit the peacekeeping force, turn the local population against it, or sap the morale of soldiers. Finally, the security of international peacekeepers could be jeopardized by the re-ignition of violence in their deployment area, notably because of the distribution of leaflets or media broadcasts that promote fear and dissension or incite people to violent actions.

"Even if the potential opponent does not possess the capability to deploy [weapons of mass destruction] operationally, simply threatening to use these types of weapons can deter military deployments and peace support operations."

The acquisition of weapons of mass destruction by potential opponents could also threaten Canadian personnel in the field. When deployed in the Persian Gulf during Operation "Friction", Canadian troops were faced with the threat of chemical or biological attacks by Iraqi forces. Even if the potential opponent does not possess the capability to deploy them operationally, simply threatening to use these types of weapons can deter military deployments and peace support operations. Actual use can of course have extremely dire consequences. The WMD threat goes further than classic weapons-grade nuclear, biological or chemical agents. Opponents could resort to the deliberate release of toxic industrial material to perpetrate an asymmetric attack on a peacekeeping force. Threats to CF personnel on overseas operations also include exposure to radiation from intentionally damaged civilian radiological sources (such as nuclear power plants), or terrorist attacks with rudimentary radiological devices.

Non-conventional operations are another possible asymmetric threat to CF personnel deployed on peace missions. Past international operations have had to cope with hit and run tactics, ambushes or suicide bombings.[11] Deployed troops are also exposed to terrorist attacks[12] and are at risk of being involved in hostage taking. The CF have been the unfortunate victim of the latter when a Canadian peacekeeper serving with the United Nations in Bosnia-Herzegovina was taken hostage and used as a human shield in 1995, and when two officers were detained and suffered injuries after being 'interrogated' in the Democratic Republic of Congo in 2000. Opponents to an international presence may also use narcotics and other vices to incapacitate and corrupt members of a peacekeeping force. Finally, acts of civil disobedience, such as demonstrations, illegal occupations of facilities or riots, could threaten the security of peacekeepers. We have notably seen this happen in Kosovo and Bosnia-Herzegovina.[13] This threat is only likely to increase as the mandate of peacekeepers now frequently includes carrying out police duties until a civilian judicial system can be developed.

COUNTERING ASYMMETRIC THREATS

Canadian troops deployed on peace support operations are exposed to many asymmetric threats. However, countering those threats presents unique challenges. Operational staffs, engineers and security forces must balance force protection requirements with specific mission needs and objectives. Excessive security measures may very well compromise some operations by isolating the deployed units from the local population, or by making them appear as an overly aggressive, even threatening force.

With regard to information operations (IO), better force protection could be achieved by developing the CF's capability (both on the human resources and technical sides) to protect its computers and other electronic systems from outside attacks. This can be done through improved encryption devices, computerized identification and intrusion detection systems, as well as through tighter 'firewalls'. The CF should also expand its potential for preventive or offensive IO in order to neutralize any system that poses a threat to its own electronic equipment or that has previously perpetrated cyber-attacks against it. It is also important for the CF to further develop its psychological operations (PSYOPS), public affairs and civil-military cooperation capabilities, since these activities can be used to protect forces from asymmetric threats by 'winning over' the local population and neutralizing the human aspects of a potential threat.[14]

The CF's response capability against weapons of mass destruction remains limited. An audit of the CF's nuclear, biological and chemical defence capabilities carried out by the Chief of Review Services (CRS) in May 2001 demonstrated this shortfall. For example, the CF Nuclear, Biological and Chemical Response Team (NBCRT), located at CFB Borden, is constrained by its mandate to deployments only within Canada, while the Nuclear Emergency Response Teams (NERTs), located at CFB Halifax, CFB Esquimalt and CFMETR Nanoose, are only deployable locally.

In the follow-up to 11 September, the CF's defence capability against WMD was given a higher priority. In that context, the CF recently created the Joint Nuclear, Biological and Chemical Defence Company. Once fully operational in 2005, the company should significantly enhance the CF's ability to protect its deployed personnel — whether in Canada or abroad — against NBC attacks.

One of the main force protection issues regarding non-conventional operations is the danger of terrorist attacks against deployed installations. It is therefore important to improve the perimeter security capabilities of the CF. This could be achieved by the procurement of better equipment, such as deployable explosive device removal equipment and intrusion alarm systems for perimeter security. On the training scene, there is a need to conduct specialist training for explosive device removal technicians. To better protect individuals, personnel security courses (e.g., protection against kidnapping) could occupy a greater place in CF training, with a refresher course adapted to conditions in the field being offered before an operational deployment.

Regardless of the type of threat, better intelligence is needed to anticipate and counter asymmetric warfare. Indeed, an understanding of potential enemies, their motivations, their strategies and methods, their objectives and, especially, their cultural context, is perhaps more important than any technological advantage. We must also realize that traditional intelligence collection means, which are technologically heavy and still driven by Cold War requirements, may not present the best options for dealing with asymmetric threats. While technological assets are vital to assess and monitor these threats (some terrorist groups are using the Internet to transmit encrypted messages to their followers), the best assets for intelligence gathering on asymmetric threats will continue to be human (HUMINT) and open sources (OSINT).

"Deployed troops are also exposed to terrorist attacks and are at risk of being involved in hostage taking."

CONCLUSION

In the last decade, the concept of asymmetric threats has risen to the top of concerns for military planners. As they were confronted with less predictable and more diffuse

DND Photo ISD01-3117a by MCpl Ken Allen

A Canadian sergeant greeting village elders in Senafe, Eritrea, during a foot patrol intended to keep a close watch on the local situation, May 2001.

DND Photo ISC98-2130

Canadian troops taking up defensive positions to protect Bosnian Serbs during a riot by Bosnian Croats in Drvar, Bosnia, April 1998. Civil disobedience is one of many forms of threat to military forces involved in peace support operations.

threat factors, many organizations molded by Cold War requirements became vulnerable. While the CF has acknowledged the importance of protecting its troops and installations against asymmetric threats, its adaptation to the new reality is far from complete. For example, although doctrine for intelligence, information operations and NBC defence is either in place, in draft or in development, the CF has no overarching doctrine to deal with asymmetric approaches. There is also no formal Canadian joint doctrine for force protection or anti-terrorism.[15]

Whatever action the CF takes to improve its capabilities to counter asymmetric threats, special consideration should be given to non-military personnel. As we have seen, civilian contractors are frequently employed to provide support services for military operations, including peacekeeping missions, even though many observers consider that this dependence on civilians will become a considerable weakness of future overseas deployments. Furthermore, military personnel are often deployed alongside civilian administrators, members of non-governmental or humanitarian organizations, journalists and, of course, the local population. Needless to say, all of these civilians must be protected as well.

The Canadian Forces is developing strategies to ensure the protection of its members against asymmetric threats, but much remains to be done. When fully implemented, however, these strategies will go a long way toward strengthening the CF's ability to be operationally effective, regardless of the environment or threat.

CMJ

NOTES

The author wishes to thank Major Jeff Tasseron, from the Directorate of Strategic Planning Coordination at NDHQ, for his constructive suggestions for revisions of this article.

1. Definition adopted by the Armed Forces Council, 18 April 2000.
2. Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance.
3. On 11 December 2002, Spanish vessels patrolling the Arabian Sea intercepted a container ship loaded with 15 North Korean-made Scud-type ballistic missiles heading for Yemen.
4. In force since 1972, the BTWC was the first treaty to ban an entire type of weapon.
5. As of November 2002, 147 countries were parties to the CWC. Website of the Organization for the Prohibition of Chemical Weapons.
6. Website of the Non-Proliferation, Arms Control and Disarmament Division, Department of Foreign Affairs and International Trade.
7. This incident was actually the cult's second chemical attack. In June 1994, it had also used sarin gas on a dormitory in the city of Matsumoto. The cult wanted to prevent three judges (who were living in the dormitory) from handing in what was likely to be a detrimental decision in a case in which it was the defendant. Seven people died in the attack and five hundred had to be transported to hospital. In Kyle B. Olson, "Aum Shinrikyo: Once and Future Threat?"
8. For more on the place of urban warfare in Western military doctrine, see Dr. Roch Legault's article "The Urban Battlefield and the Army: Changes and Doctrines," *Canadian Military Journal*, Vol. 1, No. 3, Autumn 2000.
9. Department of National Defence, Directorate of Nuclear, Biological and Chemical Defence briefing note "Threat Definition: Asymmetric Threats and Weapons of Mass Destruction," 18 April 2000.
10. The CF has already engaged in such practices by contracting some of its logistics requirements in Bosnia-Herzegovina to private firms.
11. For example, armed factions in Somalia shot down a US helicopter in 1993 and ambushed the rescuers, killing 18 soldiers.
12. Such as the 1996 bombing of US military barracks in Saudi Arabia or the October 2000 suicide attack against the American vessel USS *Cole* in the Yemeni port of Aden.
13. In February 2000, NATO peacekeepers had to use force to prevent Kosovo Albanian demonstrators from crossing a bridge dividing the city of Mitrovica and penetrating into a predominantly Serb section of the city. In April 2001, 21 peacekeepers were injured by rioting Bosnian Croats in the town of Mostar. The demonstrations followed the seizure by international officials of a bank suspected to fund a Bosnian Croat breakaway movement.
14. For more on psychological operations, see Andrew Koch's article "Hearts and Minds," *Jane's Defence Weekly*, Vol. 36, No. 7, 15 August 2001.
15. Department of National Defence, Directorate of Nuclear, Biological and Chemical Defence briefing note "Capabilities Required of DND, Asymmetric Threats and Weapons of Mass Destruction," Fourth Draft, para 70, 18 March 2001, http://dcds.dwan.dnd.ca/din_locl/pmo_nmsc/DOCUMENTS/A2SpDocs/AS%20THREAT/Capab-FourthDraftV2.doc (consulted in May 2001).