NATIONAL COUNTER-TERRORISM INTELLIGENCE REQUIREMENTS (NCTIR)

Introduction

In 2004, the Government of Canada issued its first National Security Policy (NSP), *Securing an Open Society*, to ensure that Canada would be prepared for and could respond to future threats. Recognizing that threats to national security are beyond the capacity of individuals, communities or provinces to address alone, the NSP envisaged greater integration and more strategic co-ordination of key security functions, particularly those related to intelligence collection, threat assessments and emergency preparedness through the implementation of a strategic framework and an action plan.

To make substantive improvements in integration and co-ordination with regard to terrorist threats, the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP), in co-operation with the Canadian Association of Chiefs of Police (CACP), are developing National Counter-Terrorism Intelligence Requirements (NCTIR). The NCTIR is envisaged as an integral component of a broader national strategy involving training, information-sharing and a co-ordinated response to terrorist threats involving the whole of government.

Basis of the Initiative

The working assumptions underlying this initiative are the following:

- It is crucial to develop a common understanding of the elements of terrorist threats and what information may play an important role in piecing together the puzzle of a developing threat.

- Leveraging the skills, knowledge and resources of the law enforcement and security community, as part of a national strategy to develop intelligence on terrorist threats in Canada, is now a high priority for all levels of government.

- The reach and access of front-line enforcement personnel can be critical to the early detection of terrorist activity.

- Terrorist groups, regardless of affiliation, at some point must operate at street level to plan or advance an attack.

- The role of CSIS is to collect information on threats to national security and advise the Government of Canada. Where criminal activity is identified, CSIS is authorized to inform law enforcement.

- The RCMP, through the operation of several statutes, has the primary responsibility of performing the duties assigned to peace officers, such as arrests, detentions or prosecutions of individuals involved in activities that constitute a threat to the security of Canada.

- CSIS, in co-operation with the RCMP and the CACP, has developed NCTIR.

- The purpose of NCTIR is to inform and sensitize, not task, the law enforcement community as to the valuable information they may incidentally encounter during the performance of their duties.

- NCTIR allows for a more effective two-way dialogue between CSIS and law enforcement on terrorist threats.

- NCTIR will be updated periodically and integrated into a broader training and information program led by the RCMP.

Background: National Security Policy

The NSP articulated three core national security interests: protecting Canada and Canadians at home and abroad, ensuring Canada does not become a base for threats to our allies and contributing to international security. The NSP describes the four types of terrorism affecting Canada: religious extremism, violent secessionist movements, state-sponsored terrorism and domestic extremism which result in violence and threaten Canadians.

The leading threats to Canadians – terrorism and certain types of organized crime – are beyond the capacity of individuals, communities or provinces to address alone. The NSP recognizes that the complexity of threats facing Canada requires a co-ordinated and integrated national security framework enabling this country to respond to existing threats and quickly adapt to new ones. The Canadian system needs to be fully connected to key partners at all levels: provinces, territories, communities, first-line responders, the private sector and Canadians together.

Intelligence is recognized as the foundation enabling effective measures to be enacted for the security of Canada and Canadians. To effectively manage risk, design programs and allocate resources requires a sound understanding of the environment, along with the best possible information about the threats, intentions and capabilities of those who would do us harm.

The nature of intelligence is such that there is rarely, if ever, a complete picture. Rather, intelligence reporting and assessments are based on fragmented and sometimes contradictory information. It is, therefore, essential to bring together information on threats to Canada from all available sources and properly assess it, in order to provide as accurate and complete a picture as possible. It is critical that the resulting product be conveyed in a timely, accurate and usable manner to those whose actions or decisions depend on it.

All organizations in the Canadian security community have intelligence needs. The federal partners in the community with particular national security intelligence needs that also produce strategic, tactical and criminal intelligence are CSIS, RCMP, CBSA, TC, DND/CF, CSE, Health Canada, DFAIT, NRCAN and others. The Department of Public Safety Canada has key portfolio responsibilities for national security and for protecting critical infrastructure, the vast majority of which rests in the private sector, but which also requires robust intelligence support.

As the current scope of threat assessment requirements exceeded the capacity of any one organization, the NSP announced the creation of the Integrated Threat Assessment Centre (ITAC), which was subsequently established and housed in CSIS, to ensure that all threat-related information is brought together, assessed and disseminated in a timely manner. ITAC is maturing into a key facilitator for the dissemination of terrorist threat-related assessments to all levels of government.

A key component of Canada's national security system falls under the auspices of the provinces and territories. Provincial and municipal police services, as well as provincial emergency measures organizations, play an important role. The police community, in particular, has a unique insight and reach into Canada's diverse communities.

Framework and Strategy

In February 2007, CSIS was pleased to host the first National Police and Security Conference, which was jointly organized with the Counter-Terrorism Sub-Committee of the CACP and attended by many senior officials and Chiefs of police. The conference theme was developing a national approach to multi-jurisdictional co-operation against terrorism, and included the presentation of a national threat overview with a focus on international terrorism and Canadian domestic radicalization.

The conference addressed the need for a common strategy to investigate terrorist threats and respond to an immediate threat or actual attack. The complex nature of international terrorism involves criminal investigation, intelligence collection, national co-ordination, international co-operation, the Canadian military, as well as diplomatic efforts and senior political involvement.

In order to develop a national strategy guiding all organizations at all levels of government in their efforts to protect Canada and Canadians from terrorism, key senior police and security officials discussed options to have a co-ordinated national approach, while recognizing and respecting the responsibilities of all partners. It was recognized that the street-level reach of law enforcement partners can be key to detecting and countering threats. At this conference, CSIS, as Canada's national intelligence service, was tasked to define and set National Counter-Terrorism Intelligence Requirements (NCTIR). With a view to developing a national strategy, the NCTIR will set common objectives and provide a joint understanding of information requirements.

Federal partners must have the ability, in turn, to inform their provincial and municipal partners about threats and provide leads, warnings, profiles and advice knowing that everyone is working towards the same objectives: prevention, arrest, prosecution, detection, surveillance, disruption, co-ordination, preparedness, response, reporting, dissemination and accountability. As part of the foundation for a national strategy, NCTIR have been developed and shared amongst all partners.

NATIONAL COUNTER-TERRORISM INTELLIGENCE REQUIREMENTS (NCTIR)

1. To identify the capabilities, intentions and inter-relationships, including recruitment, membership, radicalization, training, means of communication, the role of the Internet, the means and methods of fundraising and the deployment of individuals, either in Canada or abroad, who support:

- Global Jihad (GJ) and Islamist Extremism (IE).
- Hizballah.
- Secessionist movements, including but not limited to the Tamil Tigers (LTTE), Babbar Khalsa International (BKI), and the International Sikh Youth Foundation (ISYF).
- The use of serious violence directed at Canadian interests, including the Canadian military, diplomats, foreign aid workers or other official personnel abroad.
- The procurement, development or possible use of chemical, biological, radiological, nuclear or explosive material for use in violent activities related to any NCTIR.
- The involvement of criminal activity including fraud, theft, extortion, document forgery, illegal migration or immigrant smuggling suspected to be in support of an NCTIR.

COLLECTION CRITERIA IN SUPPORT OF NCTIR

1. Foreign Travel:

Individuals linked to an NCTIR travelling to and from 'hot zones', including but not limited to Afghanistan and environs, Bosnia, Chechnya, Iran, Iraq, the Palestinian territories, Pakistan, Yemen, Somalia, Sudan, Syria and Tunisia.

2. Inciting Violence:

Individuals advocating or glorifying violence through the importation, production or distribution of videos or other media, and the physical or electronic circulation of video images of terrorist or insurgent attacks in 'hot zones', for the purpose of propaganda, recruitment or training, or sponsorship, operation or use of Web sites, chat rooms or blogs significantly linked to an NCTIR.

3. Extremist Proselytizing:

Individuals proselytizing or invoking an extreme, jihadist interpretation of Islam for the purpose of recruiting fighters, glorifying jihadist violence or inciting hatred against an identifiable group, particularly citizens or the military of Canada, the US, the UK or any other ally.

4. Facilities:

Facilities, including religious, academic, public, private or commercial buildings and structures, used permanently or temporarily for the purpose of:

- Recruiting fighters, advocating or glorifying violence, inciting hatred or supporting such activities.
- Training or indoctrinating those linked to an NCTIR, directly or indirectly, such as paramilitary activities, paint-ball, martial arts or other self-defence training, survival skills or extreme sports and training in the use of electronic devices or communications equipment.
- Supporting or facilitating activities directly or indirectly, as referenced above, such as storage facilities, cache sites, guest houses, safe houses or venues of convenience.
- Bomb-making, including facilities with indications of inordinately high electrical power consumption, reports of unusual chemical smells, blacked out windows or damaged pipe systems, any of which may indicate the possibility of bomb-making activities.

5. Fundraising / Financing:

Sources and means of funding NCTIR activities including fraud, extortion, theft, drugs, stolen property, money transfers, loans, credit cards, personal income or investments, couriers, financial institutions, hawala banking systems, grants, gifts or aid from any source, including foreign governments. Organizations or other entities, including registered charities, which are used with consent or unwittingly to collect, receive, funnel, channel or otherwise facilitate NCTIR financing.

6. Documentation:

Individuals or groups, including public officials, involved in, and methods related to:

- The acquisition or fabrication of false documents, including passports, other travel documents, primary documents such as birth or death certificates, driver's licences and citizenship documents. This includes equipment related to the illicit fabrication or altering of documents such as photocopiers, commercial grade flatbed scanners, printing or laminating equipment.

- The acquisition or provision of legitimate documents through false declarations or deceit, which are knowingly provided by the true owner or facilitated by a guarantor with possible or direct knowledge of the intended use. This will include reviewing the passports or travel documents of individuals of interest, wherever possible, to verify travel and to ensure the information contained therein is valid and consistent with applications for same.

7. Networks:

Definable networks associated to any of the aforementioned requirements. This includes familial, kin, clan, tribe, school or village ties.

8. Veterans:

Individuals who have fought in or met while fighting jihad or other violent movements abroad or in foreign wars.

9. Procurement:

Individuals or groups linked to NCTIR who are involved in the procurement of:

- Non-restricted items which could be used in support of NCTIR operations, including training, attacks or reconnaissance for pre-attack planning, such as registered firearms, mock/ substitute firearms, video cameras, night-vision equipment, electronic devices, communications equipment, camouflage or protective clothing, vehicles, backpacks, tents or camping equipment.

- Computers or related equipment, flash memory cards or sticks, CD / DVD burners, Internet/ ISP accounts, Internet kiosks, taking computer or related training, seeking employment in or starting computer-related businesses.

- Cell phones, pagers, cordless or other phones, long-distance phone cards, Blackberry or similar devices, Bluetooth technology or related equipment.

- Restricted or suspicious items which could be used in support of NCTIR operations, including illegal firearms or weapons, explosives or components thereof, detonators, remote control devices, chemicals, containers possibly used to house bombs, metal potentially used as shrapnel such as nails, diesel fuel, acetone, acids, hexamine tablets (solid campfire fuel/ fire starters), hydrogen peroxide, large quantities of fertilizers, coffee, sugar, sawdust or grinding equipment.

10. Counter-surveillance:

Individuals using counter-surveillance techniques, including confrontational accusations of informing, frequent use of pay phones or Internet kiosks, especially when inconvenient, frequent changing of cell phones, sudden travel, compartmentalization of information or selective lying.

11. Reconnaissance:

Individuals engaging in possible attack planning, reconnaissance or targeting activities, including videotaping possible targets or attack routes, unusual visits to possible target sites which may be security or reconnaissance probes, the surveillance of security measures or the surveillance of individuals who may be possible targets.

12. Crime:

Individuals engaging in criminal activity related to an NCTIR, including illegal migration, petty theft or criminal assaults.

Reporting

Information related to the NCTIR should be reported through the intelligence function of the various entities directly to CSIS regional offices and to the Integrated National Security Enforcement Teams (INSET).