NORTH ATLANTIC TREATY ORGANISATION

Democratic Institutions Fellowships Programme 1997-1999

THE ROLE OF A SECURITY INTELLIGENCE SERVICE IN A DEMOCRACY

Dovydas Vitkauskas

June 1999

TABLE OF CONTENTS

Introduction

Historically, where a state was totalitarian, its leaders "knew how to rule with the help of the secret police, but not with the secret ballot"[1]. A domestic security intelligence service in such a country was therefore a very important tool of the government, aimed at repression and control of its own citizens.

This being so, the fact remains that all democratic states retain internal security intelligence agencies. What is the point of a domestic security intelligence service in a democracy? It can be literally inferred that the principal task of the service is to defend the state against threats to its national security. Because those threats could often be covertly-organised, the service needs intelligence to counter them. But what are those threats? It is clear that, during the Cold War, security intelligence services of the NATO states were tasked first and foremost with defending these countries from foreign agents and domestic subversive elements, the activities of whom were usually prompted by the communist governments. However, as the Cold War is over, are there any real threats to national security of democratic states? If so, are they static?

Furthermore, why a separate security intelligence structure is needed to protect national security? Could the police do the same job? Is a security intelligence service exclusively "internal"? Is it an independent agency, or subject to a strict control by the government in power? What are the functions of a security intelligence service in relation to the government and its position within the structure of governmental institutions? What is the system of controls and external review of a security intelligence service in a democratic country? Should parliamentarians and oversight bodies be entitled to know everything about the service, or is there a limit to the service's external review? How to conduct effective security intelligence and, at the same time, to ensure the protection of human rights and fundamental freedoms?

This project is intended to answer some of the above questions or, when no unequivocal answer is possible, to review the fields of concern denoted by these questions.

The project will focus on the role of an "internal" security intelligence service. In view of different traditions, an "internal" security intelligence service can also be referred to as a "domestic" or "national" security intelligence agency. Some of these countries call it a "security intelligence service", thereby emphasising its primary function to collect and assess intelligence, some confine themselves to calling it a "security service", thereby dropping the intelligence function from the name, some refer to it as a "secret service" to emphasise the covert nature of its operations. In some of the NATO countries security intelligence work is performed by the police; in such a system the service may also be called a "police security service". To avoid any misunderstanding or confusion, the term "security intelligence service" will be used throughout this paper to indicate all the above notions.

[1] KISSINGER, Henry, *Diplomacy*, Touchstone, New York 1995, p. 793.

In addition, it must be observed that a security intelligence service is in no way the only security/intelligence player in the complex systems of intelligence agencies of modern democratic states. In most of the NATO countries other authorities have certain security or intelligence responsibilities, including the special central governmental structures, defence, foreign affairs, immigration, customs and trade, energy, transport, finance, health authorities etc. As mentioned above, a security intelligence service could also be part of the national police force. And even where it is not, it works closely with law enforcement institutions in order to prosecute individuals and groups who commit offences against national security. Therefore, this project will inevitably touch upon certain aspects pertaining to other security and intelligence structures, insofar as a security intelligence service interacts with them.

This paper is based mainly on the review of the Canadian security intelligence model. Canada has the most recently established security intelligence service among the NATO countries. Various examples on security intelligence systems in France, Germany, Norway, the United Kingdom and the United States will be referred to in comparison, in order to emphasise certain differences and similarities in the way these states counter threats to their national security.

The purpose of the project is therefore to present a wider picture of the role of a security intelligence service in a democracy, not in a particular country. Examples of the security intelligence models of Canada and other NATO states will facilitate a more general but, hopefully, comprehensive analysis of the topic.

I. Internal and external intelligence agencies of democratic states

1. Canada

a. Historical background

The Canadian Security Intelligence Service (CSIS) evolved from a special police force created in 1873 under the name of the Royal Canadian Mounted Police (RCMP). In 1920 the RCMP became responsible for collecting security intelligence in Canada. After a big network of Soviet spies was revealed in Canada following the end of the World War II, the Canadian Government formed a special branch of the RCMP, which was subsequently called the Security Service.

Starting with the 1970's, allegations were expressed concerning the illegal and inappropriate activities of the Security Service. One of the claims in this connection was that the Security Service had stolen files on separatist militants from a Canadian political party. With a view to investigating the allegations, in 1977 the Government appointed a special commission, lead by Mr Justice David C. McDonald. The McDonald Commission comprehensively investigated several hundred of similar complaints, that touched upon not only the actions of the Security Service, but also the traditional police operations of the RCMP.

The McDonald Commission published its findings in 1981. The results of the investigation provided detailed proposals for the restructuring of the Security Service and the strengthening of the governmental control. The conclusions were *inter alia* that highest governmental officials were unaware of what was happening with security policies and operations[2]. The Commission asserted that there was a need for a domestic security intelligence service, and that it ought to be a civilian agency separate from the RCMP[3]. The recommendation was based on the argument that security intelligence investigations were quite different from the police work, and that they required different methods, training and procedures. The McDonald Commission stated that this new agency should be established by a law, which would define its mandate, functions, powers, the conditions under which those powers could be used, and the organisational structure.

The McDonald Commission described the two basic needs concerning the security of Canada: "first, the need to protect Canadians and their government against attempts by foreign powers to use coercive or clandestine means to advance their own interests in Canada; and second, the need to protect the essential elements of the Canadian democracy against attempts to destroy or subvert them"[4]. The McDonald

[2] *Freedom and Security Under the Law*, the Minister of Supply and Services of Canada, Ottawa 1981. Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police ("McDonald Commission"), Second Report, Volume 2, p. 81.
[3] *ibid*., p. 753.
[4] *ibid*., p. 40

Commission concluded that "the security system of Canada must comply with two principal standards: it must be effective and work within a democratic structure"[5].

In 1981 a transitional group was set up to study the detailed recommendations of the McDonald Commission, and to develop specific plans for creating the new agency. The transitional group endorsed five basic principles, according to which the new agency must: a) provide effective security intelligence essential to the security of Canada; b) have an adequate legal framework within which to operate under the rule of law which recognises human rights and fundamental freedoms of Canadians; c) have an effective management system, ensuring responsible direction and respect for the rule of law; d) be effectively accountable to ministers who are responsible to the Parliament; and e) be open to a satisfactorily external review, to ensure that the service does not abuse its powers and that it is not misused by the Government[6].

In 1984 the Parliament adopted the Act establishing the Canadian Security Intelligence Service (hereinafter referred to as "the CSIS Act 1984"), a civil agency separate from the police. The Act defined the service's mandate, powers, controls and external review[7]. The CSIS is the most recently established security intelligence service among the NATO states.

b. Canadian intelligence agencies

The CSIS is in charge of domestic security intelligence in Canada. At the highest level, the CSIS is responsible to the Department of the Solicitor General[8], who is responsible for three main elements of the Canadian domestic security system: security intelligence, security enforcement and protective security. The Royal Canadian Mounted Police is Canada's federal police force. It collects its own intelligence in connection with its mandate to fight particular crimes. The RCMP is responsible for security enforcement and protective security. In addition, the Criminal Intelligence Service Canada (CISC) provides the facilities to unite the criminal intelligence units of the Canadian law enforcement authorities in the fight against the spread of organised crime. As observed above, all the above structures are subordinate to the Department of the Solicitor General.

Unlike most of its allies and competitors, Canada does not have an agency dedicated specifically to gathering foreign intelligence abroad. The requirements of foreign intelligence in Canada are met by the Privy Council Office (PCO), the main structure assessing and co-ordinating assessment of intelligence in Canada, and other intelligence agencies through the relevant exchange of information with the NATO States, in particular the United States, the United Kingdom, and also Australia and New Zealand.

[5] *ibid*., p. 47.
[6] *CSIS Explanatory Notes*, 1996.
[7] A more detailed account of the above elements of the CSIS will follow below.
[8] i.e. a "Ministry of Justice" in European terms.

The Division of the Director General Intelligence within the Department of National Defence and the Canadian Armed Forces is responsible for the production and dissemination of military intelligence. The Division accommodates the National Defence Intelligence Centre (NDIC) which monitors global events and provides analysis. The Department of National Defence also operates the Communications Security Establishment (CSE) which is in charge of signals intelligence[9].

2. Other states

a. France

The interior security of France is the responsibility of two major police forces: the national police force, governed by a civil statute, which is under the supervision of the Ministry of Interior, and the national gendarmerie, which is the military police under the supervision of the Ministry of Defence.

The DST (*la Direction de la Surveillance du Territoire*) is responsible for domestic security intelligence in France. It is subordinate to the Ministry of Interior. The mandate, functions, powers, controls and review of the DST are defined in a 1982 law. The functions of the DST include foreign intelligence. It collects and analyses intelligence and develops general strategies for the country's security. As observed above, the DST is part of a wider national police structure; the DST Director maintains close relations with the Director General of the National Police. As the DST is a police service, it may, in certain circumstances, undertake law enforcement actions. The DCPJ (*la Direction Centrale de Police Judiciaire*) is an internal security service which acts as the "public face" of the DST. The Ministry of Interior also accommodates the DCRG (*la Direction Centrale des Renseignements Généraux*) which is in charge of rather "scientific" analysis of all intelligence gathered with a view to advising the government and the local authorities on current political, economic and social issues.

The Ministry of Defence accommodates the French foreign and military intelligence services: the DGSE (*la Direction Générale de la Sécurité Extérieure*) which is in charge of foreign intelligence, the DRM (*la Direction du Renseignement Militaire*) which gathers military information, including tactical intelligence, and the DPSD (*la Direction de la Protection et de la Sécurité de la Défense*) which is a protective security agency of the French army, responsible for military counter-intelligence operations, as well as political surveillance of the French military in order to ensure political reliability of the armed forces. The Defence intelligence establishment in France includes the recently created BRGE (*La Brigade de Renseignement et de Guerre Electronique*), responsible for signals intelligence support to the military. The SCSSI (*Le Service Central de la Sécurité des Systèmes d'Informations*), responsible for regulation of the use of crypt-systems, was established in 1996.

[9] Intercepting and deciphering satellite communications, etc.

b. Germany

In Germany, the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*), or the FOPC, functions as a domestic civil security intelligence service. The FOPC was established under a special law. It operates under the auspices of the Ministry of Interior which is responsible for the internal security of Germany. The FOPC, as a civil security intelligence service, is not empowered to carry out active measures or law enforcement action. In this respect, the German security intelligence model is similar to that in Canada. The German Ministry of Interior also accommodates law enforcement institutions, such as the Federal Criminal Police Office and the Federal Border Guard which also have certain security intelligence responsibilities, insofar as it relates to the prosecution of those responsible for security-related offences. There is a military intelligence service subordinate to the Ministry of Defence, and a foreign intelligence service, the so-called BND (*Bundesnachrichtendienst*), subordinate to the Federal Chancellory.

c. United Kingdom

The British Security Service, the so-called MI5, is responsible for domestic security intelligence in the United Kingdom. Although the service was established in 1909, it was placed on a proper statutory footing only following the adoption of the Security Service Act in 1989. The Security Service operates under the statutory authority of the Home Secretary, but it is formally not part of the Home Office. The Security Service has no executive powers and it is not a police force; similarly to the CSIS in Canada and the FOPC in Germany, the MI5 is a civil security intelligence service. The Home Office also accommodates the National Criminal Intelligence Service (NCIS), launched in 1992, a police intelligence service responsible for combating the top echelons of crime. In addition, the Directorate of Intelligence of the Metropolitan Police Service (MPS, also known as the "Scotland Yard") shows that the MPS is becoming a pro-active intelligence-led service. The MPS is also subordinate to the Home Office.

The British Secret Intelligence Service (SIS, also known as the MI6) conducts foreign intelligence. The Government Communications Headquarters (GCHQ) is the U.K. centre for foreign and defence signals intelligence. The GCHQ has separate naval, air and army sections for military intelligence purposes. The GCHQ also includes the Communications Electronics Security Group (CESG) which ensures the security of official and military communications networks and advice the government and industry on computer security. Both the MI6 and the GCHQ are answerable to the Foreign & Commonwealth Secretary. Tactical military intelligence is collected by the Defence Intelligence Staff which forms an integral part of the Ministry of Defence.

d. United States

The United States has established a complex system of agencies having certain security and intelligence responsibilities. Domestic security intelligence in the U.S. is collected by the Federal Bureau of Investigation (FBI), subordinate to the Attorney

General who heads the Department of Justice. The FBI is a law enforcement agency. Hence, similarly as France, the United States do not have a separate security intelligence service. The Attorney General heads the Department of Justice, which also accommodates the Drug Enforcement Administration (DEA), the National Infrastructure Protection Center (NIPC), the Office of Intelligence Policy and Review (OIPR) and the National Drug Intelligence Center (NDIC), having certain intelligence collection and assessment responsibilities.

The so-called U.S. intelligence community is composed of thirteen agencies which provide intelligence under the National Foreign Intelligence Program (NFIP). The NFIP includes the FBI Foreign Counter-Intelligence Program (FBI FCIP), and several other civilian intelligence programs, operated by the Central Intelligence Agency (CIA), the Departments of State, Energy and Treasury. In addition, defence intelligence programs within the NFIP are operated by the intelligence agencies subordinate to the Department of Defence, including the National Security Agency (NSA) which is in charge of intercepting and deciphering communications intelligence, the National Reconnaissance Office (NRO), responsible for developing, producing, and operating national imagery and signals-collection satellites, and the Defence Intelligence Agency (DIA). The NFIP is comprised of all programs, projects, and activities of the U.S. intelligence community designated jointly by the Director of Central Intelligence (the CIA Director) and the head of a United States department or agency, or by the President. Excluded from the NFIP are those portions of the U.S. defence budget that are set aside for the Tactical Intelligence and Related Activities (TIARA) and the Joint Military Intelligence Program (JMIP). Therefore, the NFIP incorporates in principle all the U.S. national-level intelligence, counter-intelligence and reconnaissance programs. The above programs are not organisations, but structures that manage resources for intelligence operations and activities. As observed above, the NFIP provides funding for the Central Intelligence Agency, an independent agency, a number of foreign intelligence and counter-intelligence elements attached to the Department of Defence, and foreign intelligence and counter-intelligence elements of the Departments of State, Energy, Treasury, and Justice, including the FBI.

The FBI collects intelligence domestically, while the U.S. intelligence community is required to avoid collecting on the U.S. citizens and organisations. If a U.S. national is committing an offence to the national security or falls within the guidelines for counter-intelligence or counter-terrorism, the FBI collects information on that person. However, certain security intelligence functions can be performed domestically by the U.S. intelligence community too, provided that the collection of information is targeted at a foreign person or organisation within the United States.

II. Mandate, functions, powers and controls of a security intelligence service - its position within the structure of governmental institutions

1. Mandate - threats to national security

The mandate of a security intelligence service defines the tasks that the service has to perform, and provides the guiding principles by which the service conducts its operations and measures its effectiveness. More than any other element in the system, the mandate must reflect the overall balance required; it must be broad enough to permit the agency to develop adequate intelligence on present and future threats to security, but it must also have clearly defined limits to ensure the respect for human rights and fundamental freedoms of nationals.

As observed above, in most of the NATO states security intelligence services function on the basis of a separate law, defining the services' respective mandates. The exception in this case is the U.S. where the FBI has been directed or authorised by Presidential statements and directives to obtain information about activities threatening American security[10].

A clearly defined mandate helps a security intelligence service to function within a statutory remit. What must be avoided in this respect are situations such as those in the communist states during the Cold War, when the rhetoric of "national security" could be used to justify everything from stealing commercial secrets to clamping down on dissent[11]. At the same time, the relevant legislation defining the treats to national security should be flexible enough to allow a security intelligence service itself to scan the horizons and prepare for looming threats in the next century. These threats may well be terrorism arising from new conflicts, or serious crime and financial fraud undermining economy of a state, or people with access to nuclear, biological and chemical weapons, or people attacking communications and computer systems[12].

In Canada, threats to national security are defined in the CSIS Act 1984. The basis for the investigations of the CSIS is the definition in the Act of the following threats: a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed towards or in support of such espionage or sabotage, b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person, c) activities within or relating to Canada directed towards or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign State, and d) activities directed towards undermining by covert unlawful acts, or directed towards or intended ultimately to lead to the

[10] Although a specific statutory basis exists for the FBI's investigations of particular crimes.
[11] RUTLAND, Peter, *Mission*: *Improbable*, Transition, Vol. 2, no. 22 (1 November 1996), p. 5.
[12] *Traditional tasks of an internal security service and its position within government institutions - U.K. presentation*. Report of MANNINGHAM-BULLER E., of the British Security Service, at the Conference for NACC/PfP Security Officials held in Brussels on 20-21 November 1996, pp. 5-6.

destruction or overthrow by violence of the constitutionally established system of government in Canada[13]. The CSIS Act 1984 also states that persons or groups involved in "lawful advocacy, protest or dissent" should not be considered as the security threats unless their actions fall within the sphere of activities listed above[14].

a. Espionage and sabotage

With a view to protecting national security, sensitive information concerning political, economic, scientific or military affairs of a state must be kept secret. All countries have secrets that other states seek to acquire in order to advance their objectives. Any unauthorised attempt to obtain such information for a foreign power is an indication of possible espionage. Sabotage is considered as activities conducted for the purpose of endangering the safety, security or defence of vital public or private property, such as installations, structures, equipment or systems.

In countering espionage, a security intelligence service catch spies, thereby disrupting activities of hostile intelligence services. In this work it is important to define what is really secret in the relevant legislation. In Canada, these secrets are defined in the Security Offences Act 1989.

Countering espionage is the "oldest" task of most of the world's security intelligence services. For example, British Security Service was set up in 1909 (it was then known as the "Secret Service Bureau") specifically to counter the espionage threat. The U.S. Federal Bureau of Investigation was founded in 1908 (it was then known as the "Special Agent Force") to investigate particular federal crimes, but already during the Word War I it was given responsibility for espionage and sabotage.

In its early years, the Canadian Security Intelligence Service also devoted much of its energy and resources to countering spying activities of foreign governments. Time has passed, however, and the threat of espionage is now declining. To keep up with the times, the CSIS has targeted its Counter-Intelligence (CI) Branch to focus not only on espionage, but on trans-national crime, economic security, and issues surrounding the proliferation of weapons of mass-destruction.

Following the end of the Cold War, voices are raised claiming that espionage is obviously something a state can do without. The costs exceed any possible gain. It is obvious that, if a country went out of the business of espionage, savings would be substantial and the gain in political terms even greater still. Since the vast majority of the intelligence information on which any country's policy depends comes from analysing the open sources of foreign publications and broadcasts, routine diplomatic reporting, and the activities of newspaper reporters, and only a tiny fraction comes from espionage, the effect on the amount of information available to policymakers would be minimal.

[13] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1., Section 2.
[14] *ibid*.

However, one type of espionage that has not declined but rather expanded after the end of the Cold Was is economic espionage. In the competitive global economy on the verge of the next century, acquiring scientific and technological information for the purpose of gaining an economic advantage has become increasingly important for many countries. Economic espionage can be defined as the use of, or facilitation of, illegal, clandestine, coercive or deceptive means by a foreign government or its surrogates to acquire economic intelligence. Economic espionage exposes the targeted state's companies to unfair disadvantages, jeopardising the jobs, competitiveness of the state, and hampering its research and development investment.

Business and governmental representatives generally agree that the cost of economic espionage activities to individual firms and the economies that host them is very expensive. In it's new national survey, the American Society for Industrial Security (ASIS) estimated that intellectual property losses from foreign and domestic espionage in the United States may have exceeded 300 billion United States dollars (USD) in 1997 alone. The 1997 survey revealed that high-tech companies were the most frequent targets of foreign spies, followed by manufacturing and service industries. Among the most sought-after information were research and development strategies, manufacturing and marketing plans, and customer lists. Information and technology that has been the target of economic espionage includes trade and pricing information, investment strategy, contract details, supplier lists, planning documents, research and development data, technical drawings and computer data-bases.

Some analysts suggest considering an international effort to ban active economic espionage by way of an international treaty that does for economic spying what the General Agreement on Tariffs and Trade aims to do for protectionism. The treaty might even actively encourage openness and the sharing of information, the better to promote scientific research, technological breakthroughs, and economic development[15].

However, in the light of the rise in economics-related spying activities, most of the NATO states have transformed their national requirements for security intelligence to reflect this modified threat environment. Economic security is now one of the main priorities of a security intelligence service.

In Canada, pursuant to Section 2 of the 1984 Act, the CSIS mandate relative to economic espionage is to investigate, when necessary, clandestine activities by foreign governments that are potentially detrimental to the economic and commercial interests of Canada. The CSIS task is also to forewarn the government when the otherwise level playing field of free market competition is deliberately tilted against a Canadian industry.

In addition, the Canadian Security Intelligence Service recently assigned more of its counter-intelligence resources to investigate the activities of foreign states that decide to conduct economic espionage in Canada in order to acquire technology in Canada that can be used for the development of weapons of mass destruction. In this connection, the CSIS monitors the activities of known or suspected foreign intelligence officers in

[15] McCURDY Dave, *Glasnost for the CIA*, Foreign Affairs, Vol. 73, no. 1 (January-February 1994), p. 132.

Canada, and prevent foreign visitors, students and delegates suspected of intelligence activities from gaining access to the country.

A particular type of economic spying activity is known as industrial espionage. In Canada, the CSIS does not investigate industrial espionage - the practice of one private sector company spying on another. If these activities are of a criminal nature, they may be investigated by law enforcement agencies. Civil remedies may be available in this respect as well.

Yet in some of the NATO states security intelligence services help domestic firms in countering industrial espionage as well. In France, for example, a special security institution, the CCSE (*le Comité pour la Compétitivité et la Sécurité Economique*) was created in 1995. Its tasks include fighting the illegal economic activities, such as lobbying and improper pressures on economic players. The DST, in its turn, maintains relations with the top officials in several thousand biggest French companies and provides them with various information programmes. A special economic security and protection of national assets department of the DST has units in the 22 regions to protect French technology. It has been operating for 20 years, not only on behalf of defence industry leaders, but also for pharmaceuticals, telecommunications, the automobile industry, and all manufacturing and service sectors.

Therefore, notwithstanding the decline in espionage and related activities after the end of Cold, countering espionage and sabotage must remain one of the principal tasks in the mandate of a security intelligence service. The service could also keep a careful watch on economic and industrial espionage conducted by other countries' and their companies within the state and warn the domestic firms that have been targeted. Defending the state's economic secrets can reveal interesting facts itself; if a particular country is targeting a specific industry, that may indicate something about that country's economic priorities.

b. Foreign-influenced activities

Espionage and sabotage are not the only kinds of foreign interference in the state affairs which affect national security. Foreign structures may try to interfere with or manipulate the political life of the state in pursuit of their own interests. Such interference may be directed not only by foreign governments, but by foreign political groups and other organisations which have the capacity to influence domestic affairs of the state.

For example, hostile foreign powers may attempt to infiltrate governmental authorities or exert pressure on public officials. In many cases foreign agents interfere with the affairs of ethnic communities within the state by threatening the nationals who have relatives abroad. Clandestine attempts of interference, or those carried out deceptively or involving personal threats such as coercion or blackmail, constitute threats to national security.

In addition to these politically motivated foreign activities, many democratic countries face even more acute threat of economically prompted international organised crime, or trans-national crime. Today, organised crime is no longer limited to a street-level activity. Members of highly sophisticated and organised criminal syndicates are now able to pursue a complex web of lucrative legal and illegal actions world-wide. Contemporary criminal organisations are adaptable, sophisticated, extremely opportunistic and immersed in a full range of illegal and legal practices. While still involved at the lower level with drug-trafficking, prostitution, loan-sharking, illegal gambling and extortion, they have expanded their activities to a quasi-corporate level where they are active in large-scale insurance fraud, the depletion of natural resources, environmental crime, migrant smuggling, bank fraud, tax fraud and corruption. In addition, their frequent use of money earned from the illegal ventures to fund legitimate ones allows trans-national criminals to launder money and earn even greater profits. Trans-national criminal syndicates are not afraid to work globally in any country where legal or bureaucratic loopholes allow them to take advantage of the system. As with international corporations, trans-national criminal organisations are quite willing to work together, often bartering for the use of each other's unique talents to accomplish specific tasks, or to make longer-term arrangements when it suits their needs.

Such groups as Asian triads, Colombian cartels, Japanese *yakuza*, Jamaican posses, *mafia* groups from the USA, Italy, Russia, Central and Eastern European countries, Nigerian crime groups and major outlaw motorcycle gangs are prominent types of such criminal organisations. For example, the largest triad in Hong Kong, the principal centre for the triads, is the *Sun Yee On*, with anywhere from 47,000 to 60,000 members carrying out activities world-wide. Yet the biggest trans-national crime threat is now coming from Russia. Although estimates vary widely, it is generally accepted that 5,000 to 8,000 criminal organisations with as many as 100,000 members control between 25 to 40 percent of Russia's GNP.

The United Nations Organisation (UN) estimates place the cost of various trans-national criminal activities in developed states at two per cent of their GNP. these figures led the 1998 G8 summit in Birmingham to label trans-national criminal activity one of the three major challenges facing the world today.

In Canada, the CSIS monitors trans-national crime under its mandate to investigate foreign-influenced activities detrimental to Canadian interests, as set out in Sections 12 and 2 (b) of the CSIS Act 1984. The service created a Trans-national Criminal Activity Unit in 1996, as part of a government-wide effort to combat this threat. The unit draws on the service's operational and strategic analysis resources in order to collect intelligence related to trans-national crime.

c. Terrorism

The actual or threatening use of violence is often politically motivated, and used as an attempt to force the government to act in a certain way. Hostage taking, kidnapping, bomb threats or assassinations are examples of violent acts that may endanger the lives of

the people and have been used to force political responses. Terrorism within a state may be intended to achieve a political objective in that country. But it may also be intended to affect political affairs in another state; in such a case it is the international terrorism threat.

Terrorism has evolved in the 1960's and 1970's and has become a traditional task nowadays. It is currently the principal task of security intelligence services of the NATO states. Around the world an average of more than one terrorist attack occurs each day. According to data published by the U.S. Department of State, international terrorist incidents rose in 1995 from 322 to 400. Fatalities declined, but injuries increased by a factor of ten. Domestic terrorism in a number of countries also was reported to have continued at a high level - comparative statistics are not available in this connection.

The 1990's have been marred by indiscriminate violence on the part of political and religious extremists, apocalyptic groups, as well as by continuing attacks on tourists and the export of regional conflicts. The most prominent examples include the following incidents: a) on 26 February 1993 Islamic extremists were responsible for a massive explosion in the underground parking garage of New York City's World Trade Center, which rocked the foundation, killing six people and injuring more than 1,000; b) the IRA bombings of civilian targets resumed in the United Kingdom when a car bomb detonated near Canary Wharf in London's East-End on 9 February 1996 killed two people, injuring 100; c) domestic terrorists exploded the deadliest terrorist bomb in American history in front of the Alfred P. Murrah Federal Building in Oklahoma City on 19 April 1995, killing 168 and injuring more than 500; d) American personnel were the target of two terrorist attacks in Saudi Arabia in 1995 and 1996; e) a nerve agent attack in the Tokyo underground by the *Aum Shinrikyo* religious cult on 20 March 1995 killed 12 people and injured 5,500; f) four people were killed on 3 December 1996, when a bomb exploded on the Paris Metro during the evening rush hour, dozens of people were injured by the device, believed planted by Algerian terrorists; g) in 1995, a total of eight bombings or attempted bombings involving the Paris Metro and Paris-Lyon high-speed rail line killed eight people and injured 160; h) Egyptian terrorists carried out three major attacks on tourist buses between 1995 and 1997, as well as an attack on tourists in Luxor in November 1997 in which 58 people were killed; i) the impact of bombings of American embassy buildings in Dar es Sallam and Nairobi in 1998 was a death toll of more than 27 people and 5,000 injuries; j) in March 1999 international tourists were kidnapped by rebel Rwandan soldiers in Uganda; eight people were killed as a result.

The democratic Western countries are particularly vulnerable to terrorist influence because of an open nature of their respective societies. Paradoxically, the most economically prosperous and safe countries and their missions abroad appear to be the most easy, "soft" targets for terrorist activities of various kinds.

Terrorism is usually politically motivated. Political violence continues to find practitioners in established terrorist organisations, as well as in new and evolving groups. Old and undiminished enmities remain, as do associated terrorist groups, sponsors and international links. The growth of Islamic extremism, hostilities in the Balkans, conflicts

in a number of the former Soviet republics in the Central Asia and Caucasus, and turmoil in other areas represent some of the factors spawning new terrorist attacks. Terrorism associated with the Middle East Peace Process and with efforts to resolve the situation in the Northern Ireland are two classic examples. The U.K. has been dealing with manifestations of Irish republican and the so-called loyalist terrorism for over a hundred years. Spain and France have long been concerned with the activities of the so-called ETA terrorist group in the Bask country, and France alone has long been dealing with the terrorist attacks in Corsica. Nationalism and ethnic unrest remain primary motivators for terrorist activity. Impact of conflicts in Algeria, Israel, Punjab and Turkey, enhanced by the presence of large non-European ethnic minorities in Europe, also poses a threat to the security of democratic countries. Increased migration enhances the terrorism threat by way of cummulation of "ethnic pockets" subject to external influence; e.g. such countries as Iran have long been exerting influence upon Islamic communities world-wide.

Religious extremism continues to be a primary and growing source of terrorism. The experience of the World Trade Center bombing signalled new dangers in a less defined terrorism threat with roots in extremist Islamic fundamentalism. Evidence points to extremists who are bound together by hatred of things Western, especially American, and the existence of Israel. Many of these terrorists are Mujahedin-hardened veterans of the Afghan and Bosnian conflicts. In 1998 Islamic Terrorist group leaders signed a *fatwa*, calling for the elimination of all American civilian and military personnel. A new strain of religious or messianic extremism is a particularly disturbing trend in the contemporary terrorist environment. Many of these extremists do not have a traditional political agenda. In such cases, the fear of retaliation that may temper the terrorist's actions is gone, as well as the desire for negotiation and the demand for change[16].

Although ideologically driven terrorism has subsided, it is not a thing of the past; left-wing groups with a history of terrorism remain active in some countries. Particularly worrisome is the growth of right-wing extremism, which feeds on economic dislocation and reaction to patterns of migration.

The terrorism threat has now become increasingly trans-frontier: the so-called GIA networks stretch across several European countries. The Provisional IRA (PIRA) terrorist network extends from Libya and Iran to Northern Ireland and the United Kingdom and further to the continental Europe. State-sponsorship of terrorism persists, providing much-needed logistical support for terrorist groups. Terrorist training centres continue to exist in the Middle East and North Africa.

The terrorism of today is complex, with diminishing emphasis on formalised group structure. The *ad hoc*, individualistic nature of those who form the amorphous membership is in direct contrast to more established terrorist groups. The terrorists of today are often more sophisticated than their predecessors. Globally mobile and knowledgeable about communications, explosives technology and computers, they have contacts around the world. Their activities and targets are difficult to predict. The use of technology, always part of the terrorist arsenal, now has been augmented by encryption

[16] *CSIS Public Report 1998*, p. 5.

and the Internet to facilitate communication and to reach a wider audience. The technology of terrorism is becoming more accessible, but the gun and the bomb retain their favourite status in terrorist attacks. An emerging concern, however, is the possibility of weapons of mass destruction being obtained or constructed by terrorist groups, including chemical and biological agents or nuclear weaponry.

Some terrorist incidents, like the Oklahoma City bombing and the Tokyo underground gas attack, indicate a disturbing trend toward less discriminate attacks and higher casualty rates. The *Aum Shinrikyo* attack in Tokyo is seen as the crossing of a threshold, opening the possibility that other terrorist groups may resort to attacks using weapons of mass destruction or may plan attacks to inflict maximum casualties. As the millennium approaches, more groups with an apocalyptic view of the world may emerge - adding yet another disconcerting element to an already uncertain and volatile environment.

Against the above background, it appears that countering terrorism now requires more effort and resources than ever. When the Canadian Security Intelligence Service was created in 1984, the ratio of operational resources devoted between the service's Counter-Intelligence (CI) and Counter-Terrorism (CT) programs was 80 percent to 20 percent in favour of the CI branch. This ratio is now 60 percent to 40 percent n favour of the Counter-Terrorism program, making public safety and the protection of peoples' lives the number one priority of the CSIS. In the United Kingdom, as a further example, more than 40 percent of the budget of the British Security Service goes to the countering of domestic and international terrorism.

The importance of fight with terrorism is reflected in the establishment of various specific institutions to assist or supplement the activities of a security intelligence service. In France, for example, in addition to the DST, there are several structures created in particular to deal with the terrorism threat. These are an inter-ministerial committee for the fight against terrorism (CILAT, *le Comité Interministériel de Lutte Anti-Terrorite*) and a special anti-terrorist co-ordination unit (UCLAT, *l'Unite de Co-ordination de Lutte Anti-Terroriste*) at the level of the General Directorate of the National Police. Similar structures aimed at finding more effective ways to deal with the terrorism threat exist in other NATO countries as well.

The fight against terrorism requires international co-operation, based on international law, established through international agreements. The NATO states play a role in the international community's development of a legal framework to counter terrorism and to bring terrorists to justice. The Convention on the Suppression of Acts of Nuclear Terrorism within the framework of the United Nations Organisation (UN) and the UN Convention for the Suppression of Terrorist Financing are currently in the draft stages and undergoing further consideration, in addition to the proposed UN Convention on the Suppression of Terrorism. In support of their countries' collaborative efforts to counter terrorist activity, security intelligence services of the NATO countries have developed co-operative arrangements within the international security and intelligence community in pursuit of exchanges of intelligence and expertise.

d. Subversion

Subversive activities as defined in the CSIS Act 1984 include: a) covert, unlawful acts which may undermine the constitutionally established system of government, and b) activities which are directed toward the destruction or overthrow of the constitutionally established system of government by unlawful or unconstitutional means. The definition of subversion in the CSIS Act 1984 distinguishes a line dividing legitimate dissent and subversive activity. While other areas of the CSIS mandate are generally concerned with activities of foreign agents, or activities directed by foreign agents, this definition determines the degree to which the service is allowed to investigate the domestically conceived affairs.

It must be noted that subversion in democratic Western countries is already an historical phenomenon. The concept of subversion was focused on hostility to democratic process. It embraced both extreme left wing (communist) and extreme right wing (fascist) subversive groups which were active throughout the Cold War, soughing to infiltrate and manipulate *bona fide* organisations, such as trade unions or pressure groups, as a way of exercising influence out of proportion to any support they could achieve through the elections. Following the end of the Cold War, the threat from subversive organisations to the parliamentary democracies of the NATO states has declined and is now insignificant. With the collapse of the Soviet communism, and taking into account the intentions and declining capabilities of subversive groups, security intelligence services of many NATO countries scaled down their work in this area.

There is an argument that a security intelligence service should abandon its tradition of targeting "subversives" because the latter term is open to too wide an interpretation. The Canadian Security Intelligence Review Committee[17], for example, has so far been unsuccessful in trying to convince the Parliament to remove the above threat from the list of the CSIS mandate in the CSIS Act 1984, although the CSIS Counter-Subversion Branch was disbanded as far back as 1987. Subversion remains a formal part of the mandate of security intelligence services in most of the NATO states.

e. New threats

On the above analysis it appears that there are four "traditional" tasks of a security intelligence service. However, national security is not a fixed concept. It is impossible to foresee what the scope and degree of even the traditional threats, such as terrorism, will be in the nearest future.

While the new technologies provide new opportunities, they can also give rise to new threats to national security. The rapid changes in travel, transportation, telecommunications, information technology and computers have quickly increased the threats of proliferation of weapons of mass-destruction, drugs and trans-national crime. Young criminals design bombs or toxins with potentially devastating power by using

[17] See below about the activities of the Canadian Security Intelligence Review Committee.

plans they find on the Internet. Not only can the information explosion be used by terrorists or criminals, but it can also be used by those trying to avoid the government's surveillance[18]. Some of these activities have already been mentioned as they technically fall within one or several categories of the four threats reviewed above.

In addition, various computer crimes can be reviewed as a separate example. It is now possible to cross borders silently over the Internet and steal someone's information, or even money, without detection and disappear. It is one of the most rapidly growing types of crime, and it is carried out often by very sophisticated "hackers".

Another threatening trend is the wide use of commercial encryption. Certain encryption hardware and software that are widely available allow criminals or terrorists to use hardly breakable codes. Among such users of encryption to hide their plans was Ramzi Ahmed Yousef, whose laptop computer was seized in Manila in 1996, and who was later convicted in the U.S. for planning to blow up 12 American aircraft in Asia; he was also charged with being the mastermind in the World Trade Center bombing. Another example is the aforementioned *Aum Shinrikyo* gassing of the Tokyo underground. Fortunately, the Japanese security intelligence and police authorities found the keys to the code and decrypted the cult's computer files, containing their further plans for the use of weapons of mass-destruction. One more similar example was a ring of child pornographers in the U.S., who were luring children to meet and engage in sexual acts with men whom they met over the Internet. The pornographers stored obscene pictures of children and messages on encrypted files on their personal computers. Only with special software and a judge's warrant to surreptitiously install the software on a suspect's PC, was the FBI able to gather the evidence. Otherwise, the code would have been unbreakable[19]. The recent scientific discoveries, such as cost-efficient algorithmic procedures for finding prime numbers of high order, will provide every computer expert with a possibility to encrypt information with a virtually unbreakable code. The challenge to a security intelligence service will become even more acute.

2. Functions

In countries where a security intelligence service is separate from the police or law enforcement institutions, e.g. Canada, Germany or the United Kingdom, the service may only apply intelligence means for information collection. It is not empowered to carry out any active measures by way of direct executive action. In such a system the service collects information and present it to the government in the form of analysis or advice. In the countries where security intelligence is collected by the policemen, e.g. France or the United States, the service not only conducts intelligence but also carries out an executive action. In the United States, for example, information obtained by the FBI investigation is presented to an appropriate attorney or official of the Department of Justice, who decide if prosecution, or other action, is warranted. In discussing what kind

[18] *The information flow to Policymakers and Feedback.* Report by Edward J. Appel, of the U.S. National Security Council, at the Conference for NACC/PfP Security Officials held in Brussels on 20-21 November 1996, p. 12.
[19] *ibid.* p. 13.

of duties and functions a security intelligence service may exercise, it is essential to bear in mind the above difference. The following list of duties and functions focuses on the Canadian model, i.e. the system where a security intelligence service is a civil agency separate from the police and not able to take any active measures.

a. Advice to the government and assistance to law enforcement authorities in investigating threats to national security

The CSIS was set up to investigate threats to the security of Canada defined in its statutory mandate. In performing its duties, the CSIS keeps the government informed of activities which may threaten the national security[20]. The service collects information and intelligence on the above activities, and must have the expertise to provide a sensitive analysis and interpretation of the information obtained. In order to be effective, the CSIS must provide advice and early warning to the government[21].

The CSIS does not have law enforcement powers, and law enforcement functions in Canada are responsibility of the police authorities. Pursuant to the provisions in Sections 13 and 14 of the CSIS Act 1984, the CSIS must provide information and intelligence to various law enforcement institutions, in order to assist them in the apprehension and prosecution of those who commit security-related criminal acts. Pursuant to Section 17 of the Act, the CSIS may, under certain conditions, enter into an agreement or otherwise co-operate with other structures not only within the branches of the government, but with other levels of the state institutions, or a government of a foreign country or an international organisation.

The CSIS has a government liaison unit which is responsible for maintaining regular contacts with the governmental institutions in order to obtain their security intelligence requirements. This enables the service to tailor distribution of its information to the specific needs of the other governmental authorities.

The CSIS works closely with the governmental departments and agencies such as Foreign Affairs and International Trade, National Defence, Revenue, Customs, Excise and Taxation, the National Research Council and the Atomic Energy Control Board. These have either an enforcement role or the expertise to support an assessment of the threat by the CSIS. The service's intelligence is shared with a number of other governmental departments and agencies, including Foreign Affairs and International Trade, Immigration, National Defence and the Royal Canadian Mounted Police. As well as investigating threats to national security, the CSIS performs security screening of prospective government employees[22], on request, to all the branches of the government with the exception of the RCMP, which conducts its own security screening.

As observed above, the roles played by security intelligence (CSIS) and law enforcement (RCMP) agencies in Canada are different. That difference is also reflected in

[20] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1., Section 12.
[21] *ibid*.
[22] For a more detailed account of the security screening function see below.

the relationship between the above agencies and the government. Following a common law tradition that the police is responsible only to the judicial branch of power, the government has a very limited involvement in the operations of law enforcement. In defining the place of the CSIS within the wide framework of the state institutions, the CSIS Act 1984 strikes a fair balance between the above principles: a) the CSIS is an agency independent from the RCMP, b) it works closely with both the RCMP and the government, c) while not involved in the detail of day-to-day operations of the CSIS, the government provides a stream of a general policy direction to the CSIS to enable it to adjust to the rapidly changing international environment. Therefore, the Canadian Security Intelligence Service responds to the direction from the government. This is the central characteristic of the relationship envisaged in the CSIS Act 1984. "The very decision as to what affects security and what not, what must be secret and what public is finally a matter of political decision and judgment"[23].

The creation of a separate civilian security intelligence service in Canada was intended to clarify the role of the RCMP and to enable it to concentrate fully on law enforcement. The RCMP also depends on threat assessments by the CSIS to determine the level of protective security required to ensure safety of foreign diplomatic missions and the highest state officials. While the CSIS has been given responsibility to collect, analyse and report information and intelligence, the RCMP should still work closely with the CSIS in areas where an appropriate police action could be taken. In order to specify the competence of the RCMP with respect to law enforcement arising out of the security-related criminal acts, the relevant legislation has been proposed with respect to the concurrent responsibility of the RCMP to investigate offences related to the security of Canada.

On the above analysis it appears that, in dealing with threats to national security, a security intelligence service first collects intelligence and provides intelligence assessments and advises the government. In addition, it works closely with law enforcement institutions in the detection, apprehension and prosecution of those responsible for security-related offences.

A more profound look into these principal functions of a security intelligence service can be taken by way of analysis of what the service does in dealing with particular threats to the national security. In countering terrorism, for example, the role of the CSIS is to provide time-sensitive evaluations of the scope and immediacy of terrorist threats posed by individuals and groups in Canada and abroad. Assessments are made of threats against the high governmental officials travelling in Canada and abroad, foreign statesmen visiting Canada, foreign missions and personnel in Canada, Canadian interests abroad, public safety and transportation security, and special events. In the field of preventing terrorism, the CSIS has developed close communications links with several ethnic communities in Canada. The service's special Community Interview Program helps to assess the likelihood of violence taking place in response to international political developments and so helps the service to identify emerging threats of terrorism.

[23] STANFIELD, Robert, a Canadian MP, intervention during the consideration in the Canadian Parliament of the report of the Mackenzie Commission. *Hansard*, 26 June 1969, p. 10639f.

The CSIS also works very closely with law enforcement agencies to obtain intelligence about membership, infrastructure and methods of terrorist groups through long-term penetration. The service further works closely with the police to deny terrorists funds, weapons and related technology, pre-empt planned attacks, provide appropriate support to the police in the detection, apprehension and prosecution of those responsible for terrorist offences. The CSIS also provides inputs to the Enforcement Information Index, an automated system administered by Citizenship and Immigration Canada that acts to alert immigration and customs officers abroad and at ports of entry to the identity of suspected and known terrorists seeking admission to Canada. The CSIS information enables the immigration officials to refuse applications from individuals suspected of involvement in terrorist activities, effectively barring their entry into Canada. The CSIS continues to take the initiative to launch formal judicial proceedings, in co-operation with the immigration authorities, to remove terrorists from the state. Security certificates are issued jointly by the Solicitor General and the Minister of Citizenship and Immigration, and reviewed by the Federal Court, after which terrorists may be deported.

Co-operation and co-ordination is recognised as essential in managing terrorist threats or incidents. In this respect, the CSIS works closely with other governmental departments and agencies at the federal, provincial and municipal levels. The prime example of this integration and co-ordination can be found in the National Counter-Terrorism Plan (NCTP), which provides for a central co-ordination of the Canadian counter-terrorism program in connection with threats or incidents. The CSIS, along with more than a dozen departments and agencies of the government have an integral role to play under the NCTP. In performing its functions in countering terrorism, the CSIS not only advises the government and co-operates with law enforcement institutions but also maintains international co-operation with foreign governments and intelligence agencies. International co-operation enables the CSIS to be in a better position to establish global terrorist trends and incidents which may or do impact on Canada. The CSIS has developed the system of long-standing, well-established exchange of information with over 100 countries and therefore is in a good position to have access to information which might not be otherwise available to other departments and agencies in Canada.

The field of countering trans-national crime can be put as a further example of interaction between the government and the CSIS on the one hand, and the service and the Canadian law enforcement agencies on the other. The latter have the lead role in the fight against trans-national crime. For this purpose, the Canadian law enforcement authorities collect tactical intelligence, i.e. short-term and operational in nature, geared towards action in the field leading to arrests and prosecutions. The CSIS function is different in this connection; it co-operates with foreign governments which have tasked their intelligence services to help combat this threat and exchanges information with intelligence agencies of other states. It is the responsibility of the service to subsequently provide the Canadian government with reliable information and strategic intelligence on the extent and nature of trans-national crime in Canada. Rather than necessarily leading to an arrest, strategic intelligence is long-term in nature. It provides a comprehensive view of a threat environment, assesses the extent of the threat and points out which areas are at risk. The service's collection of strategic intelligence can also have an important

benefit for law enforcement agencies, as the CSIS is often able to provide them with timely, "spin-off"[24] tactical information.

b. Security screening and assessment in the areas of the government employment, citizenship and immigration

The CSIS Security Screening Program is the service's most visible function. In the course of performing screening enquiries, the CSIS officers come into daily contact with the general public. The service completes thousands of security assessments per year. Security assessments fall into three program categories: the government screening, foreign screening and immigration and citizenship screening.

As regards the government screening, the CSIS reviews files of the government employees who have access to classified information and who therefore need security clearances[25]. The purpose of security assessments is to appraise the loyalty to the state and reliability of prospective government employees. The intent of this exercise is to determine whether persons being considered for security clearances are susceptible to blackmail or likely to become involved in activities detrimental to the national security as defined in Section 2 of the CSIS Act 1984.

In the field of foreign screening, the CSIS has reciprocal screening agreements with the governments of foreign states, foreign agencies and international organisations under which it provides them with security assessments. These agreements are all approved by the Solicitor General after consultation with the Department of Foreign Affairs and International Trade.

The CSIS equally provides security assessments of persons in the areas of citizenship and immigration[26]. The screening of potential immigrants to Canada is a complex process which involves several governmental departments and agencies such as Citizenship and Immigration Canada, Health Canada, Human Resources Development Canada, the RCMP and the CSIS, each of whom have specific responsibilities. In this connection, the CSIS provides advice to the Minister of Citizenship and Immigration on prospective immigrants and refugee claimants. Such advice relates directly to the security inadmissibility criteria contained in the Immigration Act, with the final decision resting with the Minister of Citizenship and Immigration. The CSIS also provides the citizenship and immigration authorities with security assessments on applicants for Canadian citizenship.

In carrying out security screening investigations, the CSIS is precluded by the legislation from using the intrusive investigative techniques which require a warrant[27].

[24] A more detailed explanation of what "spin off" information is follows below.
[25] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1., Section 13.
[26] *ibid*., Section 14.
[27] About the CSIS powers and limitations and the warrant process see below.

Persons affected by security screening decisions are able to apply to the Security Intelligence Review Committee[28] for review of those decisions[29].

The security screening and assessment functions are performed by most of the security intelligence services in the NATO countries (in the United Kingdom, for example, the government screening is known as employment "vetting").

c. Foreign intelligence

One more function of the CSIS is assistance in the collection of foreign intelligence. Foreign intelligence includes information about the capabilities, intentions and activities of foreign states, non-Canadian individuals and bodies[30]. It is in the national interest of the state to acquire intelligence on the activities of foreign powers which have a bearing on the national defence and foreign policy and international economic relations.

It must be noted however that these "foreign-related" activities are conducted by the CSIS only within Canada. The service has no mandate to conduct foreign intelligence operations outside the Canadian territory. Notwithstanding the above limitation, the CSIS has liaison offices in some foreign countries. Liaison officers are involved in the exchange of information which concerns threats to national security of Canada. The task of the CSIS liaison officers abroad is to work with selected foreign police and security intelligence agencies, collecting and analysing openly available information on global trends which may have implications on national security. The CSIS liaison officers are not involved in offensive foreign intelligence operations.

d. Disclosure of information

Another main function of the CSIS is directly related to the above mentioned functions. In the course of its investigations, the service may obtain information not directly related to its primary mandate; the service is not in principle allowed to disclose such "spin off" information[31]. There are situations however where such information is of great value to the activities of other governmental institutions. While it is not part of the service's mandate to specifically seek out such information, if it is obtained in the normal course of its operations, "spin off" information may be released to the appropriate officials. Section 19 of the CSIS Act 1984 authorises disclosing such information to certain officials if that information: a) may be used in a criminal investigation, b) relates to the international relations of the state, c) is relevant to the national defence, and d) is essential in the public interest, and that interest clearly outweighs any invasion of privacy which may result from disclosing that information; in the above case, disclosure must be reported to the Security Intelligence Review Committee.

[28] For a more detailed examination of the status and activities of the Security Intelligence Review Committee see below.
[29] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1., Section 42.
[30] *ibid*., Section 16.
[31] *ibid*., Section 18.

3. Powers and limitations

a. General principles

Discussing the kinds of powers which a security intelligence service might require to fulfil its mandate, the McDonald Commission noted: "because of the secrecy maintained by those who pose the most serious threats to the country's internal security, the security intelligence agency must be authorised to employ a variety of investigative techniques to enable it to collect information. The means available to it must range all the way from studying open sources of research material and obtaining information from citizens, police forces and government agencies (foreign and domestic) to using much more covert and intrusive methods that may involve the use of powers not available under the law to the ordinary citizen"[32]. While "the duty of [a] state to protect its secrets from espionage, its information from unauthorised disclosure, its institutions from subversion and its policies from clandestine influence is indisputable; what are matters for dispute are the organisations and procedures established by the state to meet this responsibility in an area which can touch closely upon the [human rights and] fundamental freedoms"[33].

The protection of "national security" and "economic well-being" and "the prevention of crime" are recognised in Article 8 of the European Convention of Human Rights (ECHR) as providing legitimate basis, in appropriate cases, for interference by a public authority with an individual's right to respect for his private and family life, his home and correspondence. In its established case-law, the European Court of Human Rights recognised that a state may set up a security service on a clear legal basis, and that it must also ensure that there are adequate and effective guarantees against abuse. All European members states of NATO are bound by the requirements of the ECHR. The relevant American and Canadian statutory provisions, including the Canadian Privacy and Canadian Post Corporation Acts and the Fourth Amendment to the U.S. Constitution also protects from unjustified interference with the rights of individuals to be secure in their homes, papers, affects and communications.

In most of the NATO states a proper warrant is required for a security intelligence service to carry out intrusive investigative techniques. In some countries, as Canada and the United States, such warrants are issued by a judge. In the United Kingdom, a final decision as to the issue of a warrant is a matter for a high government officer rather than a court to take.

It must be observed that Article 8 of the ECHR requires no specific judicial confirmation of intrusive investigative techniques. But every technique employed should be proportionate to the legitimate aims sought after in a particular case. In the case of

[32] *Freedom and Security Under the Law*, the Minister of Supply and Services of Canada, Ottawa 1981. Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police ("McDonald Commission"), Second Report, Volume 2, p. 513.
[33] Report of the Royal Commission on Security of Canada ("Mackenzie Commission"), June 1968, § 28.

Klass and Others v. Germany[34] the European Court of Human Rights reviewed the compatibility of a German surveillance statute with the requirements of Article 8 of the Convention. The applicants in this case had complained that their right to privacy was violated in that persons subject to surveillance under the Act at issue were neither informed, nor provided with access to judicial remedies as to the justification of any surveillance measures taken. In the above case the Court held *inter alia*: "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that [a state] must be able, in order effectively to counter such threats, to undertake the secret surveillance. … . The existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime. … . This does not mean that [a state] enjoy[s] an unlimited discretion to subject persons within [its] jurisdiction to secret surveillance. … . [It] may not, in the name of the struggle against espionage and terrorism, adopt whatever measures [it] deem[s] appropriate. … . Whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law."[35] In the above case the Court found that the German Act itself and the review procedures established by it were compatible with Article 8 of the ECHR.

Some of the same concerns arose in the Malone v. the United Kingdom case[36], where the Court reviewed the right to privacy in the context of both interception of phone calls (wiretapping) and the maintenance of a register of numbers dialled from a particular telephone (metering). The Court found that neither practice was "in accordance with law" as required by Article 8 of the ECHR. In relation to the wiretapping issue, the Court addressed two of the counterpart elements of the required legal protection; foreseebility and precision. In this connection the Court held: "the requirement of foreseebility cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence. … [I]t would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."[37] In the above case the Court found that it could

[34] Eur. Court. HR, Klass and Others v. Germany judgment of 6 September 1978, Series A no. 28.
[35] Eur. Court. HR, Klass and Others v. Germany judgment of 6 September 1978, Series A no. 28, p. 23, §§ 48-50.
[36] Eur. Court HR, Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82.
[37] *ibid*., pp. 32-33, §§ 67-68.

not be said with any reasonable certainty what elements of the powers to intercept communications were incorporated in the British legal rules, and what elements remained within the discretion of the executive. In view of the attendant obscurity and uncertainty as to the state of the law in this respect, the Court concluded that "the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society" was lacking[38]. In relation to the metering issue, the Court noted that the practice itself was a legitimate and normal business practice, unlike wiretapping. It found, however, that giving records of metering to the police, without the consent of the person being metered, in the absence of a clear statutory regulation, constituted an unjustified interference with the right to privacy under Article 8 of the ECHR. As a result of the Malone judgment, the Interception of Communications Act was passed by the British Parliament in 1985.

In the recent judgment of Lambert v. France[39] the European Court of Human Rights found a violation of Article 8 of the ECHR in the refusal by the French courts a person *locus standi* to complain of interception of some of his telephone conversations on the ground that it was a third party's line that had been tapped. The Court emphasised that such denial, although being in accordance with domestic law and in pursuance of the legitimate aims, was not necessary in a democratic society within the meaning of Article 8 of the ECHR as it could lead to a very large number of people being deprived of protection of the law laying down arrangements for judicial supervision, namely all those who had conversations on a telephone line other than their own.

On the above analysis it appears that intrusions into privacy of various kinds could be carried out only provided that adequate safeguards against various possible abuses exist. For example, the categories of people liable to a certain intrusion technique and the nature of the acts which may give rise to such a form of investigation should be clearly defined in a law. A time-limit on the duration of the intrusion technique should be specified. As regards telephone tapping, for example, procedures for drawing up the summary reports containing intercepted conversations should be specified. Similarly specified should be the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by a judge or other officer[40]. In addition, a person should have an effective legal remedy to contest the lawfulness of the intrusion technique applied.

It must be observed however that the standards of protection under Article 8 of the ECHR may differ when the information is collected for the purposes other than those of criminal prosecution. For example, pursuant to the practice of the European Court of Human Rights, a state enjoys a wide margin of appreciation under Article 8 of the ECHR in the collection and use of lawfully collected information in such fields as security screening for employment purposes[41].

[38] *ibid*., p. 36, § 79.
[39] Eur. Court HR, Lambert v. France judgment of 24 August 1998, *Reports of Judgments and Decisions* 1998-V.
[40] *mutatis mutandis*, Eur. Court HR, Kruslin v. France judgment of 24 April 1990, Series A no. 176-A, p. 24, § 35.
[41] Eur. Court HR, Leander v. Sweden judgment of 26 March 1987, Series A no. 116.

The potential for invasions by a security intelligence service into privacy, misuse of data and other types of problems will increase as telecommunications and computer technologies become more sophisticated. It follows that more people will contest the effect of the activities of security intelligence services on the enjoyment of their rights to privacy, home and correspondence. Therefore, a clear statutory basis and a tight executive or judicial control is necessary to prevent an abuse of individual's rights.

In addition, methods of security investigation must be proportionate to the threat involved; a security intelligence service must focus its attention only on those individuals or groups who really pose a threat. In addition, the more intensive is the method, the higher should be the authority to permit and control its use[42].

b. Actual powers and limitations

Various surveillance techniques are the most frequently practised methods of secret investigation. Surveillance operations involve the covert observation of targets under investigation in order to obtain intelligence about their movements and the identities of those with whom they are in contact. Where a security intelligence service is separate from the police, surveillance operations are practised at operating in concert with the police. A very important part of a security intelligence work in this connection is employing agents to collect secret intelligence.

It must be noted however that of the many investigative techniques that may be under way throughout a security intelligence service at any one time, only a small proportion will involve the use of intrusive or clandestine techniques. This being so, as long as covert threats to national security persist, a security intelligence service may need to invade the privacy of a very small minority in order to protect the security of the great majority. In order to comply with the principles set out above, a security intelligence service, in planning deployments, should aim to operate with the minimum of intrusion and expense and in proportion to the threat.

The CSIS Act 1984 provides a good legal basis for the CSIS to proceed with intrusive methods of investigation complying with the respect for human rights and fundamental freedoms. Investigations of the CSIS may begin at the level of monitoring public information and proceed to more specialised techniques, including intrusive methods of investigation such as electronic surveillance. The simpler methods of investigation could be used at the discretion of the service, subject to ministerial and management guidelines. If the investigation becomes more intensive, the more strict controls may be placed on the more intrusive techniques required. Pursuant to Sections 21-28 of the CSIS Act 1984, the exercise of certain intrusive techniques is subject to judicial control. The CSIS is not allowed to use these techniques without the warrant of a

[42] *Traditional tasks of an internal security service and its position within government institutions - U.K. presentation*. Report of MANNINGHAM-BULLER E., of the British Security Service, at the Conference for NACC/PfP Security Officials held in Brussels on 20-21 November 1996, p. 2.

judge who must be satisfied that the investigation falls within the mandate and that such intrusive methods are required in the particular circumstances of the investigation.

Electronic surveillance

One of the main powers of the CSIS is the ability to conduct electronic surveillance. In many cases electronic surveillance techniques, such as wiretapping, provide an effective means of obtaining information concerning the plans and activities related to espionage and terrorist groups. Electronic surveillance may be permitted when required, given a proper judicial approval[43].

In Norway, for example, drug-related crime is the only field of criminal investigation in which wiretapping, with a court warrant, is permitted. The discussions are foregoing there to introduce statutory amendments permitting wiretaps in the investigation of other crimes as well.

In the United States, the Foreign Intelligence Surveillance Act governs electronic surveillance and other powers of intelligence collecting authorities in America. A special court should issue a warrant for this purpose. The warrant process is kept secret to protect the investigation.

Intercepting communications

Another important element in the capacity of the CSIS under the above provision of the 1984 Act is its ability to intercept any communication, including telecommunications, written documents, records or other forms of information. The latter phase is intended to include communications which are stored, for example, in digital form in a computer file. An issue of particular concern is that of intercepting and opening of private mail, which is expressly prohibited by the Canada Post Corporation Act. The McDonald Commission argued in this respect that: "it is in their communication links that [foreign spies or terrorists groups] are often the most vulnerable. We think it is unwise to guarantee them a free and convenient channel of communications within Canada by exempting all mail communications from lawful examination by security officers"[44]. Section 21 of the CSIS Act 1984 allows the CSIS to obtain warrants to examine the mail under the controlled conditions.

In the United Kingdom, as a further example, operations to intercept mail and communications on the public telecommunications network must be specifically authorised by a warrant signed by the Secretary of State under the aforementioned Interception of Communications Act 1985.

---

[43] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1, Section 21.

[44] *Freedom and Security Under the Law*, the Minister of Supply and Services of Canada, Ottawa 1981. Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police ("McDonald Commission"), Second Report, Volume 2, p. 578.

Access to confidential personal information

One more element in the system of statutory powers of the ability of the CSIS to have access to confidential personal information. Both the federal and provincial authorities of Canada hold a great deal of information on private individuals, and the confidentiality of this information is ensured by a number of federal statutes, such as the Privacy Act and the Income Tax Act. The CSIS may also have access to this information[45].

Surreptitious search activities

In some cases, covert and surreptitious searches may be the only means available for the CSIS to obtain information or evidence concerning the activities of foreign intelligence agents, terrorists or subversive groups of various kinds. These searches may only be carried out under a proper court warrant in accordance with Section 21 of the CSIS Act 1984.

In the United Kingdom, the Intelligence Services Act 1994 provides for the issue of "property" warrants by the Secretary of State. The effect of such a warrant is to authorise otherwise unlawful entry into, or interference with, someone's property for the purpose of conducting a clandestine search.

The U.S. Foreign Intelligence Surveillance Act governs clandestine search activities in the United States, in order to conduct which a special court warrant is required.

Other activities

In carrying out their duties and responsibilities effectively, the CSIS officials may have to engage in activities which are not specifically authorised by the CSIS Act 1984, and which may ultimately appear to constitute incidental breaches of other Canadian laws. Learned legal opinions differ on the lawfulness of such activities, which might involve relatively minor infractions such as exceeding the speed limit or more serious incidents such as trespassing or damaging private property[46]. However, pursuant to Section 12 of the CSIS Act 1984, an employee of the CSIS could be justified in taking such actions, but only in respect of the actions taken "to the extent that is strictly necessary" for the performance of his statutory duties under the circumstances involved.

4. Controls

In most of the NATO states the heads of governments have statutory leadership in the area of national security. Security intelligence services in these countries are agencies the directions to which at the top level are therefore provided by the governments in power. The heads of governments - Prime Ministers in Canada, France and the United

[45] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1, Section 21.
[46] *CSIS Explanatory Notes*, 1996.

Kingdom, the Federal Chancellor in Germany, and the President in the United States are at the top governmental level of controls over all intelligence structures of these states.

Given the sensitive nature of the security problems defined in the mandate of a security intelligence service, the task of designing a system to provide effective governmental direction, management and control is of highest importance. The mechanism for the above direction and controls is composed of a series of interlocutory elements. "Controls" over a security intelligence service serves to denote "internal" level of accountability of the service. These accountability structures are located within a ministry responsible for the service. They also include the positions of highest executive officials, co-ordinators for all security services, and special inspectors.

a. Controls at the highest level

In Canada, the highest level of controls of the CSIS is executed by the Solicitor General - the Cabinet Minister who is responsible for the CSIS in the Canadian Parliament[47]. However, no exclusive control is given by the CSIS Act 1984 to the Solicitor General so that there would be no potential for political abuse.

The Solicitor General is responsible for the general direction of the service, and issues policy guidelines concerning basic operational procedures. These guidelines, or Ministerial Directions, deal with important issues such as the management of human resources, the protection of foreign citizens in Canada and the co-operation between the CSIS and the RCMP. That the Solicitor General - the Minister plays the role in the policies governing the management and operations of the CSIS is a major departure from the way the Canadian security system was previously structured. The McDonald Commission stated expressly that "in the case of a security intelligence agency, we believe that ministers and senior officials should be actively involved in such decisions because of the ramifications these decisions can have on Canada's system of government and on its relationships with other countries"[48].

As a protection against the Solicitor General issuing guidelines to the CSIS that could undermine the democratic process, the CSIS Act 1984 specifically tasks the Security Intelligence Review Committee[49], the independent review body, to examine these Ministerial Directions.

The Solicitor General is informed of security operations and problems which arise by the Director of the CSIS, the Deputy Minister (Deputy Solicitor General) and the Inspector General[50]. When the CSIS wants to perform the most intrusive operations, such as intercepting communications, it must first seek and obtain the approval of the Solicitor

[47] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1, Section 53.
[48] *Freedom and Security Under the Law*, the Minister of Supply and Services of Canada, Ottawa 1981. Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police ("McDonald Commission"), Second Report, Volume 2, p. 757.
[49] For a more detailed examination of the status and activities of the Security Intelligence Review Committee see below.
[50] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1, Sections 6 and 7.

General before applying to obtain a warrant from the courts[51]. The CSIS must also ask the Solicitor General to approve new arrangements with foreign agencies and the provision of security assessments to other governmental authorities, whether domestic or foreign[52].

This being so, the CSIS Act 1984 provides that the Solicitor General should not be involved in routine policy matters. He cannot override the decisions taken by the Director of the service with respect to specific investigations or with respect to the release of specific reports, when they are periodically submitted to the Solicitor General[53].

The Deputy Minister has a statutory duty to advise the Solicitor General on the need for and effectiveness of his general directions to the CSIS[54]. The Deputy Minister has knowledge of the operational activities of the Service - before the fact by means of his involvement in the warrant application process, on an ongoing basis through the Director's consultation with him and after the fact, by reviewing the Inspector General's certification on the periodic reports submitted by the Director[55].

If an investigation requires the use of a specified intrusive technique, a proposal to this effect is submitted to the Warrant Review Committee of the CSIS (which will include a representative of the Department of Justice and of the Deputy Minister) who have the power to decide whether or not the warrant is appropriate. The service must then apply to and receive the required approval of a judge of the Federal Court to obtain the warrant[56].

In France, Germany and the United Kingdom, the highest level of controls over, respectively, the DST, the FOPC and the MI5 is executed by the Ministers of Interior of these countries (Home Secretary in the United Kingdom). In Canada and the United States, the highest authority in control of, respectively, the CSIS and the FBI are the heads of the justice departments of these states - the Solicitor General in Canada and the Attorney General in the United States.

b. Management

In Canada, the Director of the CSIS is responsible for the management of the CSIS[57]. He consults with the Deputy Minister on the operational policy of the service, on application of warrants, and on other matters for which the Solicitor General indicates such consultation is needed[58]. The Director also submits periodic reports on the CSIS activities to the Solicitor General. Finally, the Director chairs a number of internal committees which further enhance the management and accountability of the CSIS. Two

[51] *ibid*., Section 21.
[52] *ibid*., Section 13.
[53] *ibid*., Sections 6 and 33.
[54] *ibid*.
[55] *ibid*.
[56] *ibid*., Section 21.
[57] *ibid*., Section 4.
[58] *ibid*., Section 7.

of these committees have a direct responsibility for, and authority over, the service's use of investigative techniques.

In most of the NATO states, Directors or Directors General of security intelligence services are in charge of the management of the services' daily affairs.

The role of a Director or Director General is also important to ensure that a security intelligence service does not take any action to further the interests of any political party, in particular the one currently in power. This helps to protect the important principle that in a democracy a security intelligence service must be apolitical; its role is to protect democracy, not to influence its course[59].

c. Inspection

In Canada, the CSIS Act 1984 establishes the position of the Inspector General of the service who acts as "eyes and ears" of the Solicitor General. The Inspector General examines and reports to the latter on the service's compliance with the policies and guidelines laid down by the Solicitor General.

The Inspector General cannot be denied access to the CSIS operational information pursuant to Section 31 of the CSIS Act 1984. The Inspector decides what investigations he will undertake into the service's operations or he can undertake such investigations at the request of the Solicitor General or the Security Intelligence Review Committee. The Inspector's primary means of reporting to the Solicitor General is through an annual certificate, whereby he describes the extent to which he is satisfied with the annual report of the Director of the CSIS, and submits his comments if he finds that the service has contravened the Solicitor General's directions or the CSIS Act 1984[60].

To a large extent, the activities of the Inspector General are not visible to the public or to the parliamentarians, other than the Solicitor General. The Inspector's advice to the latter is highly classified.

In France, inspection of the operation of its intelligence services is carried out by a special administrative commission, the CNCIS (*la Commission Nationale sur le Contrôle des Interceptions de Sécurité*). Separate control, insofar as it relates to the management by the French intelligence services of its computer files, is executed by another special administrative authority, the CNIL (*la Commission Nationale de l'Informatique et des Libertés*).

In the United Kingdom, similarly as in France, the performance of the MI5 is reviewed annually by an inter-departmental sub-committee of the Cabinet Official Committee on Security (SO), also known as the Sub-Committee on the Security Service

[59] *MI5 - The Security Service (Third Edition)*, HMSO Copyright Unit, the Stationery Office, London, 1996, p. 11.
[60] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1, Section 33.

Priorities and Performance (SO(SSPP)). The Committee has the responsibility to review the performance of the Security Service against plans and objectives, examine future Service priorities and to advise the Cabinet Secretary and the PSIS[61] as appropriate. Its membership comprises senior officials from various branches of the Government.

In the United States, positions of Inspector Generals exist in all federal intelligence agencies. The Inspector Generals audit the activities of intelligence services and investigate misbehaviour, and report to the highest executives in control of the intelligence services. In addition, the U.S. President's Foreign Intelligence Advisory Board and Intelligence Oversight Board provide independent, executive-level review of questionable activities of intelligence services.

d. Co-ordination of intelligence agencies

The co-ordination function is important and necessary as intelligence services which fail to co-ordinate their activities may voluntarily or involuntarily obstruct each other's work, carry out tasks twice or fail to recognise information gaps. The co-ordination function covers many tasks.

In Canada, the Prime Minister has the leadership in the area of national security. The Privy Council Office supports the Prime Minister in this connection. A senior official of the PCO, the Co-ordinator of Security and Intelligence, has a mandate from the Prime Minister to co-ordinate activities of all Canadian intelligence services.

In France, the CIR (*le Comité Interminitériel du Renseignement*) was established as far back as 1959. Its statutory footing was amended in 1989. The CIR is the principal co-ordination body of the country's intelligence services. Since there is no parliamentary control over the French intelligence services, the CIR is in charge of all principal questions relating to the intelligence agencies. One of its main functions is adopting the so-called "five-year intelligence plan" and approving the budgets of the intelligence services. The CIR is headed by the Prime Minister and is composed of 10 Ministers representing the main branches of the government. It sits once a month.

In Germany, the position of co-ordinator of intelligence services is held by a Minister of State in the Federal Chancellory. The co-ordinator chairs a weekly conference attended by the heads of the German intelligence services, the supervisory authorities and a representative of the Ministry of Foreign Affairs. He requests every intelligence service to submit reports and communicates with them also on a bilateral level.

In the United Kingdom, the central co-ordination and resourcing of the U.K. intelligence agencies rests with the Cabinet Office. In addition, the Ministerial Committee on the Intelligence Services (IS), whose terms of reference are "to keep under review policy on the security and intelligence services". For example, the IS considered the policy issues connected with the Intelligence Services Act 1994. The Prime Minister is its

[61] PSIS stands for the Permanent Secretaries' Committee on Intelligence Services. For a more detailed account about the PSIS activities see below.

chairman and the other members are the Deputy Prime Minister, Home, Defence and Foreign & Commonwealth Secretaries and the Chancellor of the Exchequer. Ministers are assisted in the co-ordination of the British intelligence agencies by the Permanent Secretaries' Committee on the Intelligence Services (PSIS) which scrutinises the services' annual expenditure forecasts, management plans and intelligence requirements. In addition, the Joint Intelligence Committee (JIC) agrees the broad intelligence requirements and tasking to be laid upon the principal collection agencies for foreign intelligence SIS and GCHQ. MI5 is also in a position to contribute intelligence on some of the JIC requirements (e.g. terrorism). These requirements are reviewed annually in a process managed by the Intelligence Co-ordinator.

In the United States, the CIA Director also holds the position of the Director of Central Intelligence (DCI) who co-ordinates the management and intelligence production responsibilities of the U.S. intelligence community within the NFIP. The NFIP programs are designated jointly by the DCI and the head of an appropriate department or agency (for example, the FBI), or by the President. Two central staffs are attached to the DCI to assist him in this respect. These are the Community Management Staff and the National Intelligence Council.

5. New areas of concern and opportunities in defining and pursuing the tasks

Security intelligence services in most of the NATO states function in principle separately from foreign or military intelligence services. In some countries security intelligence services functions separately from law enforcement agencies as well. At the same time, some overlap between various structures defending national security is inevitable. It becomes harder to distinguish between the traditional notion of security as "foreign" or "domestic", "economic" or "political". In certain situations, it is difficult to establish a proper degree to which the security of a state should be defended; this problem is particularly acute when intelligence gathered by a security intelligence service ends up in a criminal court as evidence in the course of criminal investigation. At the same time, new opportunities arise for a state, in defending its national security, to take advantage of the fields, such as facilities and expertise provided by the private sector. A security intelligence service should be very careful in defining its tasks and in pursuing them.

a. Domestic and foreign intelligence

Combining domestic and foreign intelligence functions creates the possibility that domestic security intelligence and law enforcement will be infected by the secrecy, deception, and ruthlessness that international espionage requires. Dividing responsibilities among different agencies reduces that risk. It also creates a tension and competition between the separate agencies which is itself a safeguard against abuse. However, a strict separation of domestic security intelligence and foreign intelligence proved workable enough while the Cold War continued. Apart from counter-espionage work, there was little overlap between the two. The foreign and military intelligence agencies had a desperate job to do abroad, and they faced a threat that was almost exclusively foreign. Domestic security intelligence, by contrast, had few international

dimensions and almost no way to address international criminal activity. By the 1990's, much had changed. Because the Soviet Union was no longer a threat, some of the recourses devoted to extracting its secrets could be turned to other tasks, to other foreign targets. But some of those targets had a domestic tinge. As topics like terrorism, trans-national crime and proliferation of weapons of mass-destruction rose in priority, it became harder to distinguish between targets of foreign and domestic security intelligence services. Furthermore, it became more difficult to establish targets of domestic security intelligence and law enforcement agencies[62].

Intelligence agencies were not alone in expanding their traditional beat. For example, the United States Department of Justice had gradually extended its reach into foreign affairs. If foreign heads of state could be indicted in the United States for acts committed while in office (as Manuel Noriega and Ferdinand Marcos were in the 1980's), almost any foreign policy problem could wind up as a domestic criminal matter. The recent example in this connection, whereby Spain had requested (and ultimately succeeded in persuading) the United Kingdom to decide to extradite the former Chilean dictator Pinochet to be tried in Spain, only enhances the argument that some matters, traditionally construed as "foreign", nowadays may be interpreted as "domestic".

Given that modern communications make state borders increasingly irrelevant, passport and visa controls become more liberal and technology used by the security offenders is more sophisticated and trans-national, security intelligence services of the NATO states have established close links and exchanges with security services of other allied countries and services. It cannot therefore be said that a security intelligence service is an exclusively "domestic" or "internal" agency. In sum, a security intelligence service now defends internal threats by looking externally to do so[63].

b. Political and economic security

In view of the global economic renewal and international trade, it is more difficult to separate economic policy from national security, foreign and defence policy; because all of the relationships of a state with other powers now involve elements of competition as well as of co-operation, it is perhaps more difficult to tell a friend from foe. All of this makes it more difficult for the managers of a security intelligence service to know where to focus its attention and resources, and there is a danger that various services could become so thinly spread among various crises and issues that the quality of analysis will suffer. Some analysts suggest that, if the world's major trading powers begin viewing each other with suspicion, hoarding economic breakthroughs like atomic secrets and monitoring each other like enemies, the world could easily slide into an economic version of the Cold War[64]. As already observed above, this issue is not all theoretical. The NATO states have long used intelligence services to spy on foreign firms for economic purposes.

[62] BAKER, Stewart A., *Should Spies be Cops?*, Foreign Policy, no. 97 (Winter 1994-1995), p. 37.
[63] *Traditional tasks of an internal security service and its position within government institutions - U.K. presentation*. Report of MANNINGHAM-BULLER E., of the British Security Service, at the Conference for NACC/PfP Security Officials held in Brussels on 20-21 November 1996, p. 4.
[64] McCURDY Dave, *Glasnost for the CIA*, Foreign Affairs, Vol. 73, no. 1 (January-February 1994), p. 127.

Whereas Russia, having a vast intelligence apparatus and little idea what to do with it, is anticipated to expand its decade-old program of industrial espionage. In this respect, public attention was focused on the above issues already back in 1993, with the disclosure that the CIA had warned the U.S. defence firms of espionage directed at them by French intelligence.

It must be observed that analysis of the overall impact of economic espionage, including industrial espionage, is difficult because of industry's reluctance to discuss the issue in detail. In fact, the General Accounting Office - the investigative arm of the U.S. Congress - had to abandon its plan to study the extent and impact of foreign government spying on the U.S. companies when it became clear that firms themselves had little desire to discuss the matter. There are a number of reasons for this corporate reticence. In many cases, firms fear disclosure could harm their reputation or undermine shareholder confidence.

Even the definition of industrial espionage is not so clear. For example, the United States routinely look at foreign economic trends and occasionally brief the U.S. executives about this information. American intelligence agencies provide support to the U.S. officials attending various economic summits, and keep track of other countries' attempts to steal the U.S. industrial secrets. At what point does this activity reach a critical mass and deserve the title "industrial espionage"[65]?

Evaluating activities of multinational companies further disguise the view. How is one to determine today to which country a particular business belongs? Many modern industrial giants have large operations in several, or even many, countries; which ones deserve the protection of a security intelligence service? Would a state protect from espionage all companies doing research within its territory? What if a national firm relocated its headquarters abroad, but still kept many operations or manufacturing sites in its territory; would it still qualify for the protection[66]? A security intelligence service should be very careful in answering the above questions, thereby defining its daily tasks. The ability to distinguish political and economic priorities is crucial to ensure an efficient security intelligence targeting and investigation.

c. Intelligence and evidence

Theoretically, if intelligence gathering is harnessed to the cause of catching and prosecuting criminals, then a security intelligence service should live by the rules of criminal procedure. If the latter is the case, then it can be assumed that a security intelligence service is obliged to search its files for any information that might help the defendant's case. So when the service produces an arguably exculpatory document that the police and prosecution have never shown to the defendant or the judge, it might look like a dereliction of duty. As an example of the kind of procedures that the courts imposed in this respect is found in the United States, in the Brady v. Maryland case of

[65] *ibid*., p. 132.
[66] *ibid*.

1963, where the Supreme Court held that prosecutors may not withhold from a defendant any information in a criminal case which is material and favourable to defence.

In Europe, the basic standards of judicial procedure in civil and criminal matters are set out in Article 6 of the ECHR, which guarantees the right to a fair trial. In accordance with the established practice of the European Court of Human Rights, the concept of a fair trial within the meaning of Article 6 of the Convention includes the fundamental right to adversarial procedure in criminal proceedings. That right means that each party must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other[67].

In the Edwards v. the United Kingdom judgment the European Court of Human Rights considered that it is a requirement of fairness under Article 6 that the prosecution authorities disclose to the defence all material evidence for or against the accused and that the failure to do so in that case gave rise to a defect in the trial proceedings[68]. At the same time, whatever the category or categories of the material and the reason or reasons for non-disclosure, they should be protected by public interest immunity [e.g., non-disclosure of the name of an agent or sensitive investigative technique], which could be served *inter alia* by the considerations of national security, the maintenance of which is not, in certain circumstances, incompatible with the right to a fair trial. Insofar as national security could be involved, the Court has recognised that "the use of confidential material may be unavoidable where national security is at stake, but national authorities are not free from effective control by the domestic courts whenever they choose to assert that national security and terrorism are involved"[69]. Following the above line, in its recent judgment of Tinnelly and Others v. the United Kingdom, concerning restrictions based on national security grounds on the applicants' rights to have a determination by a court of their civil claims that they were victims of unlawful discrimination, the Court accepted that the protection of national security is a legitimate aim which may entail limitations on the right of access to a court, including for the purposes of ensuring the confidentiality of the security screening data. The Court concluded that "the right guaranteed to an applicant under Article 6 of the Convention to submit a dispute to a court or tribunal in order to have a determination of questions of both fact and law cannot be displaced by the *ipse dixit* of the executive"[70]. Therefore, in each case, in considering whether a security intelligence report could be withheld from the defendant, given that the prosecution objects to the disclosure of this material on the grounds of national security, the trial court must balance the public interest in non-disclosure against the importance of the materials in question to the defence.

Therefore, although the above right for a defendant to have access to all the evidence in the case is not absolute, the above mentioned human rights requirements

[67] see, among many other authorities, Eur. Court HR, Brandstetter v. Austria judgment of 28 August 1991, Series A no. 211, p. 27, §§ 66-67.
[68] judgment of 16 December 1992, Series A no. 247-B, p. 35, § 36.
[69] Eur. Court HR, Chahal v. the United Kingdom judgment of 15 November 1996, *Reports of Judgments and Decisions* 1996-V, p. 1866, § 131.
[70] Eur. Court HR, Tinnelly & Sons Ltd and Others and McElduff v. the United Kingdom judgment of 10 July 1998, *Reports of Judgments and Decisions* 1998-IV, p. 1662, § 77.

leave prosecutors with an obligation to review their files and those of investigating authorities for information that could help the defendant. The more closely security intelligence service work with investigators, the more often this obligation will fall on it. For law enforcement authorities, who know that any relevant document will end up in a court and will be presented to the attention of defence, such searches are not welcome. But for a security intelligence service, they can present even a bigger problem. The use of intelligence information is more diverse, and the intelligence gathering process is more fluid. A security intelligence service gathers information in principle destined to policymakers. An error that creeps into an intelligence report may be uncorrected - it may even be repeated - if having that fact exactly right is irrelevant to the policy issues of the day. In addition, intelligence files are classified. Therefore, these files are more likely than law enforcement files to contain casual speculation or fragments or data that could be construed as inculpating. The prospect of releasing those files is thus more likely to come as a painful surprise[71].

The problems of interaction between security intelligence and law enforcement do not end here. To establish the credibility of an intelligence report, prosecutors will want to be briefed on the sources and methods that produced the report. In the United States, for example, to avoid a risk of intelligence sources and methods being disclosed, the Classified Information Procedures Act allows an intelligence agency to propose a sanitised substitute for classified data; but this substitute must be just as good as the original for the defendant's purposes. If it is not, the government must reveal its secrets or drop the investigation[72].

Many analysts agree that it is bad security for a security intelligence service to describe highly sensitive sources and methods to a steady stream of prosecutors - many of whom are young lawyers that will soon be making their own careers out of representing criminal defendants. However, it is even worse when a court says that classified information is relevant to the defence; in such a situation, a security intelligence service will find itself locked in a battle with prosecutors who would rather reveal classified information than give up their investigation. Therefore, in an effort to give law enforcement more information that it does not want very badly and does not use very well, security intelligence officials may be about to stretch the rules that preserve the human rights and fundamental freedoms, flirt with strict judicial limits on how intelligence is gathered, impose unworkable new search duties on a security intelligence service, spread the knowledge of intelligence sources and methods more widely, routinise conflict between prosecutors seeking convictions and agents keeping secrets, and encourage defence lawyers to exploit each of the above problems to hilt the hope of forcing the accusation to abandon prosecution in a particular case[73].

In addition, there are situations where law enforcement agencies themselves can try to exploit the power of a security intelligence service for the purposes inconsistent with the relevant legal limits. As observe above, statutory separation of security

[71] BAKER, Stewart A., Should Spies be Cops?, Foreign Policy, no. 97 (Winter 1994-1995), pp. 39-40.
[72] *ibid.*
[73] *ibid.*

intelligence from law enforcement and the difference between the legal regimes governing their respective investigations is a factor preventing an abuse by both. However, given that both agencies are subordinated to the same government, or, in some countries, such as France, Norway and the United States, they are part of the same law enforcement structure, it is difficult to imagine that security intelligence and law enforcement officers would not circumvent the legal limits in trying to implement the highest political order in certain situations. A former U.S. National Security Agency counsel Stewart A. Baker gave the following account of his experience in similar cases: "[o]ne of my office's jobs at the agency was to review requests for intelligence from drug enforcement agencies. In some cases, we suspected they were trying to shortcut constitutional or statutory limits, and their requests were denied. But I have no illusions that our objections would have prevailed if a different message had been coming from the leaders of the agency and the government"[74].

One more sensitive aspect of co-operation between security intelligence and law enforcement authorities, especially in the field of the fight against drug-related offences, is the use of the so-called *agents provocateurs* to incite commission of an offence. The European Court of Human Rights has held that the use of undercover agents must be restricted and safeguards put in place even in cases concerning the fight against drug trafficking; "while the rise in organised crime undoubtedly requires that appropriate measures be taken, the right to a fair administration of justice nevertheless holds such a prominent place that it cannot be sacrificed for the sake of expedience"[75]. The general requirements of fairness embodied in Article 6 of the ECHR apply to proceedings concerning all types of criminal offence, from the most straightforward to the most complex. "The public interest cannot justify the use of evidence obtained as a result of incitement by an undercover agent"[76]. If the authorities have no good reason to suspect that a person has propensity to crime or is predisposed to commit an offence, any instigation by undercover agents to commit an offence would from the very outset deprive that person of a fair trial within the meaning of Article 6 of the ECHR.

Notwithstanding the above considerations, security intelligence and law enforcement authorities will continue to converge. In the United Kingdom, for example, the Security Service Act 1989 was amended in 1996 by the addition of a serious crime function, pursuant to which the MI5 is now required "to act in support of the activities of the police forces and other law enforcement agencies in the prevention and detection of serious crime". The MI5 officers gave evidence at nine trials, mostly terrorist-connected, between 1992 and 1998[77]. In the British legal system, for example, when a prosecutor considers that some of the records provided by the MI5 should not be disclosed, he files an application of non-disclosure to the Home Secretary, who grants the claim for public interest immunity. But the final decision thereon is ultimately for a judge to take.

[74] *ibid*., p. 40.
[75] Eur. Court HR, Delcourt v. Belgium judgment of 17 January 1970, Series A no. 11, p. 15, § 25.
[76] Eur. Court HR, Teixeira de Castro v. Portugal judgment of 9 June 1998, *Reports of Judgments and Decisions* 1998-IV, p. 1463, § 36.
[77] *MI5 - The Security Service (Third Edition)*, HMSO Copyright Unit, the Stationery Office, London, 1996, pp. 25-26.

Therefore, when planning and carrying out intelligence investigations that may lead to a prosecution, a security intelligence service should constantly have in mind the requirements of a fair trial. For a security intelligence service to perform its function to help the prosecution adequately, the information dissemination system should distinguish between top governmental officials who need intelligence to help them make wise policy choices, and other law enforcement officials who want intelligence to help them in their investigations in criminal cases. Some analysts suggest that highest law enforcement officials - the ones that allocate resources and set strategy - need the same kind of "strategic" intelligence that other policymakers do[78]. If Asian triads are planning massive alien smuggling drives, or if the Russian mob has turned Central Asian collective farms into opium factories, a minister responsible for the security intelligence service and appropriate drug enforcement agencies need to know about it. But such information can and should be fairly tightly controlled. There is not much reason for it to go below the level of a deputy minister. There should be an effective high-level co-ordination between security intelligence and law enforcement agencies, in particular in cases where both communities have a legitimate interest in gathering information about the same person or group. The above co-ordination should be preceded by a careful analysis whether or not law enforcement has a predominant interest in a particular case. If it has, intelligence should be gathered only under law enforcement authority, subject to statutory limits and judicial supervision in accordance with criminal procedure. In such cases, a security intelligence officers will know from the start that they are working for law enforcement authorities.

d. The growing role of the private sector in security intelligence matters

The reason for a security intelligence service is to find and interpret information related to national security that the government needs but cannot obtain from the media or other commercial sources. This information can be expertise that the private sector cannot maintain because it would be unprofitable, information that the private sector will not or cannot collect because it would be unprofitable or too technologically demanding, information that the private sector cannot or will not collect because of legal constraints or risks or tailored products providing this specialised information.

Some analysts consider that there are a lot of unused fields in this respect. Many private organisations are ready provide information. "The question for intelligence planners is what types of information can be provided only by the intelligence community? When the above question is put this way, it soon becomes clear that one is aiming at a moving target. In the Information Age, the non-government, unclassified, commercial sector keeps getting better. Thus, the special niche of the intelligence community needs to be capable of changing continuously, too"[79].

Consider, for example, the fact that private companies are building surveillance hardware and satellites that are potentially so sophisticated that the government feels the need to regulate them. Officials fear that national security could be put at risk if this space

[78] BAKER, Stewart A., Should Spies be Cops?, Foreign Policy, no. 97 (Winter 1994-1995), pp. 47-48.
[79] BERKOWITZ, Bruce D., *Information Age Intelligence*, Foreign Policy, no. 103 (Summer 1996), pp. 42.

imagery were freely available. Moreover, if commercial companies are able and willing to build such satellites, why should the intelligence services do the same? Are still certain types of imagery that only the government structure can produce? If so, how important is the information that this specialised imagery provides? Is it worth the marginal cost and additional risk to maintain a dedicated, government-operated collection system to gather it? Could private industry, properly regulated, provide that specialised information?[80] Satellite imagery is an exotic example, but the same is true in other areas. In the world of human-source reporting, commercial information services are expanding to meet new demands and opportunities. The growth of global-wide television reporting by major private broadcasting companies is yet another example in this respect. As the capabilities of the private sector improve, a security intelligence service will need to keep up with the next frontier of technology or expertise that the private already fills. While one challenge for a security intelligence service is to keep up with these changes, principally the bigger challenge will be to set up a structure that can adapt with the times.

[80] *ibid*., pp. 44-45.

III. External review of a security intelligence service - "who guards the guards themselves?"

1. Structures and procedures for external review

As observed above, domestic legal provisions in the NATO states and various international human rights instruments provide that information about citizens can be obtained only to the extent that is strictly necessary and with respect to activities which may on reasonable grounds be suspected of constituting threats to the national security[81]. An abuse of powers or mismanagement of operations by a security intelligence service may have a serious impact both on the security of a state and on individual citizens. To prevent an abuse or mismanagement, an effective independent review and evaluation of the service's policies and operations is required. Such independent review is envisaged to ensure that imbalances within the security intelligence system can be identified and corrected. To this end, the provisions for an external review of a security intelligence service have been designed in the NATO states. They consist of several elements, including review by judicial and special parliamentary authorities.

Therefore, an "external review" in this section serves to denote the "second" level of accountability, which is "external" to a ministry responsible for a security intelligence service and is at arms' length from the government.

a. Judicial review

In Canada, an external review of the CSIS is done by the judiciary in the form of the warrant process[82]. When the Solicitor General permits the CSIS to conduct clandestine searches or open mail, the service must then apply to the Federal Court. Then the CSIS files an affidavit that contains the detailed information required by the judge for a decision. If the judge approves the application, a time-limited warrant is issued; the CSIS can again apply for the renewal[83].

A similar function is performed by the judicial branch in most of the NATO states. In addition to the warrant process, courts take their part in the control of security intelligence services in the course of criminal, administrative and civil proceedings, including cases when judicial authorities determine charges against any employer of a security service official accused of wrongdoing or misbehaviour.

The United Kingdom, as a further example, has set up an independent Tribunal supported by the Commissioner (a senior judge), to investigate complaints about the MI5 from members of the public. The Commissioner is also responsible for reviewing the issue by the Secretary of State of Property Warrants under the Intelligence Service Act 1994. A separate Tribunal also exists in the United Kingdom to investigate complaints

[81] see, e.g., Section 12 of the CSIS Act 1984.
[82] Also see above.
[83] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1, Section 21.

about interception of communications under the Interception of Communications Act 1985.

b. Review by special parliamentary bodies

The McDonald Commission examined the accountability of the Canadian security intelligence service in the 1970's in considerable depth, and found that the system was not performing adequately. To provide an effective remedy, the McDonald Commission recommended that a joint parliamentary committee be established for sitting Members of Parliament in the House of Commons and the Canadian Senate. This committee would review the activities of all intelligence collecting agencies and departments, along with the assistance of an advisory council on security an intelligence. The advisory council would report on an advisory basis to the Solicitor General and to the joint committee[84]. The Commission also recommended that a separate security appeals tribunal be established to hear complaints relating to refusals to issue security clearances[85]. The Special Committee of the Senate of Canada[86], convened to review the draft legislation for the new Canadian security intelligence agency, expressed concern about partisan politics interfering with the review functions if a joint committee of the Parliament was established.

The Parliament, when it passed the CSIS Act 1984, did not accept the above recommendations of the McDonald Commission. Rather, the Parliament voted for an act that gave the Security Intelligence Review Committee (SIRC) the full powers of an external review body, but with a mandate to review solely the Canadian Security Intelligence Service. The SIRC can, however, hear complaints concerning security clearance cases. This function spreads around the whole of the government.

The CSIS Act 1984 established the SIRC as a committee of three to five members of the Privy Council Office who would serve a maximum of two terms at five years each. The Privy Councillors are persons whose exceptional service to the government as senior advisors has been recognised; most of the Privy Councillors received the title when they were appointed to the Federal Cabinet. The CSIS Act 1984 stipulates that these Privy Councillors cannot be sitting members of the Parliament[87]. The CSIS Act 1984 does not require that the sitting members of the SIRC be politically affiliated with the party in power or the opposition parties. Rather, the government must consult with the opposition parties. As observed above, the CSIS Act 1984 mandates the SIRC to have non-sitting Privy Councillors as the members precisely to avoid the problem of partisanship that could impair the work of the Committee. To date, the appointed members of the SIRC, although possessing attitudes that span the moderate political spectrum, have successfully

[84] *Freedom and Security Under the Law*, the Minister of Supply and Services of Canada, Ottawa 1981. Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police ("McDonald Commission"), Second Report, Volume 2, p. 426.
[85] *ibid*., 781.
[86] *Delicate balance*: *A Security Intelligence Service in a Democratic Society*, the Minister of Supply and Services of Canada, Ottawa 1983. Report of the Special Committee of the Senate of Canada on the Canadian Security Intelligence Service.
[87] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1, Section 34.

worked in a tri-partisan manner, recognising the primary importance of the SIRC for the protection of the state[88].

The CSIS Act 1984 requires that the SIRC members conduct a review of the CSIS operations independently of the government and the Parliament. The Committee must provide an annual report to the Solicitor General, who must table it in the Parliament within fifteen sitting days of receiving it[89]. The annual reports give both the Parliament and the public a summary of the previous years' work performed by the SIRC. The Solicitor General has no authority to edit or otherwise change the SIRC annual report. In its investigations the SIRC performs two main functions that are reflected in its annual reports: a) it reviews the CSIS intelligence activities, and b) entertains complaints relating to the CSIS activities, security clearances, immigration, citizenship and human rights issues. The SIRC also may, throughout the year, provide special reports to the Solicitor General if the Committee believes that particular information warrants his attention, as the Minister responsible for the CSIS[90].

The SIRC has been given the general responsibility to review all duties and functions of the CSIS[91]. The law affords the SIRC a powerful tool to carry out its responsibilities. As is the case with the Inspector General, the CSIS Act 1984 stipulates that the Committee is able to have access to all the information that relates to the CSIS mandate[92]. Not only must the Committee act on behalf of all the Canadian nationals as the external review mechanism for the CSIS, but it must also act as a tribunal to consider complaints about activities carried out by the CSIS and report its findings to the Solicitor General[93]. On a federal government-wide basis, the SIRC acts as a tribunal to investigate and make recommendations regarding all complaints about security clearances involving governmental employees or those who wish to provide goods or services to the government[94].

The Committee does not make decisions on behalf of the government; it rather reports its findings and makes recommendations. However, since the SIRC reports at least once a year, the careful attention to the Committee's recommendations has to be paid. The recent debates between parliamentarians and the SIRC have reinforced the principles on which the Parliament bases the appointment of the SIRC members: a) the SIRC members are chosen to be the trusted representatives of the people rather than a partisan limb of a particular political party, b) the SICR members are appointed "upon good behaviour" for five years to ensure their independence, c) it is important that the SIRC members are not automatically removed when the representation in the House of Commons changes because the SIRC works independently from the Parliament, the

[88] *Parliamentary Oversight and Accountability in Canada*. Report of KLEIN, Maurice M., of the Security Intelligence Review Committee, at the Conference for NACC/PfP Security Officials held in Brussels on 20-21 November 1996, pp. 17-18.
[89] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1, Section 53.
[90] *ibid*., Section 54.
[91] *ibid*., Section 38.
[92] *ibid*., Section 39.
[93] *ibid*., Section 41.
[94] *ibid*., Section 42.

Solicitor general and the Government in power under the 1984 Act, d) the SIRC members should strive to release as much information as possible to the Parliament and to the public; however, they are bound by the statutes governing the release of secret information[95].

The principal responsibility of the Canadian Parliament in reviewing and assessing the CSIS activities is confined to the examination of the SIRC reports tabled by the Solicitor General. Following the submission, the report is referred to the parliamentary Standing Committee on Justice and Legal Affairs of the Parliament. The SIRC members appear on a regular basis in person before the Sub-Committee on National Security. The above body is a sub-committee of the Standing Committee on Justice and Legal Affairs. The SIRC is normally asked to answer questions at two times during the year.

It must be noted that the SIRC is only limited to reviewing the CSIS and has no budgetary control. It also gives rise to some frustration from parliamentarians because the elected representatives do not sit in the SIRC; in certain circumstances parliamentarians could ultimately be denied full factual account of the CSIS work by the SICR members, provided that the information requested is classified and cannot be disclosed for security reasons. However, the Canadian system seems to work well in terms of accountability.

In Germany, for example, there is a special Parliamentary Control Commission which is informed by the Federal Minister of Interior, who is responsible for the FOPC, about the activities of the service in general and about the cases of special importance. The members of the Commission are parliamentarians. The Minister can also refuse to provide information in certain cases if the reasons for withholding the information are well-founded, for example, where the protection of the source is necessary. There is a statutory requirement that reasons be given in cases when the Minister withholds information from the parliamentarians.

An external review system was recently created in the United Kingdom, where the parliamentary Intelligence and Security Committee was set up. The Committee is composed of members of the Houses of Commons and the Lords, appointed by the Prime Minister. Like in Canada, the Committee reports to the Prime Minister rather than to the House of Commons. Some analysts argue that the British model does not afford the Committee sufficient powers for a proper external review of the British intelligence agencies, given in particular that the Committee members are bound by the terms of confidentiality under the Official Secrets Act; As in Canada and Germany, the Committee members might not be able in certain cases to disclose specific details about the services' activities because of the statutory bar even if they are requested to do so by parliamentarians.

[95] *Parliamentary Oversight and Accountability in Canada*. Report of KLEIN, Maurice M., of the Security Intelligence Review Committee, at the Conference for NACC/PfP Security Officials held in Brussels on 20-21 November 1996, pp. 21-22.

The United States Congress has several external review committees, the so-called Select Committees, which keep close track of all the U.S. intelligence agencies. The Select Committees are composed of elected representatives who take oaths of secrecy and review the entire intelligence structure, practices, budgets, laws and regulations. Therefore, the U.S. system of external parliamentary review differs from those in Canada, Germany and the United Kingdom in that American parliamentarians have unlimited access to the information concerning the activities of the U.S. intelligence agencies.

In some of the NATO states, as France, while intelligence services are subject to control by various political and administrative bodies within the government, there is no parliamentary review over the intelligence agencies.

2. Actual investigations by external review bodies - fields of concern

The first Security Intelligence Review Committee, consisting of five members, was appointed by the Governor in Council of Canada in 1984. Since then there have been four Committees. At the outset the SIRC looked at personnel and training issues, as well as operational matters. The first observations of the SIRC were that the CSIS was not willing to bring in staff who were not former policemen. The McDonald Commission had concluded that the RCMP staff who had received police training had been afforded more opportunities than the "civilian members", many of whom had felt as being of "second class"[96]. In its first report the SIRC recommended that this "class" system be removed[97].

The SIRC also examined recruitment policies within the CSIS, finding that there had been not enough women, that there had been not enough francophones and that the French language had not been used enough. The Committee also thought that the CSIS required more people with foreign language skills and an understanding of foreign cultures. The SIRC also emphasised the need for the CSIS to hire employees who had, or could acquire, an understanding of values in cultures that were different from the dominant cultures in Canada[98].

The SIRC also expressed its concern about the reliance of the CSIS on the polygraph, the so-called "lie detector", which was being used in broad employment screening programs. The relevant research from the United States and the United Kingdom supported the Committee's position - the procedure did not meet scientific and psychology test standards for validity and reliability. The SIRC though that a rigorous program of security clearance investigations would provide the most reliable procedure to screen out undesirable applicants[99].

In the early years the SIRC also recommended that the CSIS disband its Counter-Subversion Branch. The Committee thought that, if a person was not suspected of

[96] *Freedom and Security Under the Law*, the Minister of Supply and Services of Canada, Ottawa 1981. Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police ("McDonald Commission"), Second Report, Volume 2, p. 687-688.
[97] *SIRC Annual Report 1985-1986*, p. 5.
[98] *SIRC - Closing the Gaps*, Ottawa 1986.
[99] *ibid*.

sabotage or espionage, and if there were no threats of serious political violence or foreign interference, then the person should not be deemed a security threat. In 1987, after an Independent Advisory Team concurred with this view and the most other SIRC recommendations, the CSIS disbanded the Counter-Subversion Branch[100].

Another significant issue that the SIRC raised was the question of what priority should the analysis and intelligence component play in a security intelligence organisation. The SICR reviewed the Intelligence Assessment Branch of the CSIS, finding that the production of advice to the government appeared to play a secondary role to the collection and retention of the intelligence material. The SICR contested that the role of intelligence production be strengthened within the CSIS, especially in the area of strategic analysis. These recommendations were subsequently implemented[101].

Over the last years the SIRC also commented on a number of other issues which went straight to the core of the CSIS operational activities: the warrant process, targeting, the insufficient reliance on open information and the retention of information which the CSIS had inherited from the RCMP and which could otherwise not be collected under the CSIS Acts 1984. The SIRC criticised the CSIS on a wide range of important issues that the service rejected even as it was transforming itself from within. This is why the SIRC criticism has been now focused on how the CSIS carries out specific investigations, while keeping an eye on the application of the policies of the service and the Ministerial Directions in order to ensure that they remain consistent with the CSIS Act 1984[102].

Norway was one of the first among the NATO states to conduct a transparent historical investigation of the activities of its police security service. In 1994 the Storting appointed the so-called Lund Commission to conduct a probe on the service's activities from 1945. The mandate of the Lund Commission was therefore similar to that of the McDonald Commission in Canada. The Lund Commission's findings were declassified and made public in 1996. The Lund Commission Report documented extensive surveillance of Norwegian citizens throughout the whole post-war period. The Report testified that it had commenced with the "special relations" being established between the Norwegian National Security Police and the leaders of the then ruling Labour Party immediately after the end of World War II. The Norwegian National Security Police had carried on its surveillance of communists and leftists, furnishing information to centrally placed persons in the Labour Party and trade unions until 1970. The Lund Commission Report testified that only openly acknowledging that one had voted for the Communist party had been sufficient to be registered in the files of the National Security Police. In the opinion of the Lund Commission, a complete absence of respect for fundamental human rights was apparent in numerous cases. It was established, for example, that throughout the 1970's the entire editorial staff of several Norwegian publications had been bugged. The Commission strongly suggested that the courts had been very servile

[100] *People and Process in Transition*, the Minister of Supply and Services of Canada, Ottawa 1987. Report to the Solicitor General by the Independent Advisory Team on the Canadian Security Intelligence Service.
[101] *Parliamentary Oversight and Accountability in Canada*. Report of KLEIN, Maurice M., of the Security Intelligence Review Committee, at the Conference for NACC/PfP Security Officials held in Brussels on 20-21 November 1996, p. 15.
[102] *ibid*.

towards the National Security Police: "it was very easy, perhaps too easy to get a court order for wiretaps", as observed by Jostein Erstad, a former chief of the Norwegian security police. The report also showed that that the then ruling governments, socialist or non-socialist, had firmly closed their eyes to the above activities. Moreover, one of the Lund Commission's essential finding's was that the lack of political and legal control over of the security intelligence service had incidentally resulted in a number of collisions between political leaders then in power on the one hand, and the Norwegian security police on the other.

3. Opening up to the public scrutiny

Historically, the only feature of the public opinion on intelligence services has been distrust. The main cause of the public distrust was the lack, or even absence, of information concerning the activities of intelligence agencies.

In 1991, the Canadian government responded to the five-year Parliamentary Review Committee's report on the CSIS Act 1984 and the Security Offences Act 1989 with *On Course*[103]. The Government made a commitment to provide the Parliament and the public with more information on the national security system. This stems from the recognition that effective legislative control over the CSIS must be accompanied by increased public knowledge about its role. The Solicitor General and the CSIS now meet this commitment by providing the Parliament and the public with the Minister's Annual Statement on National Security and the CSIS Public Report and Program Outlook. The Solicitor General, responsible for three main elements of the national security system - security intelligence, security enforcement, and protective security, produces his annual Statement on National Security which constitutes an overview of these three elements. Taken together, the Statement on National Security and the CSIS Public Report are intended to provide the public with an assessment of the current security intelligence environment and the government's efforts to ensure national security. The CSIS Public Report discusses Canada's security environment and the CSIS role in protecting national security. Increased public knowledge about the defensive, domestic nature of the CSIS mandate helps the public to understand how the national security of Canada is safeguarded by the service. The Report also improves the understanding of the purposes and processes of the service and addresses many of the popular myths surrounding security intelligence work.

Opening up of security intelligence in Norway started with the Lund Commission investigation. Following the publication of the Lund Commission Report in 1996, all political parties and the media in Norway accepted the Commission's historical criticism. The Norwegian media was almost unanimous in demanding access to the security intelligence files and redress for those who had been kept under surveillance. As a result of the Lund investigation, the process of reorganisation of the Norwegian Police Security Service was started. The government appointed the so-called Danielsen Committee,

[103] *On Course*: *National Security for the 1990s,* the Solicitor General of Canada, Ottawa 1991. The Government's response to the Report of the House of Commons Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act.

which submitted its report in March 1998. The Danielsen Committee suggested that the Norwegian Police Security Service should be centralised and should conduct itself with greater openness at all levels, that it shoal be more open to external scrutiny, and that it should have fewer staff and increased political steering.

In the United Kingdom, the policy of openness was started only in 1992, i.e. long after the similar processes were commenced in most of the other NATO states. The mandate, functions and organisation of the British Security Service were first put on the public record. In November 1997 the MI5 transferred to the Public Archive Office the first tranche of its own historical archives: its surviving records from the World War I. The late British move of openness was preceded by various scandals, which all started with the publishing in 1986 of *Spycatcher*, memoirs of Peter Wright, a former officer of the British Security Service. The government considered that the memoirs involved a breach of his life-long duty of confidentiality under the Official Secrets Act. As Wright lived in Tasmania, outside the jurisdiction of the British courts, he could not be prosecuted by way of criminal proceedings under the above statute. The government decided to bring a civil action against him in Australia. However, the Crown lost, and not only in Australia, but in Hong-Kong, New Zealand and the United States. Wright, among many other allegations, had stated in his book that the Security Service had tried to destabilise the Labour Government of Harold Wilson in the 1970's. The service denied the above allegations. It must be observed that in 1988 Wright himself admitted that the "Wilson Plot" had been unreliable. The *Spycatcher* affair erupted shortly after another former agent of the Security Service, Cathy Massiter, disclosed in the media that the MI5 had been engaged in the 1970's in targeting and bugging the telephones of entirely legitimate organisations, including trade unions. And in the early 1980's the British media reported that Michael Heseltine, then Defence Secretary, had asked the MI5 for information about links of the Campaign for Nuclear Disarmament and the opposition Labour Party. The service itself did not officially deny the occurrence of the actions alleged, although they clearly fell outside the service's statutory remit.

On the above analysis it appears that the media in democratic states already acts as an unofficial external review tool of intelligence agencies. A security intelligence service should therefore be more rapid and thorough than ever before to allow public officials to correct the truncated, sound-bite version of events so often provided by private persons, newspapers and television news[104]. There is an argument that a security intelligence service should have an official spokesman, officially identified as other governmental officials. However, to this date the public and the media in the NATO states are still not assured that information disclosed to them by a security intelligence service is genuine. In the United Kingdom, for instance, although the Security Service recently came in from the cold by appointing a "media liaison" officer, he remains anonymous, and the British journalists have to refer to him as to "security sources" or "intelligence sources".

[104] McCURDY Dave, *Glasnost for the CIA*, Foreign Affairs, Vol. 73, no. 1 (January-February 1994), p. 127.

In the United States, the efforts in opening up of intelligence services to the public scrutiny are also taking place. Old intelligence records are being declassified and published. The opening up of the U.S. intelligence agencies includes expanded relationships of the U.S. intelligence agencies with colleges and universities. For example, intelligence agencies in the U.S. sponsor unclassified research at institutions that wish to co-operate in a public and accountable fashion. Steps are being taken to make support available to professors for teaching intelligence as an academic subject. Because such actions may be met wit suspicion, however, these relationships must remain voluntary, open to public scrutiny, and consistent with academic practice[105].

At the same time, it must be borne in mind that there is some opposition to the open policies within intelligence agencies. Many officers raised in a regime of secrecy find it difficult to adjust to greater openness. The political culture of intelligence organisations, which is inward-looking and emphasises need-to-know, will not willingly give up information to the public without a clear understanding of the objective[106]. In addition, opening up intelligence agencies to the public debate may have an adverse impact on the willingness of citizens of foreign countries to offer their information to that state. Furthermore, foreign governments, which often volunteer information to a country, will be reluctant to do so if they believe that information provided in confidence will be shared publicly.

Nonetheless, given the recent developments in the global security environment following the end of the Cold War, and provided the rapid development of information and communications technologies, a security intelligence service in a democracy should now seek to assure the public, which has less visibility of its actions than the government does, that it behaves in a lawful way.

[105] GRIES, David D., *Opening Up Secret Intelligence*, Orbis, Vol. 37, no. 3 (Summer 1993), p. 369.
[106] *ibid*., 370-371.

Conclusions

As we approach the next century, modern technology has transformed international environment to provide us with new possibilities in all spheres of life. This being so, the new scientific and technological developments also provide increasingly sophisticated tools for those who seek to achieve political, economic, scientific, military and other objectives by stealing information, money, and ultimately, lives of others. The terrorism threat has unfortunately spread around the world more than ever throughout the history. Furthermore, foreign agents can now enter a particular country, carry out a mission and leave again with remarkable promptness, often within a day or even hours. The acts of political espionage which matured during the period of ideological hostility between democratic and communist states during the Cold War are now being replaced by economic and industrial spying activities between states, even friendly or allied ones, and companies trying to acquire scientific and technological information in the age of competitive global economy. Foreign-influenced political activities of the Cold War period are now overshadowed by trans-national crime undermining economies of democratic states and proliferation of weapons of mass-destruction jeopardising global efforts to establish effective control thereof.

The point of a security intelligence service in this context is to counter the above activities because they constitute threats to national security of a modern democracy. Governments of the NATO states have made different arrangements for addressing these threats in accordance with their own traditions and requirements. No uniform model of the security intelligence system exists. At the same time, drawing from the different experiences and perspectives, as well as similarities of the NATO countries, it can be unequivocally concluded that a security intelligence service is a necessary attribute of a democratic system.

The primary role of a security intelligence service is to advise policymakers on threats to national security. To be able to adjust to the rapidly changing international environment, a security intelligence service needs to obtain a stream of general policy directions from the government. At the same time, another important function of a security intelligence service is to co-operate with law enforcement authorities and to assist them in prosecuting those who commit security-related offences. To perform the above function adequately, a security intelligence service has to develop strong bilateral ties with other services of the state. Therefore, its network of contacts should be of great value and its exchanges and daily co-operation with other authorities should be extensive. The difference of the two above functions reflects the need for a delicate balance in defining the position for a security intelligence service within the governmental structure. Notwithstanding whether a security intelligence service is a separate civil agency or part of the police force, fewer bureaucratic layers should exist between those who order information at the highest political level and those who actually conduct intelligence. It must be borne in mind that a security intelligence service produces valuable intelligence only if asked the right questions. It must be clear from the very beginning what is the purpose of a certain action to be taken; situations when intelligence collected for one

purpose is reviewed in the hopes that it will shed light on a related issue, such as a possible criminal action, should be avoided.

The balance mentioned above depends first and foremost upon the organisation of the basic elements of a security intelligence service - its mandate, functions, powers, controls and external review - into a well designed system. This is why a security intelligence service in a modern democracy should function on the basis of a separate law accommodating the above elements. This statutory remit should permit the service to retain certain autonomy with the governmental structure, establishing proper mechanisms for the service's governmental control and the validation of its decisions, as well as laying down adequate arrangements for the service's external review.

Although being a "domestic" institution, a security intelligence service needs to look abroad to the sources of some "internal" security threats and to "external" security threats of foreign states as the security interests of a state extend beyond its national borders. Many acute threats of today require a concerted international action. A security intelligence service should also be able to exploit new opportunities in defending national security, including those provided by the technological progression of the private sector. In addition, as regards the analysis of its tasks, the service needs to follow the erratic and varying evolution of models of "traditional" and "new" threats to national security. Therefore, while it is important for a security intelligence service to have a clearly defined statutory mandate, the relevant legislation should be flexible enough to allow the service itself to define its tasks, accommodate recourses and prepare for emerging threats in the nearest future.

In designing a system for a security intelligence service, democratic governments of the NATO countries have attempted to define a fair balance between the obligation of a state to protect national security on the one hand, and to respect human rights and fundamental freedoms on the other. The state "must meet both the requirements of security and the requirements of democracy: we must never forget that the fundamental purpose of the former is to secure the latter"[107]. In view of the highest priority given to the protection of human rights and fundamental freedoms, the functioning of a security intelligence service must be based on the principle that the rule of law must be paramount; those protecting national security musty never move downward to the grade of those whose activities they endeavour to counter. In planning deployments, a security intelligence service should seek to act with the minimum of intrusion and expense and in proportion to the threat. Unfortunately, various examples of national and international human rights case-law currently testify that there is a room for improvement both in establishing appropriate statutory safeguards to protect individuals under secret investigation, and in ensuring that in each case the means employed by a security intelligence service are proportionate to the legitimate aims sought after.

[107] *Freedom and Security Under the Law*, the Minister of Supply and Services of Canada, Ottawa 1981. Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police ("McDonald Commission"), Second Report, Volume 2, p. 43.

Over the last years there have been numerous events relating to various scandals in the media and investigations in parliaments and courts of sources and methods that security intelligence services use in conducting intelligence and assisting law enforcement authorities. These events usually resulted in the new or amended laws and the closer external review by special parliamentary bodies and judicial authorities. This also confirms the argument that effective legislative and judicial control over a security intelligence service must be accompanied by increased public knowledge about its role.

The choice of the Canadian example in this paper does not mean that the system of mandate, functions, powers, controls and external review of the Canadian Security Intelligence Service is a pattern to be followed. All systems have their own particular advantages and deficiencies. Even assuming that more effective ways to deal with particular threats exist currently in one country, it may not remain so with the passage of time. What is crucial in this respect is that those responsible for the country's security intelligence system do not lose touch with the rapidly changing domestic and global environment.

To sum up, the role of a security intelligence service is composed of various interlocutory elements which reflect the need for a proper balance between the different necessities in a democratic society. This balance is required to ensure that a security intelligence service should protect national security while respecting human rights and fundamental freedoms, that it should serve the government while securing sufficient autonomy to ensure protection from improper political pressures, that the service's legal basis should be flexible enough to permit it to provide effective security intelligence but that a proper statutory remit should also exist to ensure freedom from abuse. The willingness of states to constantly look for improvement in the search of this balance will confirm their dedication to the principles upon which democratic societies function.

Summary

The purpose of the paper is to reveal the role of a security intelligence service in a modern democratic state by way of review of the Canadian security intelligence system. References to the relevant situation in some other NATO countries, including France, Germany, Norway, the United Kingdom and the United States, are made in comparison in order to emphasise similarities and disclose differences in the way these states counter threats to their national security. To distinguish the role of a security intelligence service, the project touches upon certain aspects pertaining to other intelligence agencies functioning in modern democracies.

The project overviews statutory provisions establishing the mandate, functions, powers, controls and external review of the Canadian Security Intelligence Service and security intelligence agencies of other democratic states. A major part of the work is devoted to the analysis of the relevant formal requirements and procedures governing the operation of a security intelligence service within the governmental structure, and the problems relating to actual implementation of these formal requirements. The way whereby democratic states defend their national security while ensuring the protection of human rights and fundamental freedoms is emphasised in this connection.

The paper contains the review of the current threats to national security of modern democracies, and the analysis of the unstable nature of these phenomena, given the changes in the global security environment following the end of the Cold War. New fields of concern, such as the rise of terrorism, economic and industrial espionage, trans-national and computer crime, proliferation of weapons of mass-destruction and other emerging threats are emphasised in this respect.

Finally, the project refers to certain recent scandals in some of the NATO states prompted by various examples of improper conduct by security intelligence services, disclosed as a result of official investigations by parliamentary bodies and private probes by the media. The above examination confirms the argument that a closer external review of a security intelligence service by parliamentary and judicial authorities is required; in addition, it warrants the need of increased public knowledge about the role of a modern security intelligence service.

References

1. *Amending the CSIS Act*, the Minister of Supply and Services of Canada, Ottawa 1987. Proposals of the SIRC for the Special Committee of the House of Commons.
2. BAKER, Stewart A., *Should Spies be Cops?*, Foreign Policy, no. 97 (Winter 1994-1995).
3. BERKOWITZ, Bruce D., *Information Age Intelligence*, Foreign Policy, no. 103 (Summer 1996).
4. BERKOWITZ, Bruce D., *Information Technology and Intelligence Reform*, Orbis, Vol. 41, no. 1 (Winter 1997).
5. *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 1.
6. *CSIS Explanatory Notes, 1996*.
7. *CSIS Public Report 1998*.
8. *Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)*, Rome, 4.11.1950, European Treaty Series No. 5.
9. *Delicate balance: A Security Intelligence Service in a Democratic Society*, the Minister of Supply and Services of Canada, Ottawa 1983. Report of the Special Committee of the Senate of Canada on the Canadian Security Intelligence Service.
10. Eur. Court HR, Brandstetter v. Austria judgment of 28 August 1991, Series A no. 211.
11. Eur. Court HR, Chahal v. the United Kingdom judgment of 15 November 1996, *Reports of Judgments and Decisions* 1996-V, p. 1866, § 131.
12. Eur. Court HR, Delcourt v. Belgium judgment of 17 January 1970, Series A no. 11.
13. Eur. Court HR, Edwards v. the United Kingdom judgment of 16 December 1992, Series A no. 247-B.
14. Eur. Court. HR, Klass and Others v. Germany judgment of 6 September 1978, Series A no. 28.
15. Eur. Court HR, Kruslin v. France judgment of 24 April 1990, Series A no. 176-A.
16. Eur. Court HR, Lambert v. France judgment of 24 August 1998, *Reports of Judgments and Decisions* 1998-V.
17. Eur. Court HR, Leander v. Sweden judgment of 26 March 1987, Series A no. 116.
18. Eur. Court HR, Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82.
19. Eur. Court HR, Teixeira de Castro v. Portugal judgment of 9 June 1998, *Reports of Judgments and Decisions* 1998-IV.
20. Eur. Court HR, Tinnelly & Sons Ltd and Others and McElduff v. the United Kingdom judgment of 10 July 1998, *Reports of Judgments and Decisions* 1998-IV.
21. *Freedom and Security Under the Law*, the Minister of Supply and Services of Canada, Ottawa 1981. Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police ("McDonald Commission").
22. GRIES, David D., *Opening Up Secret Intelligence*, Orbis, Vol. 37, no. 3 (Summer 1993).
23. *Hansard*, 26 June 1969, p. 10639f.
24. HILSMAN, Roger, *Does the CIA Still Have a Role?*, Foreign Affairs, Vol. 74, no. 5 (September-October 1995).
26. *In Flux But Not in Crisis*, the Minister of Supply and Services of Canada, Ottawa 1990. Report of the Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act.
27. KISSINGER, Henry, *Diplomacy*, Touchstone, New York 1995.
28. McCURDY Dave, *Glasnost for the CIA*, Foreign Affairs, Vol. 73, no. 1 (January-February 1994).
29. *MI5 - The Security service (Third Edition)*, HMSO Copyright Unit, the Stationery Office, London, 1996.
30. *On Course: National Security for the 1990s*, the Solicitor General of Canada, Ottawa 1991. The Government's response to the Report of the House of Commons Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act.
31. *Parliamentary Oversight and Accountability in Canada*. Report of KLEIN, Maurice M., of the Security Intelligence Review Committee, at the Conference for NACC/PfP Security Officials held in Brussels on 20-21 November 1996.
32. *People and Process in Transition*, the Minister of Supply and Services of Canada, Ottawa 1987. Report to the Solicitor General by the Independent Advisory Team on the Canadian Security Intelligence Service.

33. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, Government Printing Office, Washington, D.C. 1996. Report of the Commission on Roles and Capabilities of the United States Intelligence Community.
34. Report of the Royal Commission on Security of Canada ("Mackenzie Commission"), Ottawa, 1968.
35. RUTLAND, Peter, *Mission: Improbable*, Transition, Vol. 2, no. 22 (1 November 1996).
36. *SIRC Annual Report 1985-1986*.
37. *SIRC - Closing the Gaps*, Ottawa 1986.
38. *The information flow to Policymakers and Feedback*. Report by Edward J. Appel, of the U.S. National Security Council, at the Conference for NACC/PfP Security Officials held in Brussels on 20-21 November 1996.
39. *Traditional tasks of an internal security service and its position within government institutions - U.K. presentation*. Report of MANNINGHAM-BULLER E., of the British Security Service, at the Conference for NACC/PfP Security Officials held in Brussels on 20-21 November 1996.

Websites:

The CSIS official home-page at www.csis-csrs.gc.ca
The SIRC official home-page at www.sirc-csars.gc.ca
The FBI official home-page at www.fbi.gov
The MI5 official home-page at www.mi5.gov.uk