THE GLOBALIZATION OF TERRORISM: Canada's Intelligence Response to the Post-September 11 Threat Environment

BY Martin Rudner

THE TERRORIST ATTACKS OF SEPTEMBER 11 CATAPULTED CANADA'S INTELLIGENCE COMMUNITY TO THE FOREFRONT OF OUR SECURITY AND DEFENCE EFFORT. IN THE URGENT SCRAMBLE TO PROTECT PUBLIC SAFETY AND VULNERABLE INTERESTS, CANADIANS TURNED TO THEIR INTELLIGENCE SERVICES TO COUNTERACT AN AUDACIOUS AND ELUSIVE THREAT FROM GLOBAL TERRORISM. TO BE SURE, TERRORIST THREATS WERE NOT NEW TO CANADA. CANADIANS HAD THEMSELVES BEEN TARGETED BY INTERNATIONAL TERRORISTS IN THE RECENT PAST, AND OUR TERRITORY WAS USED AS A SANCTUARY AND BASE OF OPERATIONS BY INTERNATIONAL TERRORIST GROUPS ATTACKING OTHER FRIENDLY AND ALLIED COUNTRIES. NEVERTHELESS, CANADA'S RESPONSE TO THE ATTACKS OF SEPTEMBER 11 SIGNIFIED A SIGNIFICANT ESCALATION OF THIS COUNTRY'S COUNTER-TERRORISM COMMITMENTS. THIS WAS MANIFESTED IN A SUBSTANTIAL ROLE EXPANSION OF CANADA'S INTELLIGENCE COMMUNITY, A SHARPENING OF ITS LEGISLATIVE WEAPONRY, INTENSIFIED INTERNATIONAL COOPERATION, AND THE INTRODUCTION OF AN EXTENSIVE ARRAY OF REGULATORY INSTRUMENTS AND MEASURES TO SAFEGUARD PUBLIC SECURITY, PROTECT CRITICAL INFRASTRUCTURE, AND DISRUPT TERRORIST NETWORKS AND ACTIVITIES IN CANADA AND THEIR EXTERNAL LINKAGES. THE DISTINCTIVE TASKING OF THE INTELLIGENCE COMMUNITY IN THIS COUNTER-TERRORISM EFFORT IS TO PROVIDE GOVERNMENT AND LAW ENFORCEMENT AGENCIES WITH TIMELY, ACCURATE AND ACTIONABLE INFORMATION ON THREATS TO NATIONAL SECURITY.

THE TERRORIST THREAT ENVIRONMENT

Even prior to September 11, international terrorism figured prominently on the threat assessments of Canada's intelligence community. The annual reports of the Canadian Security Intelligence Service (CSIS) noted regularly that many of the world's terrorist groups had established a presence in this country. Canada's open society, and the presence here of large, identifiable homeland communities from societies in conflict, created a distinctly attractive arena for international terrorist networks. Whereas virtually all of the terrorist groups with a presence in Canada were engaged in ethnic, religious or nationalist conflicts elsewhere in the world, these groups did not scruple to sometimes mount attacks in this country and against Canadians. International terrorist organizations and rogue states have targeted individuals, groups and institutions in Canada, to intimidate the uncommitted, wreak vengeance on adversaries or gain public attention for their cause. Among the more notorious incidents were the Air India bombing, the assassinations of Turkish diplomats, a plot to attack on the Montreal Jewish institutions, and the foiled Millennium attempt to bomb Los Angeles International Airport.

Terrorist organizations typically maintained a presence in Canada in order to raise and transfer funds, to create false identities for operatives, to procure weaponry and material, to set up operational sanctuaries, and to support infiltration across the border to the United States or overseas. Local cells of groups like Al-Jihad engaged in financial fraud and theft, identity and document forgery, and people smuggling in support of their parent terrorist networks. Some terrorist groups, like the Liberation Tigers of Tamil Eelam, became extensively involved in criminal racketeering to generate financing for their insurgency war in Sri Lanka. Terrorist criminal syndicates were active in drug trafficking, immigrant smuggling, commercial fraud, and extortion from homeland residents in this country and elsewhere. International terrorist groups were reputed to have taken over legitimate businesses and even Non-Governmental Organizations (NGOs) as a means of money laundering and in order to disguise their activities.

As the economic downturn that followed from the attacks of September 11 amply demonstrates, international terrorism can wreak havoc on the economies of many countries, and not solely the target. Over and above the costs of their criminal activities and destruction of property and infrastructure, international terrorism has caused far-reaching economic destabilization and massive capital losses on world financial markets.. The mere risk of terrorist activities taking place in or through Canada can suffice to impel the United States to tighten controls on cross-border movements of goods and persons. This could cost the Canadians dearly.

One of the more alarming aspects of international terrorism relate to the reported attempts by terrorist groups to deploy radiological, chemical or biological weapons of mass destruction (WMD). Canada may be vulnerable both as a locale for illicit access to radiological, chemical or biological technologies and as a possible target for WMD attacks. It is known than Al-Qaeda attempted to develop radiological, chemical and biological weaponry on its own in Afghanistan, and perhaps elsewhere as well, so far unsuccessfully. There is now a risk that terrorists seeking WMD proliferation may dispatch students or researchers to enroll in university programs or join research institutions in countries like Canada in order to gain access to dual-use technologies and weapons-related expertise. Given the sensibilities of academe, countering any such espionage would call for considerable sensitivity and dexterity on the part of security authorities.

Among suspect groups, the Al-Qaeda network and its affiliates and partners constitute certainly the most dangerous threat to the security of Canada, its allies and friendly countries. This threat environment is characterized by elusive, widely-dispersed and loosely structured terrorist networks, formed in tightly knit cells embedded in various Islamic communities, and capable of deploying large numbers of trained, committed operatives almost anywhere in the world. These networks are difficult and hazardous to penetrate. In Canada, the primary responsibility for counter-terrorist intelligence is vested in CSIS, working together with other components of the Security and Intelligence Community, pertinent government departments (*e.g.* Citizenship and Immigration, Department of Justice), the Royal Canadian Mounted Police (RCMP) and local police forces.

EXPANSION OF THE INTELLIGENCE COMMUNITY

In the immediate aftermath of the terrorist attacks of September 11, the Government of Canada injected a increased funding of almost $47 million to CSIS and to the Communications Security Establishment (CSE), the signals intelligence agency, to expedite improvements in their capabilities to collect foreign intelligence. Some $37 million of this went to CSE for research and development and to upgrade its interception technology infrastructure, while CSIS obtained authorization to augment its operational staffing by over 300 during the coming years. After more than a decade of cutbacks, Canada's two major intelligence collection agencies were now to be given resources to deal with the new threat environment posed by global terrorism. The RCMP for its part was given an additional $54 million to bolster up its counter-terrorism capabilities. Subsequently, the 2001-02 federal budget provided an additional $7.7 billion to strengthen government capacity to combat terrorism and ensure national security.

CSIS is a civilian security intelligence agency, created by an Act of Parliament (CSIS Act) in 1984. Historically, CSIS and its predecessor, the RCMP Security Service concentrated primarily on Communist subversion and espionage, and on perceived threats of separatist violence in Quebec Since the early 1990s, however, CSIS has refocused its security intelligence efforts more towards counter-terrorism, economic espionage, WMD proliferation, and foreign influenced activities deemed detrimental to the national interests of Canada. Under its legislative authority, CSIS can investigate any individual, group or organization suspected of constituting a threat to the

security of Canada. CSIS conducts investigations, analyzes its findings and advises government and law enforcement agencies on activities deemed threatening to national security.

In the aftermath of September 11, CSIS is endeavoring to improve and extend its tradecraft, linguistic and political-cultural proficiencies to run agents in highly sensitive and perilous counter-terrorism operations.

A very large proportion of the foreign intelligence provided to the Canadian government derives from communications interceptions on the part of CSE and its partner signals intelligence agencies in the US, UK, Australia and New Zealand. CSE and its partners deploy sophisticated interception technologies to monitor terrestrial, microwave, radio and satellite communications, along with other electromagnetic emissions. These intercepts are then processed through advanced computer systems programmed to search for specific telephone numbers, voice recognition patterns or key words, and to decrypt text. CSE is, arguably, the most secretive entity of the Government of Canada; for decades the very existence was a classified secret. It had no statutory mandate until recently, and virtually all details of its resources, objectives and operations are still shrouded in official secrecy.

In the aftermath of September 11, CSIS is endeavoring to improve and extend its tradecraft, linguistic and political-cultural proficiencies to run agents in highly sensitive and perilous counter-terrorism operations.

The new counter-terrorism legislation enacted in Bill C-36, in the aftermath of September 11, empowered CSE to monitor communications to or from Canada (hitherto not permissible) specifically for the collection of foreign intelligence, subject to authorization by the Minister of National Defence. Communications intelligence reportedly had some success monitoring Al-Qaeda, including operations in Canada. Yet, the effectiveness of this source subsequently may have been compromised by unfortunate leaks from abroad. In any event, it was becoming clear that the increasing availability of encryption and advances in communication security were eroding the interception and cryptanalysis capabilities of signals intelligence. In order to sustain an effective role for communications intelligence in future massive new investment in costly and innovative technologies for interception and cryptanalysis and, indeed, analytical capacity building will be called for. Canada may have no other option but to turn to its allies, and in particular the United States, for the futuristic technologies required for the collection of foreign intelligence. Indeed, Canadian dependence on its American intelligence connection will likely grow even more acute apropos some of the most technically sophisticated technologies, such as satellite imagery.

The revitalization of CSIS and CSE was accompanied by a far-reaching role expansion of other components of the Canadian intelligence community. Existing intelligence units in government departments like Foreign Affairs and International Trade, Citizenship and Immigration Canada, Transport Canada, and the Canadian Customs and Revenue Agency were considerably reinforced. As well, the recently established Office for Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) was mandated to protect Canada's cyber and physical infrastructure, and a new Financial Transactions and Reports Analysis Centre (FINTRAC) was created to monitor suspicious international financial transactions. The Intelligence Assessment Secretariat at the Privy Council Office was also strengthened.

The expansion of Canada's intelligence community highlighted the challenges of operational co-ordination. Up to now the mechanisms for co-ordination among the decentralized and increasing disparate array of specialized agencies and units has always been weak, as they work mainly through periodic consultations and moral suasion. Deficiencies in the co-ordination and sharing of intelligence between organizations like CSIS, Citizenship and Immigration Canada and the RCMP, for example, reportedly resulted in mishaps in the identification of terrorist suspects. A tighter fusion of the intelligence capabilities of all components of Canada's security and intelligence community is a prerequisite for operational effectiveness. At the Cabinet level, an *ad hoc* Committee on Security was set up under the Deputy Prime Minister to oversee the direction and management of Canada's national security response to the threat of global terrorism.

STRENGTHENING THE LEGISLATIVE ARMOURY

The intelligence effort against international terrorism will have to be targeted against relatively small and amorphous sleeper cells, elusive networks, obscure organizations, suspect elements in homeland communities, and rogue governments, probably over prolonged periods of time. Intelligence operations will doubtless undergo an offensive mode to identify, penetrate, monitor and counter the terrorist threat. In order to bring suspected terrorist operative and their co-conspirators to justice, intelligence will have to work closely with law enforcement. In the aftermath of September 11, new anti-terrorism legislation has been introduced in Canada and in other countries to equip intelligence agencies and police forces with enhanced powers of surveillance and investigation, and allowed the police expanded powers of arrest. Increased attention has also being devoted to the phenomenon of illicit trans-national fund-raising and money laundering in support of international terrorism. These new legislative initiatives aroused strong reactions, leading to amendments and wholesale revisions being adopted to satisfy parliamentary and public concerns about the appropriate balance being struck between national security requirements and the preservation of civil liberties.

The Anti-Terrorism Act, which came into force in December, 2001, defined and designated terrorist groups and activities and introduced new measures designed to better enable intelligence and law enforcement agencies to identify, prosecute, convict and punish terrorist operatives and co-conspirators in

Canada. The Act gave police and national security agencies extraordinary powers of preventive detention and to compel testimony in investigative hearings. Furthermore, the Act provided enhanced authority for electronic surveillance of suspected terrorist groups, and established, for the first time, a statutory basis for CSE. To be sure, human rights safeguards were built in to the Act, including a sunset provision of five years for prevention arrest and investigative hearings, unless renewed for a further five years by resolution of both Houses of Parliament.

Along with this Anti-Terrorism law, which bolstered up the terrorism provisions of criminal law, the Government also introduced a second Bill, C-42, aimed at strengthening its own legal-institutional capacity to combat terrorism. Faced with intense public and parliamentary concern over certain of its provisions, this legislation was subsequently withdrawn and replaced with Bill C-55, the Public Safety Act. The new legislation included provisions for improving airport and aviation security, deterring the proliferation of biological weapons and related WMD technologies, and expedites coordination and the sharing of relevant information among government departments, national security and law enforcement agencies. It still retained the controversial clauses enabling the declaration any part of the country a Controlled Access Military Zone, albeit now for more limited, specified purposes. It also gives legal authority for FINTRAC to monitor and report on suspicious international financial transactions.

Canada was slow to enact legislation proscribing international terrorist organizations and criminalizing their fundraising activities, but by October of 2001 new regulations were enacted to block money transfers to terrorist organizations, in anticipation of further changes to the law regarding the suppression of terrorist financing. In addition, a raft of new regulations and orders were introduced so as to tighten security in the sensitive domains of immigration and citizenship, cross-border movement, civil aviation, shipping and ports, science and technology research, public health and critical infrastructure. Even at the provincial level, governments took steps to reinforce the security of their own respective areas of jurisdiction against the elusive threat of terrorism.

The heightened involvement of national security services in counter-terrorism, and in co-operating and information sharing with police and prosecutors, risks blurring the boundaries between intelligence and law enforcement. The new anti-terrorism legislation implies a rebalancing of the scales of justice between the requirements for national security and the principles of civil liberty, somewhat to the side of public safety. Yet, intelligence is characteristically obsessive about protecting its sources and methods; law enforcement must always comply with the rules of evidence and judicial procedures; the twain do not always meet, and resultant tensions can impede co-operation. The price of failure can be high: anything that jeopardizes the gathering of admissible evidence can compromise the prosecution of terrorists under law, any deficiency in law enforcement could culminate in an intelligence failure to prevent terrorist acts.

INTERNATIONAL COALITION-BUILDING

International co-operation in intelligence collection has always played a pivotal part in Canada's foreign and security intelligence efforts. In order to acquire foreign intelligence needed by government, and lacking a dedicated foreign intelligence service of its own, Canada has embarked on a wide range of bilateral liaison relationships with many other countries, and co-operates with several plurilateral groupings, in order to access and share foreign intelligence in relation to specific threats. Since the end of the Cold War these international intelligence relationships have refocused their attention to deal with international terrorism, transnational crime, drug trafficking, money laundering, financial fraud, people smuggling and WMD proliferation. The aftermath of September 11 inspired a vast extension of international co-operation in the intelligence domain, with many countries across the world acting to share information and collaborate in operations against suspected terrorists, cells and networks. This intelligence coalition has been just as important to the campaign against global terrorism as its counterpart diplomatic and military coalitions.

The longest standing arrangement involving Canada in international co-operation and intelligence sharing is the so-called UKUSA security agreement on signals intelligence, in force since 1948. The architecture of this agreement embraces the US, UK, Canada, Australia and New Zealand, as well as other more limited "third parties" (*e.g.* Sweden, Norway, the Netherlands) in global collaborative mechanism for signals intelligence collection, processing and product sharing. Canada's role in the UKUSA alliance was valued not so much for this country's inherent capabilities in signals intelligence production, which remains modest, as for its unique geographic advantages. During the Cold War, Canadian signals intelligence concentrated on communications across the northern Soviet Union and East Asia; later, the interception facilities at Leitrim, Ontario appeared to target Latin American satellite relays. As *quid pro quo* for this coverage, the UKUSA alliance offered Canada shared access to a global capability to collect and deliver real-time communications interceptions on foreign intelligence targets. As well, the agreement gave Canada a place at the high level strategy councils of its American and British allies, along with privileged access to the most sophisticated technologies for intelligence and defence generally.

The global interception capabilities available to the UKUSA allies from space based, terrestrial and submarine facilities are integrated into a seamlessly networked signals intelligence processing system. At the functional heart of this system is the *Echelon* "Dictionary", a specialized, powerful computer system having the capacity to store a comprehensive database on designated organizations or individuals, including names, topics of interest, addresses, telephone numbers and other criteria for target identification. Highly secret still, the *Echelon* system is able to process and sort through vast flows of telecommunications traffic to or from most parts of the world and identify specifically targeted messaging. The great challenge confronting the UKUSA partners has been how to handle the vast influx of intercepts, which can

overwhelm their capacity to analyze and translate raw communications, as reportedly occurred just before September 11.

The reciprocal sharing arrangement under UKUSA gives each partner, including CSE, virtually automatic access to the entire interception infrastructure and capability, although only for its own *Echelon* "watch list". Following the attacks of September 11, Canada reportedly intercepted encrypted communications from international terrorist networks warning of renewed terrorist assaults, which were forwarded to the American authorities. The Anti-Terrorism Act of 2001 empowered CSE to monitor communications to or from Canada, something hitherto not permissible, specifically for the collection of foreign intelligence. It is germane to note in this regard that the CSE Commissioner, who is responsible for executive oversight of the organization, has provided a public assurance that CSE does not use its international alliances to circumvent the laws of Canada, or provide allies with communications they could not otherwise legally collect for themselves.

Apart from the UKUSA alliance, Canada also relies on bilateral liaison and other plurilateral arrangements to acquire foreign intelligence. While CSIS can and does operate abroad in keeping with its statutory mandate regarding the security of Canada, the very limited extent of foreign intelligence collection abroad engenders a high propensity to exchange information with others. At present, Canada maintains bilateral liaison relations with nearly 150 countries. Much of this liaison is taken up with immigration and visa security screening. Yet, liaison with the intelligence services of even friendly countries is always an ambiguous affair. It may well be the case that liaison relationships may curtail some foreign intelligence activities in Canada, however there is a strong propensity among intelligence services to monitor neutral and even friendly countries, which can render international co-operation somewhat awkward. As it is said, "There are no friendly secret services, only the secret services of friendly states."

Canada also participates in several plurilateral intelligence sharing arrangements. These arrangements tend to be highly secretive, going by code names that are rarely affirmed. The Kilowatt group was formed in the 1970s by Belgium, Canada, France, Germany, Ireland, Israel, Italy, Luxembourg, Netherlands, Norway, Switzerland, Sweden and UK to deal with Arab terrorism, in parallel with the Megaton group that concentrated on other (non-Arab) terrorist phenomena. Later, the Egmond group was formed to deal with terrorist financial flows and with money laundering. These plurilateral sharing arrangements are backed by integrated data banks on terrorist organizations, operatives, methods and links. Along with the so-called Club of Berne, these groupings are intended to facilitate the synthesizing of available intelligence, and thereby to enhance the counter-terrorism capabilities of participating countries.

The post September 11 war on terrorism engendered an urgent effort to penetrate the tightly-knit, amorphous cells and loosely structured networks of Al-Qaeda and its affiliates. This has prompted an extension of operational co-operation with intelligence services of countries in the Middle East, South Asia and elsewhere, with whom in some cases such dealings would hitherto have been unthinkable. Exchanges of intelligence are reportedly taking place even with countries like Iran, Libya, Sudan and Syria, whose security services may have penetrated these networks and have information to trade. There is also far-reaching international cooperation in investigations, as demonstrated by the case of the Canadian Al-Qaeda suspect, Mohammed Mansour Jarabah, who was tracked from Singapore to Oman, arrested there and handed over to CSIS, who in turn made him available for interrogation in the United States. In other cases arrested Al-Qaeda suspects have been sent, secretly, for interrogation in tougher, hardened jurisdictions like Egypt or Jordan. In return for gaining the results of such investigations, countries like Canada may possibly be asked to reciprocate by sharing sensitive information regarding exiles and opposition groups, or strategic intelligence about third countries. The imperative for intelligence co-operation can sometimes make strange international bedfellows, and can have profound implications for foreign policy, civil society and human rights.

BUILDING PUBLIC CONFIDENCE

The intelligence war on terrorism will call for broad public support for the policy, legislative and operational elements of the campaign. By way of contrast with other allies, such as the UK and US, Canada has not built up an intelligence culture of innate political cultural acceptance of the role of intelligence in national security. Knowledge resources about intelligence matters are not widely available to Canadians: until recently the intelligence services themselves preferred reticence over publicity; parliamentarians had little scope or interest in probing the intelligence domain; the mass media seldom reported on intelligence and security matters except in sensationalist terms; intelligence studies were generally neglected in academe, with singular exceptions, even where there exist programs in security and defence studies. While shocked by the attacks of September 11, Canadians remain uneasy about the national security implications of the counter-terrorism effort, especially as these are perceived to encroach on democratic values and civil liberties.

Since the campaign is unlikely to be of short duration, the longer-run political sustainability of Canada's counter-terrorism effort may be predicated on building public confidence and understanding about security and intelligence matters. Three urgent confidence-building tasks can be identified: improved transparency of the security and intelligence community, consistent with its needs for elements of secrecy; more extensive recruitment and promotion of pertinent cultural proficiencies and skills in the security and intelligence community; and greater attention to public education about intelligence and security affairs. Such initiatives as these could serve. Failure to build public confidence may result in chinks in the political armour, could bring about intelligence failures and security lapses.

Public accountability for security and intelligence affairs, in the Canadian practice, has emphasized executive oversight and review. Thus, the Security Intelligence Review Committee, the Inspector-General of CSIS, the CSE Commissioner, the Auditor-General of Canada, all exercise

oversight authority of the Government of Canada to ensure compliance with law and policy. Parliamentary oversight, however, has been relatively weak in Canada. Until now there is no committee of the House of Commons responsible for oversight of the security and intelligence community as a whole; in the Senate, a newly established Standing Committee on National Security and Defence may perhaps take on that function. Indeed, the vigorous parliamentary and public discourse that accompanied the introduction of the new anti-terrorism bills should challenge Parliament to perform a more vigorous oversight function, akin to the experiences of other countries like the US and UK. A move towards a more robust system of Parliamentary oversight could help achieve greater transparency and reassurance, whilst also facilitating broader public awareness of the role and purpose of the security and intelligence community.

As Canada's security and intelligence community mobilizes itself for the war against terrorism it will also have to upgrade its capacity to deal hitherto unfamiliar and obscure protagonists. This implies a human resource development effort on the part of the intelligence services in particular to acquire the cultural and language proficiencies, and analytical and linguistic skills for the tasks ahead. Notwithstanding certain sensitivities regarding recruitment and security clearances, the Canadian security and intelligence community has moved, like its counterparts in other Western democracies, to widen its catchment of personnel and proficiencies. Not only can this contribute to operational effectiveness, but the trend towards a more inclusive security and intelligence community may help overcome any latent distrust among segments of the broader Canadian public.

In girding up to do battle against international terrorism it is incumbent upon the governments of democratic societies to prepare their publics for a prolonged, probably arduous and possibly traumatic campaign. Al Qaeda, its co-conspirators and their protagonists and supporters in Western democracies are unlikely to remain passive before the counter-terrorism effort. They will doubtless seek to exploit any chink in counter-terrorism armour, and especially the skepticism and concerns that may emerge in public opinion in democratic societies.

In order to build and sustain public confidence in the counter-terrorism effort it will be vital for governments to reach out to civil society with greater transparency and resources to help build up a repertoire of knowledge about national security affairs. Outreach can have many arms and can touch on different needs. Thus, an accelerated declassification of historical documentation can help to demystify intelligence and foster appreciation and pride in the Canadian experience. Likewise, establishing an intelligence exhibition at the Canadian War Museum, perhaps modeled after the Secret War gallery at the Imperial War Museum in London, can do much to promote interest and awareness among Canadians. Our allies have been swifter to recognize the importance of building up knowledge bases and inspiring public confidence: thus, the British government has gone so far as to commission the preparation of an official history of MI-5, which was itself once a most secretive organizations, to mark the centenary of the Security Service in 2009.

In the field of education, the Government of Canada can build on existing instruments to promote the development of national expertise on security and intelligence affairs, among students, in the academic community and in research. National associations and professional meetings can serve as valuable fora for dialogue between practitioners and concerned others sharing an interest in security and intelligence matters. Since the counter-terrorist effort may likely involve very sensitive domestic issues, especially in dealing with sleeper cells embedded in ethno-religious communities, or highly-charged foreign policy matters, such as attacks on rogue states, the maintenance of public confidence in the bona fides of their anticipated actions will have to constitute a significant element in government responses to this unprecedented security threat.

DEMOCRACIES AT WAR WITH TERRORISM

Combating international terrorism implies a very different kind of warfare than do conventional military, or counter-insurgency or even domestic counter-terrorist campaigns. Precisely because their consuming hatred of the West and its values, their asymmetric deployment of weaponry of mass destruction, their obscure command structure and embedded cellular network, their near-global linkages and self-sacrificing ethos, Al-Qaeda and its affiliated groups present a security threat of exceptional complexity, resilience and peril to open and democratic societies in Europe, North America and Asia, as to the established authorities in the Arab and Muslim worlds. To be sure, countries like Great Britain, Israel, Spain, Turkey and Sri Lanka, among others, have had considerable experience fighting terrorism. While there may be lessons to be learned from those essentially internal encounters with terrorism, the global terrorist threat is significantly further-reaching, more stealthy and furtive, and potentially more devastating. Persistent threats and attacks causing mass carnage could well jeopardize the very foundations of democratic societies, their existential security, social tolerance and economic well-being.

This globalization of terrorism and the escalation of threats places a dual onus on the intelligence community. Offensively, the function of the intelligence community is to supply the information and assessments that enable the civil and military authorities to overcome the terrorist menace. From a defensive perspective, it is the role of intelligence to support government and law enforcement agencies in protecting persons, institutions, lawful activities and constitutional ideals of Canadians. In performing these functions the principal challenge for the security and intelligence community remains, as ever, to uphold the ethos of democratic governance whilst combating the avowed enemies of those very principles.

Professor Martin Rudner is Director of the Canadian Centre of Intelligence and Security Studies, The Norman Paterson School of International Affairs, at Carleton University in Ottawa

The select bibliography for this text can be found at http://www.acs-aec.ca/e_magazine.html