5. Democratic accountability of intelligence services

HANS BORN and IAN LEIGH*

I. Introduction[1]

While spying is said to be the second oldest profession, intelligence accountability is a recent phenomenon. Until the mid-1970s, intelligence—with any oversight it might require—was considered to be a matter for the executive in nearly all democracies, let alone in dictatorships.[2] Prior to that, parliamentarians had hardly any information on or influence over the intelligence services.

Before the 1970s, the intelligence services of many countries, such as the United Kingdom, functioned on the basis of executive decrees, and there was thus no legal need to obtain parliament's approval of the structure and special powers of the services.[3] This situation started to change in the United States in the mid-1970s when, shocked by scandals involving domestic spying on anti-Viet Nam War protesters and revelations about illegal covert operations carried out by the Central Intelligence Agency (CIA), the US Congress enacted far-reaching legislation that created a key intelligence oversight role for the Congress and other oversight mechanisms. Reforms in Australia and Canada followed and the process gained momentum in the 1980s. After the end of the cold war, the third phase of intelligence oversight began in the post-Communist states, many of which—with Western encouragement and help—

[1] This chapter draws on Born, H. and Leigh, I., *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Publishing House of the Norwegian Parliament: Oslo, 2005); and Born, H., Johnson, L. K. and Leigh, I. (eds), *Who's Watching the Spies? Establishing Intelligence Service Accountability* (Potomac Publishers: Dulles, Va., 2005). Both publications are part of a wider research project, Making Intelligence Accountable, being carried out by the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and the Human Rights Centre of the University of Durham and supported by the Norwegian Parliamentary Intelligence Oversight Committee. On the project see URL <http://www.dcaf.ch/handbook_intelligence/>.

[2] Exceptions confirm the rule: the Netherlands and Germany started their parliamentary oversight earlier, in 1953 and 1956, respectively.

[3] Concerning the UK's security and intelligence services, until 1989 the only officially published details of their work was the so-called Maxwell-Fyfe directive, named after the Home Secretary who issued it in 1952. See *Lord Denning's Report*, Command Paper 2151 (Her Majesty's Stationery Office: London, Sep. 1963).

* The authors are grateful for the constructive comments of SIPRI's researchers and editors; Thorsten Wetzling, researcher at the Graduate Institute for International Relations, Geneva; and Fairlie Jensen, Research Assistant at the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Table 5.1. A legislative framework for the control of security and intelligence services

Elements of control
Subordination of the security and intelligence services to the executive (e.g. cabinet ministers, inspectors general and high-level coordinating bodies), including safeguards against possible ministerial abuse of the services
The authority of the parliament, specifically of its special parliamentary intelligence oversight committee
Authorization and appropriation of public funds
Permanent mandates of relevant agencies and their field(s) of operation
Internal control and direction within the services
Control over politically sensitive issues, such as covert operations and international cooperation
Reporting mechanisms to the executive, the parliament and the wider public
The process of appointing and dismissing the directors of the services
Any special powers or exemptions the services enjoy
The role of independent bodies such as the financial audit office and the courts and complaint mechanisms such as ombudsmen, tribunals, review boards and data protection officers

Source: These elements derive from the Geneva Centre for the Democratic Control of Armed Forces (DCAF) project Making Intelligence Accountable. See Born, H. and Leigh, I., *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Publishing House of the Norwegian Parliament: Oslo, 2005), pp. 121–29.

reformed their intelligence services by putting them for the first time on a statutory footing, supervised by both the executive and the parliament.[4]

Why did these various states successively change their old habits of keeping the intelligence services beyond public accountability? In many states, scandals provided the main impetus for change in the governance of intelligence services. This was the case in Australia, Canada, Norway and the USA, where legislative and public investigatory committees exposed human rights abuses and pushed for strengthened intelligence oversight systems.[5] Constitutional reform (e.g. in South Africa), transition to democracy (e.g. in Argentina, South Korea and Poland) and legal challenges brought by citizens (e.g. in the Netherlands, Romania and the UK) were all reasons why governments began to impose public accountability on their intelligence services. As of 2006, democratic parliamentary oversight of intelligence services on a statutory basis has become the international norm in democratic states and has received the backing of international bodies such as the parliamentary assemblies of the Council of Europe and the Western European Union.[6]

[4] Leigh, I., 'More closely watching the spies: three decades of experiences', eds Born, Johnson and Leigh (note 1), pp. 3–4.

[5] Leigh (note 4), pp. 3–5.

[6] Parliamentary Assembly of the Council of Europe, Recommendation 1713/2005, 23 June 2005, URL <http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta05/EREC1713.htm>; and Western European Union Assembly, Resolution 113, 4 Dec. 2002, URL <http://www.assembly-weu.org/en/documents/sessions_ordinaires/pv/2002/pv09.php#P225_15553>.

In the wake of the terrorist attacks on the USA of 11 September 2001, however, a number of new or renewed concerns have been raised, regarding both the professional adequacy of the Western world's intelligence services and the risk of their role and findings being distorted by political measures.[7] Various countries have carried out public and parliamentary special investigations into claims of failings or misconduct by intelligence services related, notably, to the preparation for and conduct of the conflicts in Afghanistan and Iraq. Prominent examples include the Congress-appointed 9/11 Commission in the USA; the Hutton Inquiry in the UK; the Arar Commission in Canada; the German special parliamentary inquest; and the Dutch Parliament's request to investigate the alleged torture practices of the Dutch Military Intelligence and Security Service in Iraq.[8] These special inquiries are proof that political leaders are no longer convinced that internal investigations are sufficient and are ready to meet the demand for greater public accountability.

Based on a comparative research project on intelligence accountability, this chapter focuses on how selected states have implemented democratic oversight of their intelligence services.[9] The states analysed are all democracies whose legislatures have adopted intelligence laws that put the functioning of their intelligence services on a legal footing and provide for oversight of intelligence. The sample of states includes Argentina, Bosnia and Herzegovina, Canada, Germany, Hungary, the Netherlands, Norway, Poland, South Africa, the UK and the USA.

Two further comments on scope and definitions are in order here. First, and as implied above, the initial step towards good oversight is a legislative framework adopted by a legitimate representative institution that sets out in clear and open terms such basic points as those listed in table 5.1. This chapter

[7] See Dunay, P. and Lachowski, Z., 'Euro-Atlantic security and institutions', and Guthrie, R., Hart, J. and Kuhlau, F., 'Chemical and biological warfare developments and arms control', *SIPRI Yearbook 2006: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2006), pp. 33–62, and pp. 707–31; and Dunay, P. and Lachowski, Z., 'Euro-Atlantic security and institutions', and Guthrie, R., Hart, J. and Kuhlau, F., 'Chemical and biological warfare developments and arms control', *SIPRI Yearbook 2005: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2005), pp. 43–75, and pp. 603–28.

[8] The National Commission on Terrorist Attacks upon the United States, also know as the Kean Commission, investigated the circumstances that led to the attacks as well as national preparedness for and immediate responses to the attacks; see URL <http://www.9-11commission.gov/>. The Investigation into the Circumstances Surrounding the Death of Dr David Kelly (also known as the Hutton Inquiry) investigated the circumstances surrounding Dr Kelly's death in the context of the controversy and debate over whether the British Government dossier on Iraq's alleged possession of weapons of mass destruction was of sufficient scope and quality to justify the government declaration that Saddam Hussein posed a national security threat to the UK; see URL <http://www.the-hutton-inquiry.org.uk/>. See also the website of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar at URL <http://www.ararcommission.ca/>. The mandate of the German Parliament's Committee of Inquiry of 7 Apr. 2006 is available at URL <http://www.bundestag.de/ausschuesse/ua/1_ua/auftrag/auftrag_engl.pdf>. The Dutch public inquiry followed press revelations that the Dutch Military Intelligence and Security Service used interrogation methods against Iraqi suspects (in Iraq) that amount to torture. See Hoedeman, J. and Koelé, T., 'Kabinet gelast onderzoek ontsporingen in Irak' [Cabinet requests investigation into derailments in Iraq], *De Volkskrant*, 19 Nov. 2006.

[9] See note 1.

generally assumes the existence of such frameworks and moves on to review the aspects of implementation that are especially important for oversight.[10]

Second, and especially in modern conditions where governments and societies face multiple risks arising in different dimensions, a widening range of authorities other than the intelligence services collect, analyse and use material that fits the definition of intelligence for their own specific purposes.[11] Defence intelligence is a well-known special field (and not uncommonly, a competitor with civilian agencies), and 'commercial intelligence' has its own and rather different meaning. Additionally, police, customs, immigration, transport security and even social security authorities are all increasingly involved in intelligence-like operations. For reasons of space this wider phenomenon is not covered in this chapter, but it raises obvious questions about the adequacy, consistency and coherence of democratic norms and oversight governing these different actors and activities: an important subject for further research and debate.

The major challenges of oversight are the focus of section II. In sections III, IV and V the three main pillars of oversight are described and analysed: executive oversight, parliamentary oversight and oversight by independent bodies. In this analysis, the concept of oversight is seen as a means of ensuring the accountability of the decisions and actions of security and intelligence agencies. The conclusions are presented in section VI.

II. The challenge of oversight

The need for intelligence is a fact of life for modern governments. Few states take the view that they can dispense with a foreign intelligence service and none is sufficiently immune from terrorism or the inquisitiveness of its neighbours to forgo an internal security service. Two basic patterns exist for organizing security and intelligence. In the first there is a single agency for domestic and foreign intelligence (e.g. in Bosnia and Herzegovina, the Netherlands, Spain and Turkey). In the second there are distinct agencies for domestic security and external intelligence, with either separate or overlapping territorial competences (as in Germany, Hungary, Poland, the UK and the USA). Despite these variations in the organizational structure or governmental setting, security and intelligence pose a common set of challenges for accountability the world over.

The need for secrecy versus the need for transparency

The fundamental difficulty that intelligence oversight poses is the conundrum of how to provide democratic control of a governmental function and institu-

[10] The relevant legislation for the countries discussed here is available for reference online. See the specific references to such legislation in the following discussion of individual countries.

[11] On governments' and societies' assessment of risk see the Introduction in this volume.

tions which are essential to the survival and flourishing of the state, but which must operate to a certain extent in justifiable secrecy.

In the case of security and intelligence, and in contrast to many other areas of governmental activity, it is widely accepted that official communications and operations can only be transparent to a limited extent, otherwise the relevant operations, sources and assets will be compromised. This suggests that the prevailing pattern of oversight for other governmental activities needs to be adapted for the circumstances of security and intelligence, yet that the need for rigorous control is greater, not less, than in the case of more mundane activities such as education or welfare.

The necessary secrecy surrounding security and intelligence runs the risk of encouraging and providing cover for illegal and ethically dubious practices on the part of the agencies involved. The democratic process itself may be subverted by the infiltration of political parties, trade unions or civil society groups in the name of security and intelligence. The privacy of countless individuals may be interfered with by the collection, storage and dissemination of personal data, whether accurate or flawed. Inefficiency and corruption may go unchecked. Since September 2001, because of increasingly multilateral intelligence cooperation in combating global terrorism, the risk has grown also of sharing information with regimes that may put it to discreditable use—an issue explored further in section III. Last but not least, human rights abuses or breaches of international law committed by a given country's intelligence services abroad may both harm the country's international standing and invite damaging retaliation. Furthermore, information about clandestine operations that becomes public may harm relations with the countries in which the operations are conducted or which are targeted by them.

The temptation for politicians

In modern states the security and intelligence agencies play a vital role in the support of government in its domestic, defence and foreign policies by supplying and analysing relevant intelligence and countering specified threats. It is essential that the agencies and officials who carry out these roles are under democratic supervision by elected politicians, rather than accountable only to themselves. However, there is a real danger that politicians will be tempted to use the agencies' resources of information (about political opponents) or exceptional powers (e.g. of covert entry and bugging) to serve a domestic party political agenda. This possibility of gathering information to discredit or influence domestic political figures and movements must be guarded against. Well-calibrated accountability structures therefore attempt to insulate security and intelligence agencies from political abuse without isolating them from executive control. In general, the solutions adopted by democratic states deal with this paradox in two ways: first, by balancing rights and responsibilities between the agencies and their political masters; and second, by creating

checking mechanisms outside the executive branch (see sections IV and V on parliamentary oversight and independent bodies, respectively).

The challenges of intelligence oversight in new democracies

A great challenge is faced by countries that have recently made the transition to democracy from authoritarian regimes. In the past, the main task of internal security and intelligence services in such countries was to protect authoritarian leaders from their own people rather than to protect the state or the constitutional order. Primarily, the security and intelligence services fulfilled a repressive function. An enormous effort is required to reform the old security services into modern democratic services, and the process of turning them from a tool of repression into a modern tool of security policy requires careful monitoring by the executive and the parliament. In Europe the challenge is often exacerbated by the arrival of a new post-1989 generation of politicians with no particular knowledge of intelligence services—a problem that also applies to some politicians in older democracies. It is difficult to lead or to reform intelligence services from a position of ignorance or inexperience.

Since 1989 many former Communist states in Central and Eastern Europe have set up a double-headed constitutional arrangement for leading intelligence and security services, in which the president is responsible for some important functions (e.g. appointing a director) and the prime minister deals with day-to-day issues. Such an arrangement can perhaps be explained by a concern that no executive leader should have the monopoly on the use of intelligence services. However, intelligence services in the Czech Republic, Estonia, Latvia, Lithuania, Romania and Slovakia have misused this dual structure to play off the prime minister against the president or sometimes to escape oversight altogether.[12]

III. Executive oversight: addressing politically sensitive intelligence issues

The executive branch plays a major, if not the most important, role in controlling (tasking, steering and monitoring of) intelligence services. Three issues are addressed in this section: (*a*) the role of the executive in overseeing intelligence agencies; (*b*) the oversight of international intelligence cooperation; and (*c*) the structures to ensure that executive control does not lead to ministerial abuse of the services.

[12] Oxford Analytica, 'CEE: Security problems are not just structural', Daily Brief Services, Oxford, 24 Oct. 2006.

The role of the executive

The ultimate authority and legitimacy of intelligence agencies rests on legislative approval of their powers, operations and expenditure. However, for practical reasons and because of the sensitive nature as well as the urgency of the subject matter, effective external control of these agencies must rest with the government—the executive. There is no intrinsic conflict between effective executive control and parliamentary oversight. On the contrary, the latter depends on the former. Parliaments can only reliably call ministers to account for the actions of the intelligence agencies if the ministers have real powers of control and adequate information about the actions taken in their name. Where this is lacking, the only democratic alternative is for a parliamentary body or official to attempt to fill the vacuum. This, however, is a poor substitute because, while legislative bodies can effectively review the use of powers and expenditure *ex post facto*, they are not equipped to direct and manage these matters in real time in the same way as governmental structures are.

The cabinet ministers who are responsible for intelligence services need two types of power in order to discharge their responsibilities: a sufficient degree of control over intelligence agencies and the right to demand information from them. Ministers are entitled to expect total loyalty from the agencies in implementing the policies of the government in the country's interests. They also need to have adequate control and information to be able to account to the parliament for the agencies' use of their legal powers and their expenditure.

Effective control by the executive does not, however, imply direct managerial responsibility for security and intelligence operations. In many countries, both to prevent abuse and as a prerequisite of effective control, the respective competences of the responsible ministers and the agency directors are set out in legal provisions. In the interest of effectiveness they should be distinct but complementary. If ministers are too closely involved in day-to-day matters, it will be impossible for them to act as a source of external control and the basis of democratic oversight will be undermined. The precise dividing line between the respective responsibilities of ministers and the agency heads is difficult to draw. One useful model, however, is the 1984 Canadian Security Intelligence Service (CSIS) Act, which defines the director of the service as having 'the *control and management* of the Service', '*under the direction*' of the responsible minister.[13] The Polish intelligence legislation contains a provision that clearly distinguishes between the competencies of the prime minister (giving direction) and the heads of the agencies (drawing up plans of action and reporting to parliament and the public).[14] Particularly in societies in democratic transition, where the dividing line between civilian government and the intelligence services has previously been blurred, it may be necessary to provide detailed prohibitions to prevent future abuses. For

[13] Canada, Canadian Security Intelligence Service Act, 1984, section 6(1); the act, as amended, is available at URL <http://laws.justice.gc.ca/en/C-23> (emphasis added).

[14] Poland, Internal Security Agency and Foreign Intelligence Agency Act, 24 May 2002, URL <http://www.aw.gov.pl/eng/akty-prawne/akty-prawne.html>, article 7 (in Polish).

instance, in Bosnia and Herzegovina's 2004 legislation, the Chair of the Council of Ministers has a number of detailed policy and review functions but is expressly prevented from assuming 'in whole or in part' the rights and responsibilities of the director-general or deputy director-general of intelligence.[15]

International intelligence cooperation

Developing and maintaining international and cross-agency intelligence cooperation has become imperative in today's security environment. If the new perceived threats (i.e. militants and terrorists) operate in constantly changing cross-border structures (benefiting from creations of the information age such as mobile phones and the Internet), then the intelligence operatives and services trying to track them down must respond by operating in similarly dynamic cross-border style. Despite the manifold difficulties of intelligence sharing between states, intelligence agencies of different states cooperate in a number of ways: pooling resources, trading information, drawing up common threat assessments and, unfortunately, sometimes conspiring to circumvent domestic law.[16]

There are two concerns related to international intelligence cooperation that underline the need for strict and balanced executive control. The first is the temptation for intelligence services seeking information on pressing issues to disregard the original method used by a possibly less scrupulous overseas partner for obtaining the information. International law clearly prevents the use, for example in a terrorist prosecution or in deportation proceedings, of information obtained in another state through torture.[17] Under Article 15 of the 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment,[18] any statement made as a result of torture is inadmissible in evidence in 'any proceedings', except in proceedings against the alleged torturer. It can be argued, although international law is not so specific here, that the same considerations apply even to the mediated use of information obtained by another state's security services through torture. As the British Judge David Neuberger commented in a relevant case: 'by using torture, or even by adopting the fruits of torture, a democratic state is weakening its case against terrorists, by adopting their methods, thereby losing the moral high ground an open democratic society enjoys'.[19]

[15] Bosnia and Herzegovina, Law on the Intelligence and Security Agency, 2004, URL <http://www.legislationline.org/upload/old/35d065b27c243a9098a01793763f1b86.pdf>, articles 8–10.

[16] Wetzling, T., 'Actors, activities and dimensions: understanding European counter-terrorism intelligence liaisons', eds S. Farson et al., *Handbook of Global Security and Intelligence: National Approaches* (Greenwood Publishing Group: Westport, Conn., forthcoming).

[17] Born and Leigh (note 1), pp. 66.

[18] The Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment was opened for signature on 10 Dec. 1984 and entered into force on 26 June 1987. The text of the convention is available at URL <http://www.unhchr.ch/html/menu3/b/h_cat39.htm>.

[19] Lord Justice Neuberger (dissenting), *A. and others v. Secretary of State for the Home Department*, Court of Appeal (Civil Division), [2004] EWCA Civ. 1123, URL <http://www.bailii.org/ew/cases/EWCA/Civ/2004/1123.html>. Ultimately, the House of Lords found against the use of such material if it

A second reason for concern is that international intelligence cooperation may entail transferring information on national citizens to foreign intelligence services. Many countries have introduced legal safeguards and controls to avoid personal data on their citizens being supplied to other countries in breach of domestic law.[20] The issue goes wider than concern for the originating state's citizens. Since intelligence shared with foreign intelligence services is no longer under the control of the provider, inappropriate or careless use by the recipient may harm the intelligence activities of the supplier. More importantly, the intelligence provided to a foreign entity may be used or even be essential for supporting policies counter to the interests or objectives or against the ethical standards of the providers.[21] For these and other reasons, it is essential that international intelligence cooperation should be properly authorized by ministers and should be subject to a necessary minimum of safeguards to ensure compliance with domestic law and international legal obligations. At the least, international cooperation should be based on agreements or frameworks which have been subject to ministerial approval.

Safeguards against ministerial abuse of intelligence services

As noted above, executive control of the security sector carries potential risks which require additional safeguards. First, if there is excessive secrecy, the government in effect treats information acquired by public servants as its own property. The executive may attempt to withhold information about security accountability or procedures that are legitimate matters of public debate with the purported excuse of national security. Second, the executive may be tempted to use security agencies or their capacities to gather information in order to strengthen its position. Safeguards allowing officials to refuse unreasonable government instructions in the latter context are highly desirable.

There is a delicate balance between ensuring proper democratic control of the security sector and the distortion of intelligence findings to support a particular political option. The legislation governing security and intelligence agencies should contain clear arrangements for political direction and, in the case of internal agencies, political independence, to ensure that matters of policy are determined by politicians accountable to the public.

Various forms of safeguard may be used to prevent the misuse of agencies by the executive. In Australia, Canada and Hungary there is a requirement that

was clear that it had been obtained by torture. See *A. (FC) v. Secretary of State for the Home Department*, [2005] UKHL 71, URL <http://www.bailii.org/uk/cases/UKHL/2005/71.html>.

[20] See e.g. German Bundesverfassungsschutzgesetz [Federal Constitution protection law], Nov. 2002, URL <http://www.fas.org/irp/world/germany/docs/bverfg.htm>, article 19 (3), (unofficial English translation).

[21] See e.g. Fava, C., 'Draft report on the alleged use of European countries by the CIA for the transport and illegal detention of prisoners', 2006/2200 (INI), European Parliament, Temporary Committee on the Alleged Use of European Countries by the CIA for the Transport and Illegal Detention of Prisoners, 24 Nov. 2006, URL <http://www.europarl.europa.eu/comparl/tempcom/tdip/default_en.htm>.

ministerial instructions be put in writing.[22] Such instructions may also be required to be disclosed outside the agency. The Canadian act, for example, requires that they be given to the responsible review committee,[23] and Australian law requires them to be given to the independent Inspector-General of Intelligence and Security as soon as practicable after the instruction is issued.[24] A second type of group of safeguards aims at promoting the political neutrality and bipartisan use of the intelligence services. For example, the Australian intelligence legislation gives the director-general a duty to brief the leader of the opposition.[25] A bipartisan approach to security and intelligence is more likely to be maintained if leading opposition parliamentarians do not feel that they have been wholly excluded from the 'ring of secrecy'. The Australian example is drawn from a Westminster-style parliamentary democracy, albeit a federation. In a more complex federal presidential state there may be a range of actors who should be briefed on a 'need to know' basis. In Bosnia and Herzegovina[26] and the UK, for example, intelligence laws include clear provisions that the intelligence and security services shall not allow their impartiality to be undermined—be it by furthering the interests of certain political parties or by weakening the credibility of legitimate political movements in the country.[27] A third type of safeguard is the so-called open-door policy by which the agency head is granted the right of access to the prime minister or president in order, among other things, to express any politically related concerns. In the UK, the heads of the domestic (Security Service) and foreign (Secret Intelligence Service and Government Communications Headquarters) security agencies, although responsible to the home and foreign secretaries, respectively, have the right of direct access to the prime minister.[28] A fourth group of safeguards against ministerial abuse exists within the agency: for example, legal limits on what an agency can be asked to do; legal safeguards concerning the appointment and dismissal of the agency head; and independent mechanisms for dealing with suspected illegal activities (so-called whistleblower or grievance procedures).

[22] E.g. Hungary, Act on the National Security Services, 19 Dec. 1995, URL <http://www.dcaf.ch/info/legal/countries/Hungary/Sec_Service_Act.pdf>, section 11.

[23] See e.g. Canada (note 13), section 6(2), requiring written instruction issued by the minister to the director of the service to be given to the Security Intelligence Review Committee.

[24] Australia, Inspector-General of Intelligence and Security Act, 1986; the act, as amended, is available at URL <http://www.austlii.edu.au/au/legis/cth/consol_act/ioiasa1986436.txt>, section 32B.

[25] Australia, Intelligence Services Act, 2001, URL <http://scaleplus.law.gov.au/html/pasteact/3/3483/pdf/IntelligServ2001.pdf>, section 19.

[26] See Bosnia and Herzegovina (note 15), article 6.

[27] Bosnia and Herzegovina (note 15), article 39; and United Kingdom, Security Service Act, 27 Apr. 1989, URL <http://www.opsi.gov.uk/ACTS/acts1989/Ukpga_19890005_en_2.htm#mdiv2>, section 2.

[28] United Kingdom (note 27), section 2(4); United Kingdom, Intelligence Service Act 1994, 26 May 1994, URL <http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940013_en_2.htm>, sections 2(4), 4(4).

IV. Parliamentary oversight: inside or outside the ring of secrecy?

Oversight or scrutiny of the security sector cannot remain the preserve of the government alone without inviting potential abuse. Aside from their role in setting the legal framework, it is commonplace for parliaments to scrutinize governmental activity. In most democracies it is accepted that all areas of state activity should be open for investigation by the parliament, including the security and intelligence sector. Parliamentary involvement gives legitimacy and democratic accountability. It can help to ensure that security and intelligence organizations are serving the state as a whole and protecting the constitution, rather than narrower political or sectoral interests. However, there are corresponding risks to be avoided, including undue politicization of intelligence issues and irresponsible behaviour by parliamentarians in debate. This section elaborates on the role of the parliament in the oversight of intelligence services, including the sensitive issue of parliamentarians' access to classified information.

The role of the parliament

The international norm is for the parliament to establish a specialized body which is mandated to provide oversight of the intelligence services.[29] Without such a specialized committee, it is hard if not impossible for the parliament to exercise systematic and focused oversight of the intelligence services. Table 5.2 presents an overview of different parliamentary intelligence oversight committee systems in selected European countries.

The scope of the mandate of the parliamentary intelligence oversight committee is crucial for its success. One option is for the mandate to be comprehensive and include both policy and operations (e.g. as in Germany and the USA).[30] A parliamentary oversight body that deals with operations may have greater credibility and may be given greater powers, such as powers of subpoena. However, it will face inevitable restrictions on how it conducts its investigations and on what can be reported to the parliament or the public. It will operate in effect within a ring of secrecy and that will create a barrier between it and the remainder of the parliament. Provided that it establishes a reputation for independence and thoroughness, this need not affect its legitimacy. However, the parliament and the public will have to take it on trust to a certain degree that proper oversight of operational matters is taking place without supporting evidence being available. Another danger is that such an

[29] France is one of the rare liberal democracies where the parliament does not have a specialized committee dedicated to the oversight of intelligence services.

[30] US Senate Select Committee on Intelligence, 'Rules of the US Senate Select Committee on Intelligence', section 13; and Act Governing the Parliamentary Control of Intelligence Activities by the German Federation, Parliamentary Control Panel Act (PKGrG), Apr. 1978, section 2, 2a. See the discussion in Born and Leigh (note 1), pp. 77–102.

Table 5.2. Types of parliamentary intelligence oversight committees in democracies

Type of intelligence oversight committee	Examples of use
No parliamentary intelligence oversight committee	France
No parliamentary intelligence oversight committee but the parliament has at its disposal an independent committee of experts to ensure oversight of the intelligence services; members are appointed by the parliament; committee reports to the parliament	Norway
Parliamentary intelligence oversight committee and the parliament also has at its disposal an independent committee of experts, appointed by the parliament, which reports to the parliament	Belgium
Parliamentary intelligence oversight committee in combination with an independent committee of experts, appointed by the government and reporting to the government	Netherlands
Parliamentary intelligence oversight committee with expert staff	Germany, USA
Not one but several parliamentary intelligence oversight committees for domestic, foreign and military intelligence	Romania
Ad hoc investigative committees to investigate the role of government and intelligence services	German Parliament, Committee of Inquiry

oversight body gets too close to the agencies it is responsible for overseeing. For example, although a legal requirement that the oversight body be notified in advance of certain actions by the agency may appear to strengthen control, it could also protect that body from later criticism of these operations. This is a danger, for example, in the USA, where congressional intelligence oversight committees must be notified about special intelligence operations in advance.[31] The alternative approach is to limit the mandate of the parliamentary oversight committee to matters of policy and finance only (as in the UK) or human rights and the rule of law (as in Norway).[32] These aspects can be more readily examined in the public arena with fewer restrictions on disclosure—although the publication of precise budgetary details may be prejudicial to national security. The difficulty of the latter approach, however, is that it detracts from one of the key tasks of parliamentary scrutiny: to ensure that government policy in a given field is carried out effectively and within the boundaries of the law. Without access to some operational detail, an oversight body can have or give no assurance about the efficiency or the legality of the intelligence services.

[31] Such activities are regulated in the 1974 Hughes–Ryan Act; the 1980 Oversight Act, and the 1991 Intelligence Authorization Act. On congressional involvement in authorizing covert operations see Johnson, L. K., 'Governing in the absence of angels: on the practice of intelligence accountability in the United States', eds Born, Johnson and Leigh (note 1), pp. 64–66.

[32] Norway, Act Relating to the Monitoring of Intelligence, Surveillance and Security Services, Act no. 7, 3 Feb, 1995, URL <http://www.dcaf.ch/info/legal/countries/Norway/Law/IntelligenceAct.pdf>, section 2.

Access to secret information

As mentioned above, effective scrutiny of security and intelligence is painstaking and unglamorous work for politicians, conducted almost entirely behind the scenes. Sensitive parliamentary investigations require in effect a parallel secure environment in the parliament for witnesses and papers. The preservation of necessary secrecy may create a barrier between the few parliamentarians involved and the remainder, causing those within the ring of secrecy to be envied or distrusted by colleagues. It is therefore essential that a cross section of parliamentarians who can command widespread trust and public credibility are involved—for example, senior politicians and leaders of parliamentary factions. The parliament, and particularly the oversight body, must have sufficient power to obtain information and documents from the government and intelligence services. The precise extent to which a parliamentary oversight body requires access to security and intelligence information and the type of information concerned depends on its mandate. An oversight body that has functions which include reviewing operations and effectiveness will require access to more specific information than one with a remit solely covering policy. Clearly, however, an oversight body should have unlimited access to the information necessary for discharging its duties.

Oversight is not only a matter of having access to information, but also of being informed about matters which are important but on which information is not available to the parliament as a whole. The US Congress has acknowledged this problem and has passed laws requiring that the executive keeps the congressional intelligence oversight committee completely and currently informed of the intelligence activities of all agencies, including covert actions.[33] Inevitably, for reasons of national security, there is a limit to what this committee can report to the rest of the Congress or the public. Different approaches are followed by various countries. In Australia, for example, the committee is not allowed to disclose in a report to the parliament the identity of, or more general information about, intelligence employees and other operationally sensitive information.[34] In the UK, the Intelligence and Security Committee (ISC)—a committee of parliamentarians from both houses—is required by law to produce at minimum one annual report to the parliament. The report, however, is first submitted to the prime minister who can unilaterally delete text from it, although in all cases to date changes have been agreed by consultation. The ISC's annual reports have contained many such deleted passages (marked by asterisks) in recent years. Additionally, the prime minister decides about the timing of the publication of the ISC's report, which may permit him or her to dampen its impact by delaying release until public interest in the relevant events has waned, or to synchronize the date of publication with the government's prepared response. Members of the ISC have

[33] Johnson (note 31), pp. 64–66.
[34] Australia (note 25), schedule 1, part 1, clause 7.1.

complained about unnecessary delay in releasing their findings.[35] The danger of the British system is that the executive could use such procedural powers to interfere with and limit the parliamentary accountability of the intelligence services.

A last, but not unimportant, issue is whether parliamentarians are capable of keeping secrets. Research into the functioning of parliamentary intelligence oversight committees has indicated that parliaments rarely leak classified information.[36] This is not strange because parliamentarians are aware that, if they leak, they will lose the trust of the intelligence services and the government as well as the public. Furthermore, unless parliamentarians have immunity in such cases, leaking officially classified information is illegal. In many countries members of parliamentary intelligence oversight committees are screened and vetted before they are allowed to take a seat on the committee.[37] Vetting of parliamentarians is, however, a delicate subject. It can be argued that legislators should be immune from vetting (as they are in Argentina, the UK and the USA) because it creates inequality between parliamentarians and because the legislative mandate of parliamentarians should automatically imply access to classified information. Again, if parliamentarians are vetted (as for example in Poland and South Africa), the problem arises of their being dependent for security clearance on the same service that they are supposed to oversee. To avoid a conflict of interests and responsibilities in countries with such a procedure, the ultimate decision about appointing a parliamentarian to the intelligence committee is reserved for the leadership of the parliament alone. The intelligence services therefore play an advisory, not a deciding, role in the security clearance of parliamentarians for oversight work.[38]

The possibility of having access to information does not necessarily mean that members of the parliament will make use of that possibility. Parliamentarians may fear that their independence and freedom of speech will be compromised if they have knowledge of classified matters. In the Netherlands, for example, Socialist Party parliamentarians refused to become members of the parliamentary intelligence oversight committee for this reason. In the USA only 12 members of the House of Representatives made use of the right to read the 2006 classified intelligence bill (which passed in a vote of 327 to 96 in April 2006), and thus the great majority of members voted in favour of the bill without knowing its contents. The reason why so many members chose not to read the bill is that they would not be allowed to disclose any classified

[35] Leigh, I. 'Accountability of security and intelligence in the United Kingdom', eds Born, Johnson and Leigh (note 1), pp. 88–89.

[36] Born, H. and Johnson, L. K., 'Balancing operational efficiency and democratic legitimacy', eds Born, Johnson and Leigh (note 1). pp. 225–39.

[37] Vetting is a process by which an individual's personal background and political affiliation is examined to assesses his or her suitability for a position that may involve national security concerns. See Born and Leigh (note 1), p. 88.

[38] Born, H. and Johnson, L. K., 'Balancing operational efficiency and democratic legitimacy', eds Born, Johnson and Leigh (note 1). pp. 225–39.

information drawn from it during plenary debates in the Congress, even if the media had already reported on the matters concerned.[39]

V. Non-political oversight: the role of courts and independent bodies

The previous sections described the importance of the executive and of the parliament in relation to the accountability of intelligence and security agencies. The third branch of the state—the judiciary—also has a role to play, both as the ultimate guardian of the constitution and the law and through various review functions.

The role of the judiciary

It would be misleading to describe the judiciary as routinely involved in oversight. Intelligence-related cases that reach court are sporadic, and judges generally do not see it as their task to supervise the exercise of governmental functions but rather to review their constitutionality, legality or compliance with human rights standards as necessary. Nevertheless, because of the centrality of the rule of law as a source of control on arbitrary power in modern democracies, judicial practice is important. Judges are the final arbiters of the statutory powers that security and intelligence agencies possess.

There are both strengths and dangers in judicial scrutiny of intelligence matters. On the positive side, in most liberal states judges are perceived to be independent of the government; their presumably detached view lends credibility to the system of oversight in the eyes of the public. Traditionally, the courts have been perceived as guardians of individual rights and, arguably, judges are well suited to oversight tasks that involve the interests of individuals—for example the scrutiny of surveillance. There are, however, also problems that in part arise from the necessary tensions and limitations in judicial review of any governmental function, and in part are specific to the field of security.[40] Court procedures necessitate sensitive data being disclosed beyond the controlled environment of the security sector itself. Even if legal proceedings take place in camera, the judge, court staff and lawyers may be required to read or handle the information. This raises the difficult question of security vetting. In some countries judges are vetted or access to the handling of this category of cases is restricted to a small group. This may, however, raise questions about pre-vetted judges' impartiality in such proceedings, since the effect of the vetting requirement is to make them acceptable to one party in the case. In other countries vetting would be constitutionally unacceptable and the

[39] Not all of the 2006 intelligence bill is classified, but it contains classified provisions and sections. 'Classified intelligence bills often unread: secret process can discourage House debate', *Boston Globe*, 6 Aug. 2006, p. A1.

[40] Lustgarten, L. and Leigh, I., *In From the Cold: National Security and Parliamentary Democracy*, (Oxford University Press: Oxford, 1994), pp. 320–59.

seniority and reputation of the judges involved is taken as sufficient guarantee that they can be trusted with secret information.

The more general danger is that over intrusive control by the judges risks involving them in the tasks of the executive and blurs the separation of powers between these two branches of the state. The politicization of the judiciary may also result from the use of judges to conduct inquiries with a security dimension. Their wider credibility and legitimacy may be at risk of being undermined. Judicial scrutiny should be sparing and suitably modest in areas of government policy where judges have no special competence, for example, in assessing whether intelligence justified a decision to take a particular military action or whether it established an imminent threat to the state. Legal control by the courts proper can only operate effectively within the limited range of issues where a person's rights are affected by security decisions. Much security work, however, eludes this criterion since it does not affect a person's recognized legal rights (e.g. gathering information on individuals from public sources, or surveillance in public places). Even if individuals are affected, in many instances they are unlikely to bring legal challenges because the role of the agencies concerned will not be apparent to them (e.g. the targets of surveillance in some countries will never learn that they have been targeted). Challenges by an affected individual are most likely where there are legal procedures against that individual, such as prosecution or deportation, based on intelligence material. Much other security work is not directed towards immediate legal procedures in this way (e.g. long-term intelligence gathering) and is therefore likely to remain unchecked by legal challenge. State interests may be protected also by specific bars on the use of intelligence material in evidence for reasons of public policy. Examples include the common law concepts of public interest immunity or executive privilege and the current statutory bar on admissibility in court of evidence obtained from telephone tapping under the UK's 2000 Regulation of Investigatory Powers Act.[41] This act not only deprives prosecutors of potentially valuable evidence but also immunizes warrants for phone tapping from judicial challenge.

In several countries there are judicial procedures that have been specially adapted to a security context: thus, in Canada designated Federal Court judges hear surveillance applications from the CSIS and deal with immigration and freedom of information cases with a security dimension.[42]

The US 1978 Foreign Intelligence Surveillance Act (FISA) has operated for more than two decades.[43] It created a special court of judges for overseeing surveillance warrants issued by federal police agencies against suspected foreign intelligence agents inside the USA. According to FISA, the electronic surveillance of telephone calls between the USA and foreign countries needs the authorization of the FISA special court. In December 2005 *The New York*

[41] United Kingdom, Regulation of Investigatory Powers Act, 2000, URL <http://www.opsi.gov.uk/Acts/acts2000/20000023.htm>.

[42] Leigh, I., 'Secret proceedings in Canada', *Osgoode Hall Law Journal*, vol. 34 (1996) pp. 113–73.

[43] United States, Foreign Intelligence Surveillance Act (FISA), 1978, URL <http://caselaw.lp.findlaw.com/casecode/uscodes/50/chapters/36/toc.html>.

Times revealed that President George W. Bush had secretly authorized in 2002 the National Security Agency (NSA) 'terrorist surveillance program' to monitor calls between the USA and foreign countries without court authorization.[44] President Bush claimed that the NSA programme was both legal and necessary in the 'global war against terrorism'.[45] The American Civil Liberties Union (ACLU), however, contested the legality of the NSA programme in court and a federal judge ruled in August 2006 that it was illegal.[46] The Democratic Party gained control of the US Congress in the November 2006 elections, and the NSA Oversight Act bill was introduced in the House of Representatives in January 2007.[47] If passed, it would reaffirm that the FISA court authorization is the sole legal basis for wiretaps.

Similarly, in the UK designated judicial commissioners deal with some forms of authorization of surveillance—although not in court—under the 2000 Regulation of Investigatory Powers Act; other judicial commissioners review the system and check on the warrants and authorizations granted to the security and intelligence services by ministers. Even in cases such as this, where judges are used in order to safeguard the rights of individuals, there is the danger that familiarity and acclimatization to security material will gradually undermine their qualities of independence and external perspective. If judges become case hardened through overexposure to security techniques, information and assessments as revealed in intelligence-based warrant applications, then they may become less effective in practice at protecting individuals' rights. Evidence from countries that require prior judicial approval of surveillance warrants, such as Canada and the USA, does not suggest high rates of refusal. This casts into doubt whether such judges are really bringing an independent perspective to the process: ultimately, there may be little difference in outcome between this procedure and a system of approval within the agency itself or by a government minister.

One solution to the difficulties of handling intelligence as source material in court proceedings is the use of special, security-cleared legal representatives in deportation, employment and (increasingly) criminal cases.[48] Initially adapted from Canadian procedure, this system aims to balance so-called open justice with the state's security interests.[49] It allows a vetted lawyer to test the

[44] Risen, J. and Lichtblau, E., 'Bush lets U.S. spy on callers without courts', *New York Times*, 16 Dec. 2005.

[45] Lichtblau, E., 'Bush defends spy program and denies misleading public', *New York Times*, 2 Jan. 2006.

[46] *ACLU v. NSA*, Detroit District Court, 17 Aug. 2006; and Cable News Network, 'NSA eavesdropping program ruled unconstitutional', 17 Aug. 2006, URL <http://www.cnn.com/2006/POLITICS/08/17/domesticspying.lawsuit/>.

[47] Broache, A., 'Congress off to slow start with tech', *New York Times*, 9 Jan. 2007; and US House of Representatives, NSA Oversight Act, H.R. 11, 4 Jan. 2007, URL <http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.11:>.

[48] British Treasury Solicitor, *Special Advocates: a Guide to the Role of Special Advocates* (Stationery Office: London, 2005).

[49] In the UK the Special Immigration Appeals Commission (SIAC) was established by the Special Immigration Appeals Commission Act 1997, following the ruling of the European Court of Human Rights in the Chahal case. *Chahal v. the United Kingdom*, 22414/93 [1996] ECHR 54, 15 Nov. 1996,

strength of the government's case and to challenge the evidence even where the complainant and his or her lawyer are excluded from parts of the legal process on security grounds. The European Court of Human Rights has advocated such procedural innovations as a means of satisfying Article 6 of the European Convention on Human Rights (the right to a fair and public trial),[50] even in security cases.[51] The UK's use of such special advocates has been criticized, however, by some of those who have undertaken the role and by a parliamentary select committee.[52]

Complaint systems

More generally, as explained above, the courts are inherently flawed as a means of accountability for or redress against security and intelligence agencies There is a clear need for alternative avenues of redress for individuals who claim to have been adversely affected by the exceptional powers often wielded by security and intelligence agencies. A proper complaint system can also bolster accountability by highlighting administrative failings and lessons to be learned, leading to improved performance. At the same time, the system should not help those who are legitimately targeted by a security or intelligence agency to find out about the agency's work. A complaint system should be independent, robust and fair to the complainant on the one hand, but sensitive to security needs on the other. For European states, the European Convention on Human Rights also has a bearing because of the rights it establishes to a fair trial by an independent and impartial tribunal, to respect for private life and to the availability of an effective remedy.[53]

An oversight system may handle complaints in a variety of ways. An independent official, such as an ombudsman, may have the power to investigate and report on a complaint against an agency—as in the Netherlands.[54] Other countries give jurisdiction to deal with complaints against the services as part

URL <http://www.worldlii.org/eu/cases/ECHR/1996/54.html>. The SIAC is able to receive intelligence information in closed hearings and without the presence of the appellant and through use of Special Advocates. Its initial jurisdiction was in cases of deportation on grounds of national security. However, the 2001 Anti-Terrorism Crime and Security Act extended the jurisdiction to include review of detention following a ministerial certificate that a non-national was a security threat; the latter provisions were, however, superseded with the introduction of 'control orders' under the 2005 Prevention of Terrorism Act, URL <http://www.opsi.gov.uk/ACTS/acts2005/20050002.htm>.

[50] On the right to a fair trial see *Edward and Lewis v. the United Kingdom*, [2003] 15 BHRC 189, 22 July 2003, URL <http://worldlii.org/eu/cases/ECHR/2003/381.html>. See also the European Convention on Human Rights, Rome, 4 Nov.1950, URL <http://www.hri.org/docs/ECHR50.html>.

[51] *Chahal v. the United Kingdom* (note 49).

[52] British House of Commons, Constitutional Affairs Select Committee, Seventh Report of Session 2004–5, the operation of the Special Immigration Appeals Commission (SIAC) and the use of Special Advocates, HC 323-I, 3 Apr. 2005, URL <http://www.publications.parliament.uk/pa/cm200405/cmselect/cmconst/323/323i.pdf>.

[53] Cameron, I., *National Security and the European Convention on Human Rights* (Iustus Forlag: Uppsala, 2000); and Cameron, I., 'Beyond the nation state: the influence of the European Court of Human Rights on intelligence accountability', eds Born, Johnson, and Leigh (note 1), pp. 34–53.

[54] Netherlands, Act of 7 February 2002, providing for rules relating to the intelligence and security services and amendment of several acts (Intelligence and Security Services Act 2002), URL <http://www.aivd.nl/contents/pages/4704/IntelligenceandSecurityServicesAct2002.pdf >, article 83.

of an independent inspector general of security and intelligence's general oversight role. New Zealand's Office of the Inspector-General of Intelligence and Security (established in 1996) and South Africa's Office of the Inspector-General of Intelligence are examples of this approach (see below for more on inspectors general).[55] Commissioners appointed under freedom of information or data protection legislation may also be able to investigate complaints in these fields against the agencies. These various ombudsman-type systems each stress the importance of an investigation by an independent official on behalf of the complainant. Their primary focus may be administrative failure rather than a legal error as such, and they give less emphasis to the complainant's own participation in the process and to transparency. The conclusion is usually a report, rather than a judgement or formal remedies, and (if the complaint is upheld) a recommendation for making amends and preventing recurrence of the mistake.

A less common approach is to deal with the complaints and grievances of citizens through a parliamentary intelligence oversight committee, as in Germany and Norway.[56] Such a procedure may be a good way to gain insight into potential executive shortcomings—of policy, legality and efficiency. The individual complainant may, however, feel that the complaint process is insufficiently independent—especially if the oversight body is too closely identified with the agencies it oversees or operates within the ring of secrecy. The disadvantages of having a single body handle complaints and oversight can be alleviated by maintaining distinct legal procedures for these different roles. A better option, however, is to give the two functions to different bodies, while ensuring that the oversight body can be alerted to the broader implications of specific complaints. Members of the services, as well as the public, are permitted in some countries to bring service-related issues to the attention of an ombudsman or parliamentary oversight body. In South Africa, for example, members of the service may complain to the Inspector-General, and in Germany officials may raise issues with the Parliamentary Control Panel.[57]

Complaints may also be handled by a specialist tribunal, established to deal with complaints either against a particular agency or over the use of specific powers. The UK has examples of both—the Intelligence Services Commissioner and the Commissioner for the Interception of Communications. Alternatively, a specialist oversight body may handle complaints through a tribunal-type procedure: this is one of the roles given to the Security Intelligence Review Committee (SIRC) in Canada. Tribunals have advantages over regular courts in handling security- and intelligence-related complaints: they can develop a distinct expertise tailored specifically to sensitive information.

[55] The South African office was created pursuant to section 210b of the South African Constitution. Constitution of the Republic of South Africa 1996, 8 May 1996 (amended 11 Oct. 1996), URL <http://www.polity.org.za/html/govdocs/constitution/saconst.html?rebookmark=1>.

[56] Sejersted, F., 'Intelligence and accountability in a state without enemies: the case of Norway', eds Born, Johnson, and Leigh (note 1), pp. 119–41.

[57] German Bundestag, Secretariat of the Parliamentary Control Commission, *Parliamentary Control of the Intelligence Services in Germany* (Bundespresseamt: Berlin, 2001), pp. 19–20.

Such processes are unlikely to involve a full public legal hearing. Complainants nevertheless face major hurdles: even if granted a hearing, they are likely to have severe practical difficulties in proving a case, in obtaining access to relevant evidence or in challenging the agency's version of events. To combat some of these problems, special security-cleared counsel have been introduced in Canada and in the UK to assist the tribunal reach a more objective assessment of the evidence and the arguments, even if full details cannot be disclosed to the complainant.

Inspectors general and auditing

A number of countries have created independent offices such as inspectors general, judicial commissioners or auditors to check on the activities of the security sector, with statutory powers of access to information and staff.[58] These offices provide impartial verification and assurance for the government that secret agencies are acting in accord with its policies, effectively and with propriety. They may also give redress for complaints. The concept of the inspector general derives from the US intelligence community, which now has a dozen or so officers of this kind, independent of the agencies they oversee. Some are statutory officials (e.g. the inspectors general for the CIA and the Department of Defense); others are derived from administrative arrangements established by the relevant minister (e.g. with regard to the Defense Intelligence Agency and the National Reconnaissance Office); and some report to the Congress as well as to the executive branch. A number of these inspectors general examine agency efficiency and the avoidance of waste and perform audit functions, in addition to looking at legality and policy compliance.

Usually inspectors general function within the ring of secrecy: their primary function is to strengthen accountability to the executive, rather than providing public assurance about accountability in Canada. The Inspector-General of the CSIS is an example: he or she has full access to information in the hands of the service in order to discharge this role.[59] Similarly, under legislation in Bosnia and Herzegovina the Inspector General exercises 'an internal control function' and may review the agency's activities; investigate complaints; initiate inspections, audits and investigations; and issue recommendations.[60] The Inspector General has a duty to report at least every six months to the SIRC and to keep the relevant ministers informed of developments on a regular and timely basis. The Inspector General's powers include questioning agency employees and obtaining access to agency premises and data. In South Africa, in contrast, the Inspector-General's role is to report to the parliament. In effect the office breaches the ring of secrecy and provides public assurance, in its report to the parliament, that an independent person with access to the

[58] United Kingdom, Cabinet Office, Intelligence and Security Committee Annual Report 2001–2002, URL <http://www.cabinetoffice.gov.uk/publications/reports/intelligence/Intelligence.pdf>, appendix 3.

[59] Canada (note 13), c. 21, sections 33.2 and 33.3.

[60] Bosnia Herzegovina (note 15), article 32.

relevant material has examined the activities of the security or intelligence agency. Not surprisingly, the Inspector-General is not allowed to publish much of the material on which an assessment of the agency's work is made, although it may be shared with other oversight bodies. Other types of inspectors general who report to the executive may also maintain an informal working relationship with parliamentary bodies; this is the case in Australia, and a number of the US inspectors general report periodically to the Congress.

Regardless of whether an inspector general reports to the legislature, the executive or the courts, careful legal delineation of the office's jurisdiction, independence and powers are vital. Independent officials may be asked to review an agency's performance against one or more of several standards: efficiency, compliance with government policies or targets, propriety or legality. In every case, in order to make a reliable assessment, the office will need unrestricted access to files and personnel. An independent official is unlikely in practice to be able to examine more than a fraction of the work of an agency. Consequently, some inspectors general operate by 'sampling' the work and files of the agencies overseen, in the hope that this will produce a ripple effect inducing the agency to establish more widespread procedures. Some also have jurisdiction to deal with individual complaints (as in Australia[61]).

The auditing of financial propriety is another independent function.[62] Both the executive and the legislature have a legitimate interest in ensuring that budgets voted for intelligence are spent lawfully and effectively. However, as with the handling of complaints, it requires some ingenuity to devise systems for protecting secrecy while ensuring that auditors have the wide access to classified information necessary to let them certify whether the services have used government funds within the law. Restrictions designed to protect the identities of certain sources of information and the details of particularly sensitive operations may be imposed on the access granted to an auditor general. What distinguishes the auditing of security and intelligence services from regular audits of other public bodies, however, is the nature of the reporting mechanisms. In order to protect the continuity of operations and the methods and sources of the services, special reporting mechanisms are in place in many countries. For example, in the UK only the chairmen of the parliament's Public Accounts Committee and the Intelligence and Security Committee are fully briefed about the outcome of the financial audit. These briefings may include reports on the legality and efficiency of expenditure, on possible irregularities and on whether the services have operated within or have exceeded the budget. In many countries, the public annual reports of the security and intelligence service (e.g. in the Netherlands) or of the parliamentary oversight body (e.g. in the UK) include statements about the outcome of the financial audits.

[61] Australia (note 24), sections 10–12.
[62] Born and Leigh (note 1), pp. 113–19.

VI. Conclusions

Democratic oversight of the intelligence services, including oversight by executive, parliamentary and independent bodies, has become even more essential against the background of the post-September 2001 fight against terrorism for at least four reasons. First, many services have been granted increased personnel numbers and higher budgets, creating a need for parliamentary oversight in order to ensure that taxpayers' money is effectively spent. Second, in various countries the special powers of intelligence services have significantly increased, which in turn increases the need for civil liberty supervision, especially by judges but also through other independent complaint mechanisms. [63] Third, higher levels of international cooperation have increased the need for effective executive control, as elaborated in this chapter. Finally, although intelligence services were always politicized to a certain extent (as shown, for example, by the Watergate scandal of the early 1970s and the missile gap discussion in the 1960s in the USA) the war in Iraq and the fight against terrorism have strengthened the apparent trend towards politicization of intelligence, creating an urgent need to insulate the services from political manipulation.

It should be underlined that democratic intelligence oversight systems have come into operation only comparatively recently (i.e. mostly since the mid-1970s and in many states only since the 1990s). This development represents a move away from a guardian state, in which important issues are left to the discretion of professionals, towards a democratic state in which important issues are subjected to normal democratic decision-making procedures. On the one hand, this can be regarded as a positive development in any democratic polity because it leads to a better system of checks and balances covering the intelligence services among other things. On the other hand, the submission of intelligence services to public accountability means that their role and work become increasingly part of public debate. The danger exists that political actors in these debates will use the control of the services to promote their party interests. In other words, democratic accountability of intelligence services is designed to limit the risk of politicization but also carries a danger of heightening that risk. These and other challenges can be addressed, for example, through more substantial oversight of international cooperation and increased access to classified information by elected office holders. It remains to be seen how the fledgling intelligence oversight systems reviewed in this chapter will cope with the full challenge of overseeing the secret intelligence community in the years to come.

[63] See e.g. the 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act). US, USA Patriot Act, H.R. 3162, 24 Oct. 2001, available at URL <http://www.epic.org/privacy/terrorism/hr3162.html>. On the act see Public Broadcasting Service (PBS), 'Background report: the US Patriot Act', Online Newshour PBS, 27 Mar. 2006, URL <http://www.pbs.org/newshour/indepth_coverage/terrorism/homeland/patriotact.html>.