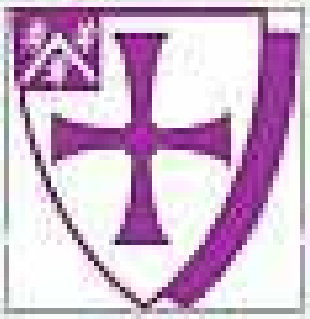
Geneva Centre for the Democratic Control of Armed Forces



Human Rights Centre, Department of Law, University of Durham

Norwegian Parliamentary Intelligence Oversight Committee

Making Intelligence Accountable:

Legal Standards and Best Practice for Oversight of Intelligence Agencies

Hans Born and Ian Leigh

Making Intelligence Accountable:

Legal Standards and Best Practice for Oversight of Intelligence Agencies

Hans Born and Ian Leigh

Geneva Centre for the Democratic Control of Armed Forces

Human Rights Centre, Department of Law, University of Durham (UK)

Norwegian Parliamentary Oversight Committee

Authors
Hans Born and Ian Leigh.

Editorial Assistants
Thorsten Wetzling and Ingrid Thorburn.

Advisory Board
Ian Cameron, Alistair Corbett, Alain Faupin, Hakon Huus-Hansen, Kalman Kocsis, Fredrik Sejersted, Fred Schreier.

Consultees
Andrew Butler, Marina Caparini, Richard B. Doyle, Willem F. van Eekelen, Peter Gill, George Lotz, Barry Wickersham.

Language Editor
Oliver Wates.

ISBN
92-9222-017-9

Publisher
Publishing House of the Parliament of Norway, Oslo.

Original version: English, Oslo, 2005.

Preface

Establishing a system of intelligence service accountability that is both democratic and efficient is one of the most daunting challenges faced by modern-day states. This arduous task is indispensable, however, as political guidance and direction to the reform of intelligence services contributes to the avoidance of abuses as well as to the enhancement of efficiency for all participating branches of government.

Little systematic international comparison of democratic accountability over intelligence services has been carried out; as a result, no set of international standards for democratic intelligence accountability has evolved. The Geneva Centre for the Democratic Control of Armed Forces, the Norwegian Parliamentary Intelligence Oversight Committee and the Human Rights Centre of the University of Durham have teamed up to produce this publication which seeks to fill this gap by cataloguing and evaluating the legal standards that currently exist regarding democratic accountability of intelligence services. In doing so, this report also identifies and recommends best practice applicable to both transition countries and well-established democracies.

These standards and examples of best practice do not make the assumption that there is a single model of democratic oversight which works for all countries. Rather, the system of democratic oversight of intelligence services depends on a country's history, constitutional and legal system as well as its democratic tradition and political culture.

The rules and practices that are accepted and effective in one place may be less relevant in another. Given these different realities, some of the suggestions within the handbook will inevitably appear unsuitable for some countries. This said, from a democratic governance point of view, the oversight of the intelligence services is a shared responsibility of the executive, the legislature and the judiciary. A sound system of checks and balances is necessary, in which the executive does not have the exclusive privilege of overseeing the intelligence services. Thus, the intelligence agencies themselves, national parliaments, as well as external review bodies all have a role to play in this endeavour.

It is hoped that this publication will enhance public awareness of this complex and important field of governance and that it will contribute to ensuring that security policy and practices genuinely reflect the aspirations of the people they are meant to serve.

Ambassador Leif Mevik
Chairman, Norwegian Parliamentary
Intelligence Oversight Committee

Ambassador Dr. Theodor Winkler
Director, Geneva Centre for the
Democratic Control of Armed Forces

Contents

Preface		3
Contents		5
List of Boxes		7
List of Acronyms		10
Section I	***Introduction***	
Chapter 1	***Defining Democratic Oversight of Security and Intelligence Services***	13
Chapter 2	***The Need for Oversight of the Security and Intelligence Services***	16
Chapter 3	***In Search of Legal Standards and Best Practice of Oversight: Objectives, Scope and Methodology***	21
Section II	***The Agency***	
Chapter 4	***Defining the Mandate***	29
Chapter 5	***Appointing the Director***	34
Chapter 6	***Authorising the Use of Special Powers***	37
Chapter 7	***Information and Files***	43
Chapter 8	***Internal Direction and Control of the Agency***	46
Section III	***The Role of the Executive***	
Chapter 9	***The Case for Executive Control***	55
Chapter 10	***Ministerial Knowledge and the Control of Intelligence***	57
Chapter 11	***Control over Covert Action***	60
Chapter 12	***International Cooperation***	64
Chapter 13	***Safeguards against Ministerial Abuse***	68
Section IV	***The Role of Parliament***	
Chapter 14	***The Case for Parliamentary Oversight***	77

Chapter 15	*The Mandate of Parliamentary Oversight Bodies*	80
Chapter 16	*The Composition of a Parliamentary Oversight Body*	85
Chapter 17	*Vetting and Clearance of the Oversight Body*	88
Chapter 18	*Parliamentary Powers to Obtain Information and Documents*	91
Chapter 19	*Reporting to Parliament*	94
Chapter 20	*Budget Control*	96
Section V	*The Role of External Review Bodies*	
Chapter 21	*Resolving Citizens' Grievances*	105
Chapter 22	*Oversight of Agencies within the Administration by Independent Authorities*	110
Chapter 23	*Independent Audit Offices*	113
Overview of Best Practice		121
Geneva Centre for the Democratic Control of Armed Forces		131
Human Rights Centre, Department of Law, University of Durham		132
Norwegian Parliamentary Intelligence Oversight Committee		133
Contributors		135
Glossary		137

List of Boxes

Box No. 1:	Norms and Standards for Democratic Oversight of Security and Intelligence Services as adopted by (selected) international organisations	14
Box No. 2:	Oversight Institutions and Actors	15
Box No. 3:	Non-Derogable Human Rights	18
Box No. 4:	Necessity of Legislating for the Intelligence Services due to the ECHR (UK)	19
Box No. 5:	Quality of Law Test	20
Box No. 6:	The European Court of Human Rights and 'National Security'	30
Box No. 7:	A Legislative Definition of National Security (Bosnia and Herzegovina)	31
Box No. 8:	Safeguards to Prevent the Use of Intelligence Agencies by Government Officials against their Domestic Political Opponents (Argentina)	32
Box No. 9:	Involvement of the Parliament in Appointing the Director (Australia)	34
Box No. 10:	Involvement of the Executive in Appointing the Director (Hungary)	35
Box No. 11:	Grounds for Dismissal of the Agency Head (Poland)	35
Box No. 12:	Special Powers of Internal Security and Intelligence Services	37
Box No. 13:	Selected 2002 Guidelines of the Committee of Ministers of the Council of Europe on Human Rights and the Fight Against Terrorism	39
Box No. 14:	Cases of the European Court of Human Rights on the Right to Privacy	41
Box No. 15:	Right to inspection of information (The Netherlands)	44
Box No. 16:	Reporting on Illegal Action Provisions in the Bosnian Law on the Security and Intelligence Agencies	46
Box No. 17:	Disclosure Protection Rules (Canada)	47
Box No. 18:	South African Code of Conduct for Intelligence Employees	48
Box No. 19:	Bosnia and Herzegovina's Law on the Intelligence and Security Agency	49
Box No. 20:	The Delineation of Competences between the Minister and the Director of Service (Poland)	56
Box No. 21:	Rights of the Minister – Responsibilities of the Agency	58
Box No. 22:	Consultation of the Director with the (Deputy) Minister	58
Box No. 23:	Covert Action Defined (US)	60
Box No. 24:	Authorisation of Covert Action Abroad (UK)	61
Box No. 25:	Torture	62
Box No. 26:	Legalising Ministerial Control Over Covert Action	63

(Australia)
Box No. 27: Various Practices of Intelligence Cooperation: Bilateral Sharing 64
Box No. 28: Multilateral Sharing of Intelligence: A Renewed EU–US Commitment 65
Box No. 29: Giving Information on National Citizens to Foreign Security Services: An Example from German Intelligence Legislation 67
Box No. 30: The Duty of the Bosnian Intelligence Service to Cooperate with the International Criminal Tribunal for the Former Yugoslavia 67
Box No. 31: Direction and Control of the National Security Services in Hungary 69
Box No. 32: Duties of the Minister vis-à-vis the Agency (Australia) 69
Box No. 33: Measures to Safeguard the Impartiality of the Agency 70
Box No. 34: The Head of Agency's Right of Access to the Prime Minister (UK) 70
Box No. 35: Comparison of the External and Parliamentary Oversight Bodies in Selected Countries 78
Box No. 36: A Comprehensive List of Tasks for a Parliamentary Oversight Body 81
Box No. 37: Elements of Parliamentary Oversight (Germany) 81
Box No. 38: The Provision of *ad hoc* Reference of Operational Matters to the Parliamentary Oversight Body 83
Box No. 39: Parliamentary Oversight Focusing on the Rule of Law and Human Rights: The Example of Norway 83
Box No. 40: Appointing Members of Parliamentary Oversight Bodies: Examples from selected states 86
Box No. 41: Clearance of the Norwegian Parliamentary Intelligence Oversight Committee 88
Box No. 42: Dealing with Denial of Security Clearances for Members of Parliament of Bosnia and Herzegovina 89
Box No. 43: The Argentinean Joint Committee's Right to Information 91
Box No. 44: Duty to keep the Congressional Committees Fully and Currently Informed about Intelligence Activities (US) 91
Box No. 45: Reporting of Covert Action to the US Congressional Intelligence Committees 92
Box No. 46: Consulting External Expertise (Luxembourg) 93
Box No. 47: Informing Legislature and Executive about a Committee's Activities and Recommendations (South Africa) 94
Box No. 48: Restrictions on Disclosure to Parliament (Australia) 95
Box No. 49: Financial Auditing by the German Parliamentary Control Panel 98
Box No. 50: Comprehensive Budget Control by Parliament (Hungary) 99
Box No. 51: Handling of Complaints: the Dutch National Ombudsman 106

Box No. 52:	Handling of Complaints: the Norwegian Parliamentary Intelligence Oversight Committee	106
Box No. 53:	Handling of Complaints: the Canadian Security Intelligence Review Committee	107
Box No. 54:	The Functions of the Canadian Inspector-General	111
Box No. 55:	The Auditor General	114
Box No. 56:	Statutory Disclosure of Information of the Services to the Auditor (UK)	115
Box No. 57:	Financial Accountability (Luxembourg)	116
Box No. 58:	Independent Audit of Projects: the Example of the National Headquarters Building Project of the Canadian Security and Intelligence Services (CSIS) by the Auditor General of Canada	117

List of Acronyms

AHRB	Arts and Humanities Research Board
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
CAT	Convention against torture
CIA	Central Intelligence Agency (US)
CoE	Council of Europe
Cth	Commonwealth
CSIS	Canadian Security Intelligence Service
CDPC	European Committee on Crime Problems
DAC	Development Assistance Committee (OECD)
DCAF	Geneva Centre for the Democratic Control of Armed Forces
DSD	Defence Signals Directorate (Australia)
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EHRR	European Human Rights Reports
EOS	Norwegian Parliamentary Intelligence Oversight Committee
EU	European Union
FRG	Federal Republic of Germany
GCHQ	Government Communications Headquarters (UK)
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
IPU	Inter-Parliamentary Union
MI5	Security Service (UK)
MI6	Secret Intelligence Service (UK)
OECD	Organisation for Economic Cooperation and Development
OSCE	Organisation for Security and Cooperation in Europe
PACE	Parliamentary Assembly of the Council of Europe
PC-S-SEC	Group of Specialists on Internal Security Services (CoE)
PKGrG	Law on the German Parliamentary Control Panel
PKGr	German Parliamentary Control Panel
RCMP	Royal Canadian Mounted Police
RSA	Republic of South Africa
SIRC	Security Intelligence Review Committee (Canada)
UK	United Kingdom
UN	United Nations
UNDHR	Universal Declaration of Human Rights
UNDP	United Nations Development Programme
UN GA	United Nations General Assemby
USC	United States Code
WEU	Western European Union

Section I

Introduction

Chapter 1

Defining Democratic Oversight of Security and Intelligence Services

There could scarcely be a more appropriate time to address the issue of oversight of security and intelligence services. In the wake of 9/11, the second Iraq war and 11/M (terror attacks in Madrid on 11 March 2004), many of those responsible for overseeing intelligence in both parliaments and the executive are currently involved in investigating the services and the way political leaders handle intelligence. Those involved in oversight, including not only parliamentarians and the responsible ministers, but also the judiciary and (more loosely) media and civil society organisations, face a difficult task. In balancing the commitments both to security and democracy, they have to judge whether proposals from the intelligence services are justified in terms of making the services more effective on the one hand, while keeping them accountable and within the rule of law, on the other hand.

International Consensus

At the same time there is a growing international consensus on the issue of democratic oversight of intelligence services. International organisations such as the Organisation for Economic Co-operation and Development (OECD),[1] the United Nations (UN),[2] the Organisation for Security and Cooperation in Europe (OSCE),[3] the Parliamentary Assembly of the Council of Europe (PACE)[4] and the Inter-Parliamentary Union[5] all explicitly recognise that the intelligence services should be subject to democratic accountability. Box No. 1 gives a further overview of norms and standards of oversight of security and intelligence services as adopted by regional and global international organisations.[6]

Democratic Oversight: Various Institutions and Actors

Democratic accountability of intelligence services requires executive control and parliamentary oversight as well as inputs by civil society. Overall, the objective is that security and intelligence agencies should be insulated from political abuse without being isolated from executive governance[7]. Security and intelligence services must be responsive to the needs of the people through their elected representatives, i.e. elected civilians in the cabinet and parliament who embody the primacy of political control over the security and intelligence services. In short, democratic oversight of the security services includes a range of institutions and actors (see Box No. 2).[8]

Box No. 1:
Norms and Standards for Democratic Oversight of Security and Intelligence Services as adopted by (selected) international organisations

Organisation	Norm/Standard	Source
UNDP	Democratic civil control of the military, police and other security forces (report enumerates principles of democratic governance in the security sector)	Human Development Report (2002)
OSCE	'The democratic political control of military, paramilitary and internal security forces as well as of intelligence services and the police' (specified by a detailed set of provisions)	Code of Conduct on Politico-Military Aspects of Security (1994)
Council of Europe (Parliamentary Assembly)	'Internal security services must respect the European Convention on Human Rights…Any interference by operational activities of internal security services with the European Convention on Human Rights must be authorised by law.' 'The legislature should pass clear and adequate laws putting the internal security services on a statutory basis'.	Recommendation 1402 (1999)
EU (European Parliament)	Specifying the 'Copenhagen Criteria' for accession to include: 'legal accountability of police, military and secret services […].'	Agenda 2000, § 9
Summit of the Americas	'The constitutional subordination of armed forces and security forces to the legally constituted authorities of our states is fundamental to democracy'	Quebec Plan of Action (2001)
Inter-Parliamentary Union	'Democratic oversight of intelligence structures should begin with a clear and explicit legal framework, establishing intelligence organisations in state statutes, approved by parliament. Statutes should further specify the limits of the service's powers, its methods of operation, and the means by which it will be held accountable'.	*Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices,* Handbook for Parliamentarians no. 5. Geneva: IPU/DCAF, 2003, p. 64.
Assembly of Western European Union (WEU)	'Calls on the national parliaments to: (1) Support plans for reforming intelligence systems, while defending parliamentary prerogatives with a view to more efficient and effective democratic scrutiny of intelligence gathering activities and of the use to which that information is put.'	Resolution 113 (adopted unanimously and without amendment by the Assembly on 4 December 2002 [9th sitting].)
OECD	The security system [including security and intelligence services] should be managed according to the same principles of accountability and transparency that apply across the public sector, in particular through greater civil oversight of security processes.	DAC Guidelines and Reference Series 'Security system reform and governance: policy and good practice', 2004

Each actor or oversight institution has a different function. The executive *controls* the services by giving direction to them, including tasking, prioritising and making resources available. Additionally, the parliament focuses on *oversight,* which is limited more to general issues and authorisation of the budget. The parliament is more reactive when setting up committees of inquiry to investigate scandals. The judiciary is tasked with *monitoring* the use of special powers (next to adjudicating wrong-doings). Civil society, think-tanks and citizens may *restrain* the functioning of the services by giving an alternative view (think-tanks), disclosing scandals and crises (media), or by raising complaints concerning wrong-doing (citizens).

Box No. 2:
Oversight Institutions and Actors

- Internal control by the services themselves through legalising their functioning by law (enacted by parliament), internal direction and stimulating a professional work attitude;
- The executive, which exercises direct control, determines the budget, and sets general guidelines and priorities for the activities of the security and intelligence services;
- The legislature, which exercises parliamentary oversight by passing laws that define and regulate the security and intelligence services as well as their special powers and by adopting the corresponding budgetary appropriations;
- The judiciary, which both monitors the special powers of the security and intelligence services and prosecutes wrong-doing by their employees;
- Civil society groups, media, think-tanks and research institutes which monitor the set-up and functioning of the security and intelligence services, primarily on the basis of public sources. Individual citizens may restrain the use of special powers by security and intelligence services via special tribunals, independent ombudsmen or commissioners/inspectors-general, as well as national and international courts.
- On the international level, no oversight of security and intelligence services exists, although the European Court of Human Rights (ECHR), operating under the European Convention on Human Rights, can receive petitions from individuals about the actions of governmental bodies in nearly all European states.

Additionally, because democratic oversight of the intelligence services involves the behaviour of various actors involved, it is also about political culture. Keystones of democratic accountability such as transparency, responsibility, accountability, participation and responsiveness (to the people) imply a culture and certain behaviour which goes beyond laws and other legal rules. Nevertheless, laws should lay down a framework which fosters a culture of openness and respect for human rights.

Chapter 2

The Need for Oversight of the Security and Intelligence Services

Security and intelligence services perform a valuable service to democratic societies in protecting national security and the free order of the democratic state. Because the services work clandestinely and the nature of their tasks requires them to fulfil their obligations in secret, they are at odds with the principle of open society. It is because of this paradox (defence of an open society by secretive means), that the security and intelligence services should be the object of democratic accountability and civilian control. The public control of these services is important for at least five reasons.

Firstly, contrary to the concept of openness and transparency which is at the heart of democratic oversight, security and intelligence services often operate in secret. As secrecy may shield their operations from scrutiny by the public, it is important that the parliament and especially the executive have a close eye on the services' operations. Secondly, the security and intelligence services possess special powers, such as the ability to interfere with private property or communications, which clearly can limit human rights and require monitoring by the designated oversight institutions. As put forward by the Parliamentary Assembly of the Council of Europe (CoE):

> Serious concerns exist that internal security services of CoE member States often put the interest of what they perceive as those of national security and their country above respects for the rights of the individual. Since, in addition, internal security services are often inadequately controlled, there is a high risk of abuse of power and violations of human rights, unless legislative and constitutional safeguards are provided.[9]

In particular, problems arise in cases where the internal security services have acquired certain powers such as preventive and enforcement methods, in combination with inadequate control by the executive, legislature and judiciary, as well as when a country has a large number of different secret services.[10]

Thirdly, during the post Cold War era and especially after 11 September 2001, the intelligence communities of nearly all states are in a process of readjustment to the new security threats. The greatest perceived threat to the functioning of democratic societies is no longer that of a foreign military invasion, but rather organised crime, terrorism, spillovers of regional conflicts or failed states, and the illegal trafficking of people and goods. This readjustment process should be under the supervision of the elected civilian authorities who can provide assurance that the restructuring of the services are aligned to the people's need. Furthermore, because intelligence services are large government bureaucracies with an inherent resistance to change and with a certain degree of bureaucratic inertia, outside institutions such as the executive and

the parliament have to ensure that the desired changes are implemented in an efficient manner.

Fourthly, security and intelligence services are tasked to collect and analyse information about possible threats and to make threat assessments. As the threat assessments form the point of departure for the other security forces of the state (military, police, border guards), it is important that these threat assessments are made under democratic guidance. This is especially relevant because these assessments imply a prioritisation of threats which usually have major political implications.

A fifth reason applies to those countries which were under an authoritarian regime and which have made their transition to democracy recently. In the past, the main task of internal security and intelligence services in those countries was to protect authoritarian leaders against their own people. Primarily, the security and intelligence services fulfilled a repressive function. One can imagine the enormous task that has to be undertaken to reform the old security services into modern democratic services. Reforming services to change them from a tool of repression into a modern tool of security policy requires careful monitoring by the executive and parliament.

The Need for Legislation

The rule of law is a fundamental and indispensable element of democracy. Only if security and intelligence agencies are established by law and derive their powers from the legal regime can they be said to enjoy legitimacy. Without such a framework there is no basis for distinguishing between actions taken on behalf of the state and those of law-breakers, including terrorists. 'National security' should not be a pretext to abandon the commitment to the rule of law which characterises democratic states, even in extreme situations. On the contrary, the exceptional powers of security services must be grounded in a legal framework and in a system of legal controls.

Legislation is the legal embodiment of the democratic will. In most states, approving legislation (along with scrutinising government actions) is among the key roles of the parliament. It is therefore appropriate that in democracies where the rule of law prevails, intelligence and security agencies derive their existence and powers from legislation, rather than exceptional powers such as the prerogative. This enhances the agencies' legitimacy and enables democratic representatives to address the principles that should govern this important area of state activity and to lay down limits to the work of such agencies. Moreover, in order to claim the benefit of legal exceptions for national security to human rights standards it is necessary that the security sector derive its authority from legislation.

Parliamentary approval of the creation, mandate and powers of security agencies is a necessary but not sufficient condition for upholding the rule of law. A legal foundation increases the legitimacy both of the existence of these agencies and the (often exceptional) powers that they possess. As in other areas, one key task of the legislature is to delegate authority to the administration but also to structure and confine discretionary powers in law.

Restricting Constitutional and Human Rights

Legislation is also necessary where it is intended to qualify or restrict the constitutional rights of individuals in the security interests of the state. This can occur in two distinct ways. The first is through the regular limitation of human rights to take account of societal interests.[11] The restriction of freedom of expression of intelligence officials to preserve secrecy concerning their work is an obvious example. Secondly, in emergency situations where the security of the state is gravely affected, temporary suspension of some rights by way of derogation may be permitted. As Box No. 3 shows, some human rights are non-derogable, however.

Box No. 3:
Non-Derogable Human Rights

According to Article 4 para. 2 of the ICCPR, no derogation is permitted from the following rights:

- To life (Article 6);
- Not to be subjected to torture or to cruel, inhuman or degrading treatment or punishment (Article 7);
- Not to be held in slavery or servitude (Article 8);
- Not to be imprisoned for failure to perform a contractual obligation (Article 11);
- Not to be subject to retroactive penal measures (Article 15);
- To recognition as a person before the law (Article 16);
- To freedom of thought, conscience and religion (Article 18).

Source: International Covenant on Civil and Political Rights (entered into force in 1976).

In the case of rights that may be restricted or limited at the international level, the European Convention on Human Rights, for example, allows restrictions to the rights of public trial, respect for private life, freedom of religion, freedom of expression and of association 'in accordance with law' (see Box No. 5, Quality of Law Test), and where 'necessary in a democratic society' in the interests of national security.[12] Additionally, if the services possess the legal power to interfere with private property and communications, citizens should have a legal procedure available for making complaints if any wrongdoing occurs. This is one way in which states that are signatories to the ECHR can meet their obligation to provide an effective remedy for arguable human rights violations under Article 13 of that Convention (see also Chapter 21).

Assuming the necessity for legislation to restrict political and human rights as a point of departure, two implications are distinguishable. Firstly, intelligence services have to be established by legislation and secondly, the special powers that intelligence services exercise must be grounded in law.

Security Agencies Should be Established by Legislation

Many states have now taken the step of codifying in law the constitutions of their security forces. Some recent examples include legislation in Bosnia and Herzegovina,

Slovenia, Lithuania, Estonia and South Africa.[13] However, there are considerable variations. Not surprisingly, concern about agencies operating in the domestic sphere gives rise to fears of abuse or scandal even in long-established democracies. In transitional states often the domestic security agency has been tainted by a repressive past.

Accordingly, many states have now legislated for these agencies, mostly in the last two decades. There are fewer reasons to place a country's own espionage agency on a legal basis – the UK was unusual in doing so in the case of the Secret Intelligence Service (MI6) in the Intelligence Services Act 1994.[14] Again, only a few states have legislated for military intelligence[15] or intelligence coordination.[16]

Box No. 4:

Necessity of Legislating for the Intelligence Services due to the ECHR (UK)

In the case of *Harman and Hewitt v UK*[17] brought under the ECHR, the lack of a specific statutory basis for the UK Security Service (MI5) was held to be fatal to the claim that its actions were 'in accordance with the law' for the purpose of complaints of surveillance and file-keeping contrary to Article 8 of the Convention on the right to privacy. An administrative charter – the Maxwell-Fyfe Directive of 1952 – was insufficient authority for the surveillance and file-keeping since it did not have the force of law and its contents were not legally binding or enforceable. In addition, it was couched in language which failed to indicate 'with the requisite degree of certainty, the scope and the manner of the exercise of discretion by the authorities in the carrying out of secret surveillance activities'.[18] As a consequence of the ruling in the case, the UK passed a statutory charter for MI5 (the Security Service Act 1989), and later took a similar step for the Secret Intelligence Service and GCHQ also (see the Intelligence Services Act 1994).

Specific Powers that Security and Intelligence Agencies Exercise Should be Grounded in Law

Legality requires that security forces act only within their powers in domestic law. Consequently, only lawful action can be justified by way of interference with human rights under the European Convention. For example, when the Greek National Intelligence Service was found to have been conducting surveillance on Jehovah's Witnesses outside its mandate, it was held to have violated Article 8, which guarantees respect for one's private life.[19]

The rule of law requires more than a simple veneer of legality, however. The European Court of Human Rights refers additionally to the 'Quality of Law' test (see Box No. 5), this requires the legal regime to be clear, foreseeable and accessible. For example, where a Royal Decree in the Netherlands set out the functions of military intelligence but omitted any reference to its powers of surveillance over civilians, this was held to be inadequate.[20] Similarly, in *Rotaru v Romania,*[21] the Strasbourg Court held that the law on security files was insufficiently clear as regards grounds and

procedures since it did not lay down procedures with regard to the age of files and the uses to which they could be put, or establish any mechanism for monitoring them.

The 'quality of law' test of the ECHR puts a particular responsibility on legislatures. One possible response is to write into the law general statements that the powers of agencies can only be used where 'necessary', that alternatives less restrictive of human rights are always to be preferred, and that the principle of proportionality should be observed.[22] Perhaps preferable is the alternative, followed in the new legislation from the Netherlands, of giving detailed provisions governing each investigative technique that the agency may utilise (see Chapter Six).[23]

Box No. 5:
Quality of Law Test

The European Convention of Human Rights stipulates that in a democratic society the right of privacy (Art 8), the freedom of thought, conscience and religion (Art 9) as well as the freedom of expression (Art 10) and the freedom of assembly and association (Art 11) can be limited, among others, in the interests of national security and public order. However, the Convention also prescribes that these limitations have to be made 'in accordance with the law'. Case law of the European Court of Human Rights has said, *inter alia*, that security and intelligence services can only exercise their special powers if they are regulated by law. In this respect, according to the European Court:

- Laws includes common law rules as well as statutes and subordinate legislation. In this case, the Court stated that to qualify as 'law' a norm must be adequately accessible and formulated with sufficient precision to enable the citizen to regulate his conduct (*Sunday Times v UK,* 26 April 1979, 2 EHRR 245, para 47);
- A law which 'allows the exercise of unrestrained discretion in individual cases will not posses the essential characteristics of foreseeability and thus will not be a law for present purposes. The scope of the discretion must be indicated with reasonable certainty.' (*Silver and Others v UK,* 25 Mar. 1983, 5 EHRR 347, para 85);
- Checks and other guarantees to prevent the misuse of powers by the intelligence services must be established if there is to be consistency with fundamental human rights. Safeguards must exist against abuse of the discretion established by law (*Silver and Others v UK*, para 88-89);
- As far as these safeguards are not written in the law itself, the law must at least set up the conditions and procedures for interference (*Klass v FRG,* No. 5029/71, Report of 9 March 1977 para 63. *Kruslin v France,* 24 April 1990. A/176-A, para 35, *Huvig v France,* 24 April 1990, A/176-B, para. 34).

Source: European Court of Human Rights' website http://www.echr.coe.int/
Ian Cameron, *National Security and the European Convention on Human Rights*, 2000, Kluwer Law International.

Chapter 3

In Search of Legal Standards and Best Practice of Oversight: Objectives, Scope and Methodology

In order to assist in the process of clarifying the nature of oversight and to spread good practice, the Geneva Centre for the Democratic Control of Armed Forces (DCAF), the Human Rights Centre of Durham University (UK) and the Norwegian Parliamentary Intelligence Oversight Committee decided to join forces in drafting legal standards for democratic accountability of the security and intelligence services and in collecting best legal practices and procedures of oversight. The publication proposes legal standards on the basis of analysis of the legal framework for oversight in liberal democracies in the Americas, Europe, Africa and Asia. The aim is to distil the best practices and procedures from the intelligence oversight legislation of various democratic states and so to provide a useful reference tool for parliamentarians and their staff, for (government) officials from other oversight institutions, the intelligence services themselves, as well as civil society (media, research institutes, etc). The main aspects of democratic oversight of security and intelligence services are covered, including the executive, legislature, the judiciary, as well as independent oversight organisations such as ombudsmen or inspector-generals.

Good Governance

The legal standards and best practice were selected on the basis of whether they constitute or promote good governance of the security sector. As an important aspect of the democratic oversight of the security sector, good governance is crucial to any functioning government. As the World Bank states,

> Good governance is epitomised by predictable, open and enlightened policy-making, a bureaucracy imbued with a professional ethos acting in furtherance of the public good, the rule of law, transparent processes, and a strong civil society participating in public affairs.[24]

The following principles are at the centre of good governance:

- Equity;
- Participation;
- Pluralism;
- Partnership;
- Subsidiarity;
- Transparency;
- Accountability;

- Rule of law;
- Human rights;
- Effectiveness;
- Efficiency;
- Responsiveness;
- Sustainability;[25]

While good governance reflects the rules, institutions and practices for effective and democratic government, including the respect of human rights, poor governance is characterised by 'arbitrary policy-making, unaccountable bureaucracies, un-enforced or unjust legal systems, the abuse of executive power, a civil society unengaged in public life, and widespread corruption'.[26] A government's adherence to the principles of good governance is of great importance to the setting of acceptable political and legal boundaries to the functioning of security and intelligence services.

Scope

The scope of the exercise is, however, limited in two ways. Firstly, the proposed legal standards deal with intelligence services only, not law enforcement. Secondly, because more detailed issues are normally regulated by executive ordinances and decrees, only the more general issues of democratic oversight are addressed.

Collecting and assessing legal standards for oversight, which can be helpful when overseers are adopting new or amending existing oversight laws, is not the panacea of all oversight problems. The main reason is that laws can only go so far. Political and administrative culture, the media and public opinion are ultimately the best safeguards for democratic values. Modern history is littered with states that have disregarded human rights while subscribing to high-sounding constitutional documents and treaties. Nevertheless, a legal framework can help to reinforce these values and give them a symbolic status that will encourage powerful actors to respect them. This is particularly so where new institutions are created – the legal framework can be a means of inculcating a new democratic order and concretising reforms.

The search for universal principles might appear to be fruitless in view of different political and cultural traditions. Quite apart from the differences between established Western states and emerging democracies, there is also a wide variety of constitutional models, notably 'Presidential executives' like the USA, 'dual executives' like France, or Westminster-style Parliamentary executives. Some countries give powers of constitutional review to their courts based on the pattern of the US Supreme Court, in others (of which the UK is the exemplar) the courts defer to Parliament. Even within the one type of system, wide variations may exist – quite different patterns of oversight for security and intelligence have emerged in the UK, Australia, Canada and New Zealand, for example.[27]

For this reason we have not attempted to provide a simple blueprint or a model law which can be incorporated into domestic law, regardless of constitutional differences. Rather, our approach is to identify common issues that arise regardless of these differences and then to suggest ways in which these can be overcome, both by

proposing minimum democratic standards, and by giving examples of good legal practice in a variety of different countries. By collecting and discussing good legal practice of oversight of security and intelligence services in democracies, the proposed legal standards intend to give lawmakers, government officials and representatives of civil society, in both established and establishing democracies, guidelines and options for legislation. The proposed legal standards should not be interpreted as a straightjacket for democratic oversight. Rather, they represent a set of principles from which particular national rules may be developed. A 'golden rule' or law for democratic oversight cannot and will not exist.

Methodology

The legal standards and best practice need to be developed at four levels for the oversight of the intelligence and security services. Each of these can be seen as a layer of democratic oversight that is encapsulated by the next layer:

- Internal control at the level of the agency
- Executive control
- Parliamentary oversight
- Oversight by independent oversight bodies

Firstly, oversight takes place at the level of the agency itself. Control at this level includes issues such as the proper implementation of laws and government policies, the authority and functioning of the head of the agency, the proper handling of information and files, the use of special powers according to the law, and the internal direction of the agency. Internal control procedures of this kind at the level of the agency itself are an essential foundation for external democratic oversight by the executive, parliament and independent bodies. These internal control mechanisms ensure that the policies and laws of the government are carried out in an efficient, professional and legal manner.

The second layer refers to control by the executive which focuses on tasking and prioritising the services, including ministerial knowledge and control over the services, control over covert operations, control over international cooperation and safeguards against ministerial abuse. The third layer concerns parliamentary oversight, which fulfils an important role in the system of checks and balances by overseeing general policy, finance and the legality of the services. In most countries, the functioning of the services is grounded on laws enacted by parliaments. The role of the independent oversight bodies, the fourth layer of democratic oversight, concerns an independent check from the viewpoint of the citizen (eg ombudsman or parliamentary commissioner), the viewpoint of the prompt execution of government policy (for example the Inspector General) and from the viewpoint that taxpayers' money is involved (by independent audit offices).

Two important actors are not visibly included in this layered approach to democratic oversight. The judiciary (including international courts) is left out as its functioning is discussed at various places within the four layers, for example, concerning the use of special powers or handling complaints. Additionally, civil society is left out as this

publication focuses primarily on the role of (independent) state institutions. Nevertheless, the position of the citizen is discussed at various points in this document, for example, when it comes to the handling of files and information and the role of parliament as representative of the citizens as well as the existence of procedures for handling complaints.

The examples of the legal standards and practice are based on extensive comparative research in democratic societies. The sample of analysed countries includes, among others, Argentina, Australia, Belgium, Bosnia-Herzegovina, Canada, Estonia, Germany, Hungary, Luxembourg, the Netherlands, Norway, Poland, South Africa, Turkey, the United Kingdom and the U.S.A. The selected states are all democracies whose legislatures have adopted intelligence oversight laws; they are examples of both parliamentary and presidential political systems; and they include established and newly established democracies, as well as a variety of political cultures.

Endnotes Section I – Introduction

1. OECD, Development Assistance Committee, *Development Co-operation Report 2000*, p. 8. Report available at: <http://www.oecd.org/home/>.
2. UNDP, *Development Report 2002*, Deepening democracy in a fragmented world, p. 87. Report available online at: <http://hdr.undp.org/reports/global/2002/en>.
3. OSCE, *Code of Conduct on Politico-Military Aspects of Security*, 1994, paragraphs 20-21.
4. Parliamentary Assembly of the Council of Europe, *Recommendation 1402*. Available online at: <http://assembly.coe.int/Documents/AdoptedText/ta99/EREC1402.htm>.
5. Born, H., Fluri, Ph., Johnsson, A. (eds.), *Parliamentary Oversight of the Security Sector; Principles, Mechanisms and* Practices, (Geneva: IPU/DCAF, 2003), pp. 64-69.
6. See also Hänggi, H., 'Making Sense of Security Sector Governance', in: Hänggi, H., Winkler, T. (eds.), *Challenges of Security Sector Governance*. (Berlin/Brunswick, NJ: LIT Publishers, 2003).
7. Leigh, I., 'More Closely Watching the Spies: Three Decades of Experiences', in: Born, H., Johnson, L., Leigh, I., *Who's watching the Spies? Establishing Intelligence Service Accountability* (Dulles, V.A.: Potomac Books, INC., 2005).
8. Based on Born, H. et al., '*Parliamentary Oversight*', p. 21.
9. Parliamentary Assembly of the Council of Europe, Recommendation 1402, pnt. 2.
10. *Ibid*., pnt. 5.
11. See also the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (UN Doc, E/CN.4/1985/Annex 4), available at: <http://www1.umn.edu/humanrts/instree/siracusaprinciples.html>; Lillich, R. B., 'The Paris Minimum Standards of Human Rights Norms in a State of Emergency', *American Journal of International Law*, Vol. 79 (1985), pp. 1072-1081.
12. European Convention on Human Rights, Arts. 6, 8, 9, 10, and 11.
13. Slovenia: Law on Defence, 28 December 1994, Arts. 33-36; The Basics of National Security of Lithuania, 1996**;** Estonia: Security Authorities Act passed 20 December 2000; RSA: Intelligence Services Act, 1994.
14. The same Act also covers the signals intelligence agency, GCHQ.
15. See, for example, the Netherlands, Intelligence and Security Services Act 2002, Art. 7.
16. Article 5 of the same Netherlands Act; National Strategic Intelligence Act 1994 of the Republic of South Africa.
17. *Harman and Hewitt v UK* (1992) 14 E.H.R.R. 657.
18. *Ibid.,* para. 40.
19. *Tsavachadis v Greece*, Appl. No. 28802/95, (1999) 27 E.H.R.R. CD 27.
20. *V and Others v Netherlands*, Commission report of 3 Dec. 1991; and see also in applying the 'authorised by law' test to various forms of surveillance: *Malone v UK* (1984) 7 E.H.R.R. 14; *Khan v UK,* May 12, 2000, European Ct HR (2000) 8 BHRC 310; *P G. and J.H. v UK*, European Court of Human Rights, 25 Sept. 2001, ECtHR Third Section.
21. No. 28341/95, 4 May 2000. See also *Leander v Sweden* (1987) 9 E.H.R.R. 433, holding that in order to be 'in accordance with law' the interference with privacy must be foreseeable and authorised in terms accessible to the individual. In the context of security vetting this did not require that the applicant should be able to predict the process entirely (or it would be easy to circumvent), but rather that the authorising law should be sufficiently clear as to give a general indication of the practice, which it was.
22. This is the approach taken in Estonia (Security Authorities Act, paragraph 3).
23. Intelligence and Security Services Act 2002, Articles 17-34.
24. The World Bank, 'Governance: The World Bank's Experience,' cited in Born, H. et al, '*Parliamentary Oversight*', p. 23.

25. Special mention must be made of Magdy Martinez Soliman, *Democratic Governance Practice Manager, Bureau for Development Policy UNDP*, for her valuable insights on the principles of good governance. For the purpose of this publication, refer to the Glossary which features a selection of the most relevant concepts for intelligence accountability. Regarding the other concepts, refer to, for example the UNDP glossary, available at: <http://www.undp.org/bdp/pm/chapters/glossary.pdf>
26. *Ibid.*
27. Lustgarten, L, Leigh, I, *In From the Cold: National Security and Parliamentary Democracy* (Oxford: Oxford University Press, 1994), Chapters 15 and 16, which gives a fuller treatment of the issue of accountability.

Section II

The Agency

Chapter 4

Defining the Mandate

A key aspect of accountability for security and intelligence agencies is that their role and sphere of operation should be clearly defined. This should be done in legislation – emphasising that responsibility for delineating the tasks of a security or intelligence agency lies with Parliament and that this role should not be changed without reference to legislators. In transitional states particularly this may help to provide protection from abuse of the agencies by the government. A legal basis is also necessary because of the exceptional powers with which these agencies are often entrusted.

It is also important that security and intelligence agencies are differentiated from other institutions, such as law enforcement bodies, and the legislative mandate can help to do so. Failure to make these clear distinctions, however, will lead to blurred lines of accountability and to the risk that the special powers that security and intelligence agencies possess are used in routine situations where there is no pre-eminent threat to the state.

There are difficult distinctions which need to be made here between threats to national security and criminal action.[1] Terrorism and espionage are criminal matters which directly undermine or even contradict democratic processes, as well as threatening the integrity of the state and its key institutions. Organised crime is different, however. The Council of Europe adopted the following definition:

> Organised crime means: the illegal activities carried out by structured groups of three or more persons existing for a prolonged period of time and having the aim of committing serious crimes through concerted action by using intimidation, violence, corruption or other means in order to obtain, directly or indirectly, a financial or other material benefit.[2]

To many states organised crime, as well as drug- and people-trafficking, are major social and economic ills, yet they do not threaten the stability or survival of the apparatus of government. In a few states, especially some transitional democracies, these issues may assume this level of threat and may therefore justifiably be counted as threats to 'national security'.[3] In most instances organised crime is marked by a scale, longevity and conspiratorial infrastructure that distinguishes it from 'ordinary' criminal activity but does not elevate it to the level which justifies the use of the security and intelligence agencies to investigate or to counter it. On occasion there may be demonstrable links between organised crime and terrorism but this cannot be assumed in every case. Consequently, in some countries, while the security and intelligence agencies are not the lead agencies responsible for investigating organised crime, nevertheless they are given power to assist the law enforcement agencies.[4]

Box No. 6:
The European Court of Human Rights and 'National Security'

Based on the case-law of the Court the following activities – among others – can be considered threats to national security:

- espionage (for example Klass v Federal Republic of Germany judgement of 6 September 1978, paragraph 48);
- terrorism (idem);
- incitement to/approval of terrorism (the Zana judgement of 19 December 1997, paragraphs 48-50);
- subversion of Parliamentary democracy (the Leander judgement of 26 March 1987, paragraph 59);
- separatist extremist organisations which threaten the unity or security of the State by violent or undemocratic means (the judgement in the case of United Communist Party of Turkey and others of 30 January 1998, paragraphs 39-41);
- inciting disaffection of military personnel (Application N° 7050/75 *Arrowsmith vs. United Kingdom* – Report of the European Commission of Human Rights adopted on 12 October 1978).

Source: ECHR case-law.

In any event, it is plainly better to specify by means of detailed legislation the various aspects of national security rather than leaving the mandate of the security and intelligence agencies essentially open-ended through the use of phrases such as 'protecting the security of the state'. The importance of giving specific content to the concept of national security is illustrated by two examples – one from the case-law of a respected international arbiter (the European Court of Human Rights, see Box No. 6) and the second from a recent piece of legislation adopted by Bosnia and Herzegovina (see Box No. 7).

In addition, it is useful to consult the Council of Europe experts' report, which states that 'other matters which may be considered threats to national security are (a) external threats to the economic well-being of the State, (b) money-laundering on a scale likely to undermine the banking and monetary system, (c) interference with electronic data relating to defence, foreign affairs or other matters affecting the vital interests of the State, and (d) organised crime on a scale that may affect the security or well-being of the public or a substantial section of it.'[5]

The example of the Bosnia and Herzegovina law points to the merits of having a codified legal definition of 'national security'. First, it enables parliamentarians to become directly involved in the process of discussing vital national security interests. Often these general debates are very illuminating and contribute to the quality of the law. Second, a definition adds legitimacy to the intelligence practices undertaken in the pursuit of the legally addressed national security interests. Having a law which clearly defines the aspects of national security thus helps to protect a nation against the politicisation and downright abuses of its intelligence services.

A second noteworthy aspect that concerns the agencies' mandate deals with their territorial competences and different level of engagement. In so doing, it is possible to distinguish between four distinct variable factors: internal (domestic) service, external (foreign) service, mandates limited to the collection and analysis of information, as well as mandates allowing agencies to act to counter domestic or foreign security threats. With regard to the first two factors, it seems common practice to refer to 'intelligence services' for agencies with foreign mandates and to 'security services' for agencies with domestic mandates. Both 'intelligence services' and 'security services' can have either a more pro-active mandate or be restricted to the gathering and analysis of information. Combining these factors, several different types of institutional arrangements have been adopted by states:

A. A single agency for security and intelligence (both domestic and external) eg Bosnia and Herzegovina, The Netherlands, Spain and Turkey.
B. Separate agencies for domestic and external intelligence and security, with either separate or overlapping territorial competences eg UK, Poland, Hungary and Germany.
C. A domestic security agency but no acknowledged or actual foreign intelligence agency eg Canada.

Box No. 7:
A Legislative Definition of National Security (Bosnia and Herzegovina)

For the purpose of this Law, 'threats to the security of Bosnia and Herzegovina' shall be understood to mean threats to the sovereignty, territorial integrity, constitutional order, and fundamental economic stability of Bosnia and Herzegovina, as well as threats to global security which are detrimental to Bosnia and Herzegovina, including:

1. terrorism, including international terrorism;
2. espionage directed against Bosnia and Herzegovina or otherwise detrimental to the security of Bosnia and Herzegovina;
3. sabotage directed against the vital national infrastructure of Bosnia and Herzegovina or otherwise directed against Bosnia and Herzegovina;
4. organised crime directed against Bosnia and Herzegovina or otherwise detrimental to the security of Bosnia and Herzegovina;
5. drug, arms and human trafficking directed against Bosnia and Herzegovina or otherwise detrimental to the security of Bosnia and Herzegovina;
6. illegal international proliferation of weapons of mass destruction, or the components thereof, as well as materials and tools required for their production;
7. illegal trafficking of internationally controlled products and technologies;
8. acts punishable under international humanitarian law; and organised acts of violence or intimidation against ethnic or religious groups within Bosnia and Herzegovina.

Source: Article 5, Law on the Intelligence and Security Agency of Bosnia and Herzegovina 2004.

In this regard, the particular situation of intelligence services in federal states such as the United States or Germany should also be mentioned. Due to its federal state structure, each of the 16 German states (*Bundesländer*) has its own intelligence service (*Landesamt für Verfassungsschutz*), which cooperate with each other and the

federal intelligence service (*Bundesamt für Verfassungsschutz*). Generally, it holds true that the more intelligence services there are, the greater will be the danger of fragmented oversight.

Generally, it holds true that the more intelligence services there are, the greater will be the danger of fragmented oversight.

Where an intelligence agency has powers to act externally it is common to find safeguards for the position of the state's own citizens (see, for instance, the legislation governing the Australian Secret Intelligence Service and the Defence Signals Directorate).[6] The use and control of special powers of intelligence agencies merits its own discussion (see Chapter 6).

Maintaining Political Neutrality

In post-authoritarian societies there are often strong memories of security and intelligence services endowed with broad mandates and sweeping powers used to protect dictatorial regimes against rebellions from their own people. Services were used by such regimes to suppress political opposition, to prevent any kind of demonstration and to eliminate leaders of labour unions, the media, political parties and other civil society organisations. In doing so, the services intervened deeply in the political and daily life of the citizens. After the transition to democracy, the new leaders were determined to curtail the mandate and powers of the services and to guarantee its political neutrality. A clear example of this practice is given by the Argentine National Intelligence Law of 2001. The law includes, amongst other things, institutional and legal safeguards to prevent the use of services by government officials against political opponents (see Box No. 8).

Box No. 8:

Safeguards to Prevent the Use of Intelligence Agencies by Government Officials against their Domestic Political Opponents (Argentina)

'No intelligence agency shall:
1. Perform repressive activities, have compulsive powers, fulfil police functions or conduct criminal investigations unless so required by justice on account of a judicial proceeding or when so authorised by law.
2. Obtain information, collect intelligence or keep data on individuals because of their race, religion, private actions, and political ideology, or due to their membership in partisan, social, union, community, cooperative, assistance, cultural or labour organisations, or because of legal activities performed within any field.
3. Exert influence over the institutional, political, military, police, social, and economic situation of the country, its foreign policies, and the existence of legally formed political parties, or influence public opinion, individuals, the media, or any kind of associations whatsoever'.

Source: Article 4 of National Intelligence Law No. 25520 (Argentina,).

Best Practice

- ✓ The role of a security or intelligence agency should be clearly defined and limited to matters which should be specified in detail and involve serious threats to national security and the fabric of civil society;
- ✓ The concepts of threats to national security and the fabric of civil society should be legally specified;
- ✓ The territorial competence of a security or intelligence agency should be clearly defined and any powers to act outside the territory should be accompanied by safeguards;
- ✓ The tasks and powers of the agency within its mandate should be clearly defined in legislation, enacted by parliament;
- ✓ Especially in post-authoritarian states, it is important to have legal and institutional safeguards in place, preventing the misuse of security and intelligence against domestic political opponents.

Chapter 5

Appointing the Director

A key aspect of the legislation governing intelligence and security agencies is the process for appointing the Director. Personal qualities of leadership, integrity and independence are necessary in the person appointed. This will inevitably be a senior official position and it is important that the process of appointment reinforces and guarantees the status of the position. It is desirable that members of the executive (either the head of state, or in a mixed system, the prime minister) take the initiative in making such appointments, on advice.

As a minimum, it is necessary that the appointment should be open to scrutiny outside the executive. Constitutional traditions vary, however, in how this takes place in the case of senior government posts. In some countries (for instance, the UK) the safeguards against abuse rest on conventions which, if they were broken, would lead to political criticism and possible censure by independent officials. In other states, a formal confirmation or consultation procedure is commonplace, which enables the legislature to either veto or express their opinion on an appointment. This may be underwritten by a constitutional requirement either that official appointments must be approved by parliament or, alternatively, that they can be blocked by a parliamentary vote (for example, Congressional confirmation of federal officials and judges under the US Constitution). Notice that a parliamentary verdict of non-agreement on a proposed nominee may not have the *de jure* consequences of a veto vote but often it will *de facto*. Other noteworthy practices can be found in Belgium, Australia and Hungary. In Belgium, the director-general is obliged to take the oath before the chairman of the Permanent Committee for Supervision of the Intelligence and Security Services before taking office.[7] In Australia, the Prime Minister must consult with the Leader of the Opposition in the House of Representatives (see Box No. 9) concerning the proposed appointment. This provision aims to achieve a broad political backing for the Director's appointment. Whatever the process, these procedures have in common that the government has the initiative, since it alone can propose the name, but then Parliament has a checking role. The checking role may prevent unsuitable candidates being proposed in the first place and may lead to the government discussing, and in some instances, negotiating with other political actors in order to avoid political controversy and to ensure a bi-partisan approach.

Box No. 9:
Involvement of the Parliament in Appointing the Director (Australia)

'(…) Before a recommendation is made to the Governor-General [Head of State] for the appointment of a person as Director-General, the Prime Minister must consult with the Leader of the Opposition in the House of Representatives.'

Source: Intelligence Service Act 2001 (Cth), Part 3, Section 17 (3).

Considering the executive's involvement in the appointment of the Director, the Hungarian law is of interest (see Box No. 10) as it addresses both the respective Minister and the Prime Minister. By increasing the number of cabinet ministers involved in the appointment process, the Hungarian model aims to create a greater political consensus among the political decision-makers.

Box No. 10:
Involvement of the Executive in Appointing the Director (Hungary)

Section 11, 2
In his competence of direction, the Minister (…)
j) shall make proposals to the Prime Minister for the appointment and discharge of the directors general.

Source: Hungarian Law on the National Security Services, Act CXXV of 1995.

Apart from the appointment process, it is also necessary that safeguards should exist, against both improper pressure being applied on the Director and abuse of the office. Provisions for security of tenure, subject to removal for wrongdoing, are therefore commonplace, as demonstrated by the legislation example from Poland (see Box No. 11).

Box No. 11:
Grounds for Dismissal of the Agency Head (Poland)

Article 16
The Head of the Agency may be dismissed in the case of:
his resignation from the occupied post, renunciation of Polish citizenship or acquiring the citizenship of another country, being sentenced by a valid verdict of the court for a committed crime or for a revenue offence, losing the predisposition necessary to hold the post, non-execution of his duties due to an illness lasting continuously for over 3 months.

Source: The Internal Security Agency and Foreign Intelligence Act, Warsaw, 24 May 2002.

Best Practice

- ✓ Legislation should establish the process for the appointment of the Director of a security or intelligence agency and any minimum qualifications or any factors which are disqualifications from office;
- ✓ The appointment should be open to scrutiny outside the executive, preferably in parliament;
- ✓ Preferably, the opposition in parliament should be involved in appointing the Director;
- ✓ Legislation should contain safeguards against improper pressure being applied on the Director and abuse of the office (for example provisions for security of tenure, subject to removal for wrongdoing);
- ✓ The criteria for appointment and dismissal should be clearly specified by the law;

- ✓ Preferably, more than one cabinet member should be involved in the process of appointing a Director, eg the head of state/prime minister and the relevant cabinet minister.

Chapter 6

Authorising the Use of Special Powers

Some intelligence bodies are solely concerned with reporting and analysis (for example the Office of National Assessments (Australia), the Information Board (Estonia) or the Joint Intelligence Committee (UK)). However, where security and intelligence agencies have a pro-active, information-gathering, capacity they will usually be granted specific legal powers and all the more so where their role includes countering or disrupting threats to security, actively gathering intelligence, or law enforcement in the field of national security. 'Special powers' refers therefore to the granting of enhanced powers to security and intelligence agencies that directly affect civil liberties (see Box No. 12).

Box No. 12:
Special Powers of Internal Security and Intelligence Services

The collection of information may require that the intelligence services possess exceptional or special powers, which allow for the limitation of human rights, especially the right to privacy. The following special powers can be distinguished:

1. conduct surveillance and record information as well as trace information;
2. to conduct a search of enclosed spaces or to search closed objects;
3. to open letters and other consignments without consent of the sender or addressee;
4. to use stolen or false identities, keys, special software or signals for clandestinely entering, copying or corrupting databases;
5. to tap, receive, record and monitor conversations, telecommunication, other data transfer or movement – within the country or from abroad;
6. to turn to providers of public telecommunication networks and public telecommunication services with the request to furnish information relating to identity of users as well as all the traffic that has taken place or will take place;
7. to have access to all places for installing observation.

Source: Richard Best, *Intelligence Issues for Congress*, Congressional Research Service, 12 September 2001, Washington DC.

Typically, greater powers are granted than those normally available to the police or other law enforcement bodies because threats to security are seen to be more serious than ordinary criminality.

We do not attempt here to define or limit the exact powers that are appropriate, except to the minimal extent that international legal standards arising from the protection of non-derogable human rights must be observed, whatever the threat to

the state; for example, there are no circumstances in which assassination or torture are appropriate state-sanctioned techniques available to public officials.

In the wake of 9/11, the Council of Europe felt the need to formulate a list of minimal standards that should govern the use of special powers in the efforts made to fight international terrorism (see Box No. 13 overleaf).

Box No. 13:

Selected 2002 Guidelines of the Committee of Ministers of the Council of Europe on Human Rights and the Fight Against Terrorism

II Prohibition of arbitrariness All measures taken by states to fight terrorism must respect human rights and the principle of the rule of law, while excluding any form of arbitrariness, as well as any discriminatory or racist treatment, and must be subject to appropriate supervision.

III Lawfulness of anti-terrorist measures 1. All measures taken by states to combat terrorism must be lawful. 2. When a measure restricts human rights, restrictions must be defined as precisely as possible and be necessary and proportionate to the aim pursued.

IV Absolute prohibition of torture The use of torture or of inhuman or degrading treatment or punishment, is absolutely prohibited, in all circumstances, and in particular during the arrest, questioning and detention of a person suspected of or convicted of terrorist activities, irrespective of the nature of the acts that the person is suspected of or for which he/she was convicted.

V Collection and processing of personal data by any competent authority in the field of state security Within the context of the fight against terrorism, the collection and the processing of personal data by any competent authority in the field of state security may interfere with the respect for private life only if such collection and processing, in particular: (i) are governed by appropriate provisions of domestic law; (ii) are proportionate to the aim for which the collection and the processing were foreseen; (iii) may be subject to supervision by an external independent authority.

VI Measures which interfere with privacy 1. Measures used in the fight against terrorism that interfere with privacy (in particular body searches, house searches, bugging, telephone tapping, surveillance of correspondence and use of undercover agents) must be provided for by law. It must be possible to challenge the lawfulness of these measures before a court. 2. Measures taken to fight terrorism must be planned and controlled by the authorities so as to minimise, to the greatest extent possible, recourse to lethal force and, within this framework, the use of arms by the security forces must be strictly proportionate to the aim of protecting persons against unlawful violence or to the necessity of carrying out a lawful arrest.

XV Possible derogations (…) 2. States may never, however, and whatever the acts of the person suspected of terrorist activities, or convicted of such activities, derogate from the right to life as guaranteed by these international instruments, from the prohibition against torture or inhuman or degrading treatment or punishment, from the principle of legality of sentences and of measures, nor from the ban on the retrospective effect of criminal law.

Source: Guidelines on human rights and the fight against terrorism as adopted by the Committee of Ministers of the Council of Europe on 11 July 2002, available at http://www.coe.int/T/E/Com/Files/Themes/terrorism/CM_Guidelines_20020628.asp

Use of Intelligence Information in Court Proceedings

Provided international law is observed, the exact special powers granted to a security or intelligence agency have to be understood in terms of the normal powers available to law enforcement agencies and the pattern of criminal justice and criminal procedure in the country concerned. Special powers may include telephone tapping, bugging, interception of mail and electronic forms of communication, covert video filming, intrusion into property, vehicles and computer systems. Legal systems differ with regard to the extent to which the use of these techniques contravenes general principles, for example, of property law. Nevertheless, it is generally accepted that concerns over the intrusion to privacy involved in such surveillance requires them to be grounded in law and subject to controls over their use.

In some countries, such as Germany, evidence from security agencies is given in legal proceedings, whereas in others they play a purely supporting role in any legal investigation. In some systems, for example Ireland and Spain, specially constituted courts or tribunals deal with issues involving alleged terrorism in which intelligence may be given. Similarly, even in the field of criminal investigation there are important variations between countries that use an investigating judge, or an independent prosecutor, whether a trial is inquisitorial or adversarial over the treatment of evidence.

These significant variations make it unrealistic to attempt to prescribe a common approach in any detail to many oversight issues involving special powers. The concern of these recommendations is with oversight and not with detailed operational control or detailed human rights standards. Our comments about a minimally acceptable approach are therefore restricted to a high level, concerning the rule of law and proportionality.

Oversight of Special Powers

Helpful practical guidance on what this means in relation to one area of importance – surveillance – was given by the McDonald Commission (the Commission of inquiry into abuses by the Royal Canadian Mounted Police) which reported in 1980. To ensure the protection of privacy from intrusive surveillance, the McDonald Commission proposed the following four general principles:

- that the rule of law should be strictly observed;
- investigative techniques should be proportionate to the security threat under investigation and weighed against the possible damage to civil liberties and democratic structures;
- less intrusive alternatives should be used wherever possible; and
- control of discretion should be layered so that the greater the invasion of privacy, the higher the level of necessary authorisation.[8]

A fifth point should be added to the McDonald Commission principles: legislation governing exceptional powers should be comprehensive. If the law covers only some of the available techniques of information-gathering there will be an in-built temptation

for an agency to resort to less regulated methods (for instance those that do not require approval outside the agency itself). This also reinforces the importance of the McDonald Commission's third principle. Examples of comprehensive legislation can be found for instance in Germany, the Netherlands and the UK.[9] It is noteworthy that the latter cover not only surveillance but also the gathering of information through human sources.

Nevertheless, the McDonald Commission principles provide a useful framework for discussing oversight under the headings of: the rule of law; proportionality; and controls against misuse of special powers.

First, the rule of law. It is a requirement of the rule of law that particular powers that the security services exercise must be grounded in law. Specific legal authority is necessary therefore, for example, for telephone tapping or bugging. It is highly desirable that legislation should be clear, for example, on the grounds for using special powers, the persons who may be targeted, the exact means that may be employed, and the period for which they may be used. Some of these matters may be specified in a warrant or other authority, but it is important that specific instructions should be given.

Box No. 14:

Cases of the European Court of Human Rights on the Right to Privacy

In a series of cases under Article 8 of the ECHR, the European Court of Human Rights has affirmed the need for a clear legal basis for exceptional powers such as phone tapping, interception of private communications systems and bugging. Moreover, the Court has applied to these powers a 'quality of law' test which focuses on the clarity, foreseeability and accessibility of the legal regime (See also Box No. 5). Legislation governing telephone tapping has failed this test where it does not indicate with reasonable clarity the extent of discretion conferred on the authorities, especially concerning whose telephone could be tapped, for what alleged offences and for how long, and did not deal with the destruction of recordings and transcripts. Similarly, legally privileged communications between a lawyer and his or her client require better protection from interception than a decision about recording them being simply delegated to a junior clerk. Although these decisions relate to the standards under one international human rights treaty which is not universally applicable, nevertheless they are useful indicators of a rigorous legality-based approach to the use of exceptional powers.

Sources: *Harman and Hewitt v UK* (1992) 14 EHRR 657; *Tsavachadis v Greece*, Appl. No. 28802/95, (1999) 27 EHRR CD 27; *Malone v UK* (1984) 7 EHRR 14; *Khan v UK,* May 12, 2000, European Ct HR (2000);BHRC 310; *P G; J.H. v UK*, European Court of Human Rights, 25 Sept. 2001, ECtHR Third Section; *Leander v Sweden* (1987) 9 E.H.R.R. 433.

The second important principle – proportionality – also applies under the European Convention on Human Rights to special powers (eg surveillance); information gathering; and to legal privileges and exemptions for security and intelligence agencies. The Court of Human Rights has consequently applied this test to consider whether laws permitting telephone tapping for reasons of national security were

necessary in the interests of democratic society under Art. 8 ECHR.[10] In so doing it has considered the range of institutional safeguards for authorisation and review of these powers in several countries. The same approach has been applied to legislation permitting the opening and retention of security files.[11]

Thirdly, it is important that there should be controls against the misuse of exceptional powers. Such controls might concern the process for authorising use of special powers, the period for which they can be authorised, the use that may be made of any material obtained, and remedies for people claiming abuse of these powers (see Chapter 21). Controls may operate either before or after the use of the powers, as the following examples show.

Prior to surveillance or information-gathering many systems require the authorisation of a person external to the agency. This may be a judge (as in Bosnia and Herzegovina, Estonia, Canada) or a court (for example in the Netherlands under the Intelligence and Security Services Act or the US under the Foreign Intelligence Surveillance Act) or a minister (eg UK). In the latter case, because a minister is part of the executive, it is important that proper controls against political abuse exist. In this regard it is noteworthy that the German legislation requires that the minister approves the use of special powers and that the minister must report them to the parliamentary committee on intelligence oversight.[12]

Controls after the event may include laws governing what (for example, tapes, photographs, transcripts) can be retained (and for how long) and who it can be disclosed to and for what purposes. Depending on the legal system in question, material obtained or retained in breach of this regime may be inadmissible. Even where this is the case, however, it can only be regarded as a control where prosecution is likely to result from the gathering of information in the first place.

Best Practice

- ✓ It is a requirement of the rule of law that any special powers that the security or intelligence services possess or exercise must be grounded in legislation.
- ✓ The law should be clear, specific and also comprehensive, so that there is no incentive for an agency to resort to less regulated means;
- ✓ The principle of proportionality should be embedded in legislation governing the use and oversight of special powers;
- ✓ There should be controls against the misuse of special powers involving persons outside the agency, both before and after their use;
- ✓ All actions taken by security and intelligence services to fight terrorism should respect human rights and the principle of the rule of law. Whatever the acts of a person suspected or convicted of terrorist activities, intelligence services may never derogate from the right to life as guaranteed by the ECHR and the International Covenant of Civil and Political Rights (ICCPR);
- ✓ In order to safeguard against arbitrary use of special powers and violations of human rights, the agency's actions must be subject to appropriate supervision and review.

Chapter 7

Information and Files

Plainly, much of the work of security and intelligence agencies involves holding information (some of it personal) about the actions and intentions of individuals. Individuals may justifiably be of concern to an agency for reasons connected with terrorism, sabotage of key infrastructure or espionage. Apart from detecting or countering these activities per se, personal information may be held for the purposes of security clearance, especially in the case of access to posts of national importance.

Nevertheless, there are clear dangers associated with the creation, maintenance, and use of files containing collected personal data. These are: the risk of over-inclusiveness (that information is gathered because it *may* be useful, rather than for a defined purpose), that the information held is false, unsubstantiated or misleading, that it may be disclosed inappropriately (that is to the wrong people or for incorrect purposes) and that the opportunities or careers of individuals may be affected adversely with no opportunity to correct matters.

Dangers of these kinds have led to the setting of international standards for the holding of personal data. One example is the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985. This has the purpose 'to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him' (Article 1). As an example of national regulations, consider a recent Dutch legislation (see Box No. 15 overleaf).

The European Court of Human Rights treats the storing by a public authority of information relating to an individual's private life, the use of it, and the refusal to allow an opportunity for it to be refuted, as amounting to an interference with the right to respect for private life in Article 8 (1) of the ECHR. The Court's case-law requires there to be a domestic legal basis for the storage and use of information and that, in order to comply with the 'quality of law' test, the law should be accessible to the person concerned and foreseeable as to its effects (ie formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct).[13]

Box No. 15:
Right to inspection of information (The Netherlands)

Article 47 – Right to inspection of personal data

1. The relevant Minister will inform anyone at his request as soon as possible but at the latest within three months whether, and if so which, personal data relating to this person have been processed by or on behalf of a service. The relevant Minister may adjourn his decision for four weeks at the most. A motivated written notification of the adjournment will be made to the person who has made the request before the expiration of the first term.
2. In so far as a request referred to in the first paragraph is conceded to, the relevant Minister will as soon as possible but no later than four weeks following the notification of his decision, give the person who has made the request the opportunity to inspect the information concerning him.
3. The relevant Minister will ensure that the identity of the person making the request is properly established.

Article 51 – Right to inspection of information other than personal data

1. The relevant Minister will inform anyone at his request as soon as possible but at the latest within three months whether information other than the personal data concerning the administrative matter referred to in the request, can be inspected. The relevant Minister may adjourn his decision for a maximum of four weeks. The person making the request will receive a reasoned notification of the adjournment in writing before the expiration of the first term.
2. In so far as a request referred to in the first paragraph is complied with the relevant Minister will provide the person making the request with the relevant information as soon as possible but no later than within four weeks after the notification of his decision.

Source: Intelligence and Security Services Act 2002, Articles 47, 51, The Netherlands, (Unofficial translation).

Best Practice

- ✓ The legislative mandate of the security and intelligence agencies should limit the purposes and circumstances in which information may be gathered and files opened in respect of individuals to the lawful purposes of the agency;
- ✓ The law should also provide for effective controls on how long information may be retained, the use to which it may be put, and who may have access to it and shall ensure compliance with international data protection principles in the handling of disposal information. There should be audit processes including external independent personnel to ensure that such guidelines are adhered to;
- ✓ Security and intelligence agencies should not be exempted from domestic freedom of information and access to files legislation. Instead they should be permitted, where relevant, to take advantage of specific exceptions to disclosure principles referring to a limited concept of national security and related to the agency's mandate;[14]

- ✓ The courts or whatever other independent mechanism is provided under the legislation should be free to determine, with appropriate access to sufficient data from the agency's files, that such exceptions have been correctly applied in any case brought by an individual complainant;
- ✓ Where information is received from an overseas or international agency, it should be held subject both to the controls applicable in the country of origin and those standards which apply under domestic law;
- ✓ Information should only be disclosed to foreign security services or armed forces or to an international agency if they undertake to hold, and use it subject to the same controls as apply in domestic law to the agency which is disclosing it (in addition to the laws that apply to the agency receiving it).

Chapter 8

Internal Direction and Control of the Agency

This chapter focuses on essential safeguards within an agency to ensure legality and propriety. Inevitably it is impossible to spell out in legislation every matter of detail concerning the operation of a security and intelligence agency. Moreover it may be undesirable to do so where this would give public notice of sensitive operational techniques. It is nonetheless important that these details have a basis in law, be standardised to prevent abuse, and that oversight bodies should have access to the relevant administrative rules.

Reporting on Illegal Action

The most reliable information about illegal action by a security or intelligence agency is likely to come from within the agency itself. Hence, a duty to report illegal action and to correct it is useful and also strengthens the position of staff within the agency in raising concerns that they may have about illegality. For example, the US Department of Defense has created an internal channel for the reporting of questionable or improper intelligence activities to the Assistant Secretary of Defense (Intelligence Oversight) and the General Counsel, who are responsible for informing the Secretary and Deputy Secretary of Defense.[15]

The same is true of so-called whistle-blower provisions, which give protection from legal reprisals to such persons when they raise issues of this kind with the appropriate oversight bodies. The following example from Bosnia and Herzegovina demonstrates how this can be regulated in the law on security and intelligence services.

Box No. 16:
Reporting on Illegal Action Provisions in the Bosnian Law on the Security and Intelligence Agencies

Article 41
Should an employee believe that s/he has received an illegal order, s/he shall draw the attention of the issuer of the order to his/her concerns with respect to its illegality. In cases where the issuer of the order repeats the order, the employee shall request a written confirmation of such order. If the employee continues to have reservations, s/he shall forward the order to the immediate superior of the issuer of the order and report the matter to the Inspector General. The employee may refuse to carry it out.

Source: Bosnian Law on the Intelligence and Security Agency.

Equally, of course staff should be made explicitly accountable for acting illegally (including following illegal orders). In hierarchical and bureaucratic bodies employment disciplinary sanctions are sometimes more visible and effective than external criminal liability.[16]

Additionally, and by way of reciprocity, staff should be protected in reporting illegality, from both disciplinary action and criminal prosecution. A detailed illustration of a public interest defence to criminal liability for unauthorised disclosure protection can be found in section 15 (4) of the Canadian Security of Information Act 2003. In the case of disclosures about criminal offences where the public interest in the disclosure outweighs the public interest in non-disclosure (see Box No. 17) provided that an unsuccessful attempt has first been made to raise the issue through internal channels with the deputy minister and with the relevant oversight bodies.[17]

Box No. 17:
Disclosure Protection Rules (Canada)

In deciding whether the public interest in the disclosure outweighs the public interest in non-disclosure, a judge or court must consider:

a. whether the extent of the disclosure is no more than is reasonably necessary to disclose the alleged offence or prevent the commission or continuation of the alleged offence, as the case may be;
b. the seriousness of the alleged offence;
c. whether the person resorted to other reasonably accessible alternatives before making the disclosure and, in doing so, whether the person complied with any relevant guidelines, policies or laws that applied to the person;
d. whether the person had reasonable grounds to believe that the disclosure would be in the public interest;
e. the public interest intended to be served by the disclosure;
f. the extent of the harm or risk of harm created by the disclosure; and
g. the existence of exigent circumstances justifying the disclosure.

Source: Canada, Security of Information Act (1985), s. 15 (4).

Professional Code of Ethics for Security and Intelligence Services

Many professional groups where high risks and interests are at stake possess a code based on their professional ethos – a collection of behavioural rules deemed necessary to perform the respective jobs in a just and morally satisfactory manner. To devise a professional code of ethics, and to offer training courses for intelligence staffers, is a useful means to set, communicate and maintain a minimum level of shared practices among intelligence employees. For example, in the US, the Assistant to the Secretary of Defense (Intelligence Oversight) is tasked with, among others, the institutionalisation of the orientation, awareness and training of all intelligence personnel in intelligence oversight concepts (e.g. upholding the rule of law, protection of statutory and constitutional rights of US persons).[18]

The Republic of South Africa opted for a codified code of conduct for intelligence workers that gives clear guidance to workers on the ethical scope of their activities. (See Box No. 18 below).

Box No. 18:

South African Code of Conduct for Intelligence Employees

The following Code of Conduct was proposed in the 1994 White Paper on intelligence and applies equally to every employee of South African intelligence services.
The Code of Conduct makes provision for *inter alia*:

- a declaration of loyalty to the State and the Constitution;
- obedience to the laws of the country and subordination to the rule of law;
- compliance with democratic values such as respect for human rights;
- submission to an oath of secrecy;
- adherence to the principle of political neutrality;
- a commitment to the highest degree of integrity, objectivity and unbiased evaluation of information;
- a commitment to the promotion of mutual trust between policy-makers and intelligence professionals.

Under a democratic government, those agencies entrusted with the task of intelligence work should agree to execute their tasks in the following manner:

- they should accept as primary, the authority of the democratic institutions of society, and those constitutional bodies mandated by society to participate in and/or monitor the determination of intelligence priorities;
- they should accept that no changes will be made to the doctrines, structures and procedures of the national security framework unless approved of by the people and their representative bodies; and
- they should bind themselves to the contract entered into with the electorate through a mutually agreed set of norms and code of conduct.

Source: Republic of South Africa, White Paper on Intelligence (October 1994), Annex A.

Arguably, adherence to a professional ethos is crucially important at the internal administrative level. It also important that there should be detailed legal framework to guide the work of individual officers. This has two major advantages. First it ensures that discretionary decisions are taken in a structured and consistent fashion across the agency. Secondly, it allows for the legal regulation of operationally sensitive techniques where it would be against the public interest for them to be specified in detail in publicly accessible legislation. Box 19 (overleaf) shows the type of issues that might be regulated in this way.

Box No. 19:

Bosnia and Herzegovina's Law on the Intelligence and Security Agency

Article 27

The Director-General shall be responsible for issuing, *inter alia*, the following Rule Books, regulations and instructions:

a. Code of Ethics
b. Data Security Plan
c. Book of Rules on Classification and Declassification of Data
d. Book of Rules on the Security Clearance Procedure
e. Book of Rules on the Safeguarding of Secret Data and Data Storage
f. Regulations on Dissemination of Data
g. Book of Rules on the Recruitment, Handling and Payment of Informants
h. Book of Rules on the Application, Use and Engagement of Special and Technical Operational Means
i. Book of Rules on Use of Firearms
j. Book of Rules on Work
k. Book of Rules on Salaries
l. Book of Rules on Internal Security
m. Book of Rules on Disciplinary Procedure
n. Book of Rules on Employment Abroad
o. Book of Rules on Basic and General Vocations of Employees of the Agency
p. Book of Rules on Cooperation with Bodies and Institutions in Bosnia and Herzegovina
q. Book of Rules on the Conclusion of Memoranda of Understanding with Bodies and Institutions in Bosnia and Herzegovina
r. Book of Rules on Cooperation with International Bodies and Intelligence Exchange
s. Book of Rules on Liaison Officers
t. Book of Rules on Identification Cards.

Source: Bosnian Law on the Intelligence and Security Agency, 2004

Best Practice

- ✓ Intelligence services should not be beyond the law. Therefore staff who suspect or become aware of illegal actions and orders within the services should be under a duty to report their suspicions;
- ✓ A codified practice should be in place which guarantees appropriate support and security for whistleblowers;
- ✓ Intelligence Services staff should be trained to a code of conduct which includes consideration of the ethical boundaries to their work. This training should be kept up to date and available to staff throughout their tenure;
- ✓ Internal administrative policies should be formalised with a clear legal status.
- ✓ Matters too detailed or sensitive to appear in legislation should be governed by formal internal administrative policies with a clear legal status.

Endnotes Section II – The Agency

1. On the differences between the two see the essays of Brodeur, J.-P., Gill, P. in: Brodeur, J.P, Gill, P., Töllborg, D., *Democracy, Law and Security: Internal Security Services in Contemporary Europe*, (Aldershot: Ashgate, 2003).
2. Council of Europe, *Crime Analysis: Organised Crime - Best Practice Survey No. 4*, (Strasbourg: CoE, 2002), p. 6.
3. 'Each country has to determine whether the actions with which it is concerned are on such a scale or of such significance as to amount to a threat to the national security of the State, bearing in mind that the security of the State is not the same thing as the continuance in power of a particular government.' Council of Europe, Experts Report: European Committee on Crime Problems (CDPC), Group of Specialists on Internal Security Services (PC-S-SEC), Addendum IV, *Final Activity Report,* 40703, para. 3.2.
4. eg in the UK, see Security Service Act 1996, s. 1, referring to a secondary role to 'support of the activities of police forces and other law enforcement agencies in the prevention and detection of serious crime'.
5. Council of Europe, Experts Report, para. 3.2.
6. Intelligence Services Act 2001 (Cth), s. 15.
7. Act Governing the Supervision of the Police and Intelligence Services, 1991, Art. 17.
8. Commission of Enquiry into Certain Actions of the RCMP, *Freedom and Security under the Law*, (Otttawa, 1980), Vol. 1, pp. 513 ff.
9. German *Sicherheitsüberprüfungsgesetz* 1994, Dutch Intelligence and Security Services Act 2002*;* UK Regulation of Investigatory Powers Act 2000.
10. *Klass v FRG*, (1979) 2 EHRR 214; *Mersch v Luxembourg*, (1985) 43 D and R 34.
11. *Leander v Sweden* (1987) 9 E.H.R.R. 433; *Esbester v UK* App. No. 18601/91, 2 April 1993.
12. German *Bundesverfassungsschutzgesetz*, 1990, § 9 (3) 2.
13. In *Rotaru v Rumania*, Appl. No. 28341/95, 4 May 2000 the Strasbourg Court held that the law on security files was insufficiently clear as regards grounds and procedures, since it did not lay down procedures with regard to the age of files, the uses to which they could be put, the persons entitled to consult them, the form the files were to take, or establish any mechanism for monitoring them. See also *Leander v Sweden* (1987) 9 E.H.R.R. 433, holding that in order to be 'in accordance with law' the interference with privacy must be foreseeable and authorised in terms accessible to the individual. In the context of security vetting this did not require that the applicant should be able to predict the process entirely (or it would be easy to circumvent), but rather that the authorising law should be sufficiently clear to give a general indication of the practice, which it was.
14. For discussion of the operation of such exemptions in Canada see: Leigh, I., 'Legal Access to Security Files: the Canadian Experience', *Intelligence and National Security*, Vol. 12:2, (1997), pp. 126-153.
15. Further information available at: <http://www.pentagon.mil/atsdio/mission.html>.
16. See e.g. Intelligence Law of Bosnia and Herzegovina, Article 59. Employees may be held accountable for violations of official duty as set forth in this Law. Violation of official duties shall be understood to mean: a) undertaking actions defined as a criminal offence against official duty, or other serious or minor offences which are harmful to the reputation of the Agency; b) disclosure of a State, military or official secret in contravention of applicable legislation and regulations; c) abuse of official position or exceeding authority; d) failure to execute a legal order of a direct superior; e) undertaking actions which may impede or prevent citizens or other persons from realising their rights pursuant to this and other relevant law; f) causing substantial material damage in the course of his/her work, intentionally or through extreme negligence; g) unexcused absence from work; h) failure to execute entrusted tasks and duties in a timely and proper manner; and i) violation of the

Code of Ethics Disciplinary responsibility under this Article shall not be understood as precluding criminal liability, where applicable. The procedure for determining disciplinary responsibility shall be specified in a Book of Rules issued by the Director-General.

17. Section 15.5 of the Canadian Security of Information Act 2003.
18. Further information available at : <http://www.pentagon.mil/atsdio/faq.html>.

Section III

The Role of the Executive

Chapter 9

The Case for Executive Control

In modern states the security and intelligence services play a vital role in serving and supporting government in its domestic, defence and foreign policy by supplying and analysing relevant intelligence and countering specified threats. This is equally true of domestic security (especially counter-terrorism, counter-espionage and countering threats to the democratic nature of the state) and in the realm of international relations, diplomacy and defence. It is essential, however, that the agencies and officials who carry out these roles be under democratic control through elected politicians, rather than accountable only to themselves; it is elected politicians who are the visible custodians of public office in a democracy.

The ultimate authority and legitimacy of intelligence agencies rests upon legislative approval of their powers, operations and expenditure. However, for practical reasons and because of the sensitive nature of the subject matter, effective external control of these agencies must rest with the government – the executive. There is no inherent conflict between effective executive control and parliamentary oversight (See Section IV). Quite the contrary: effective parliamentary oversight *depends* on effective control of the agencies by ministers. Parliaments can only reliably call ministers to account for the actions of the intelligence agencies if 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 legislative bodies can effectively review the use of powers and expenditure *ex post facto*, but they are not inherently well-equipped to direct and manage these matters, whereas governmental structures are.

Within a healthy constitutional order ministers need both powers, a sufficient degree of control over intelligence agencies and the right to demand information from them, in order to discharge their responsibilities as members of an elected executive acting on behalf of the public. Ministers are entitled to expect unswerving loyalty from the agencies in implementing the policies of the government in the nation's interests. They also need to have adequate control and information to be able to account to Parliament for the agencies' use of their legal powers and their expenditure.

Effective control by the executive does not, however, suggest direct managerial responsibility for security and intelligence operations. Both to prevent abuse and as a prerequisite of effective control, the respective competences of the responsible ministers and the agency heads should be set out in legal provisions. In the interests 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 whole oversight scheme will be weakened. The precise line between the respective functions of ministers and the agency heads is difficult to

chart. One useful model, however, is expressed in the Canadian Security Intelligence Service Act 1984. It refers to the Director of the Service having 'the *control and management* of the Service' that is '*under the direction'* of the Minister.[1] The Polish intelligence legislation contains a noteworthy provision that clearly distinguishes between the respective competences of the Prime Minister and the Heads of the Agencies (see Box No. 20 below).

Box No. 20:

The Delineation of Competences Between the Minister and the Director of Service (Poland)

Article 7:

- The Prime Minister shall define the directions of the Agencies' activities by means of instructions.
- The Heads of the Agencies, not later than three months before the end of each calendar year, each within his competence, shall present the Prime Minister with plans of action for the next year.
- The Heads of the Agencies, each within his competence, every year, before 31st January, shall present the Prime Minister with the reports of the Agencies' activity in the previous calendar year.

Source: The Internal Security Agency and Foreign Intelligence Agency Act 2002, Poland.

The Dutch intelligence legislation also deserves closer inspection. It demands that 'the services and the coordinator exercise their duties in accordance with the law and in subordination to the relevant Minister'.[2] In so doing, this provision places special emphasis on the necessity to work in 'accordance with the law' which also constrains the leadership of the Minister.

Transitional societies, wherein the line between civilian government and the military has been blurred, may find it necessary to provide detailed prohibitions to prevent future abuses. For instance, in the new Bosnia-Herzegovina legislation, while the Chair of the Council of Ministers has a number of detailed policy and review functions,[3] under Article 10 he or she is expressly prevented from assuming 'in whole or in part' 'the rights and responsibilities' of the Director-General or Deputy Director-General.[4]

The same law also spells out the Director-General's rights and responsibilities in a way that makes clear their day-to-day managerial character. The tasks include among others preparation of the annual budget of the agency, the directing of analytical, technical, administrative and partnership cooperation operations, and the external operations of the agency. It also lists the protecting of intelligence sources, intentions and operations from unauthorised disclosure as well as obtaining, through the Chair, approval and support from the Minister of Foreign Affairs for activities that may have a serious impact on the foreign policy of Bosnia and Herzegovina.[5]

Chapter 10

Ministerial Knowledge and the Control of Intelligence

Effective democratic control and policy support depends on a two-way process of access between ministers and officials. Ministers need access to relevant information in the hands of the agency or to assessments based upon it and need to be in a position to give a public account, where necessary, of the actions of the security sector. Conversely, officials have to be able to brief government ministers on matters of extreme sensitivity. It is thus important that ministers have an open door policy towards the agencies.

Legislation 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. It is preferable that various mechanisms be explicit in legislation and be backed by appropriate legal duties. This is not because it is desirable that daily relations between the agencies and ministers should be handled legalistically. Rather, a legal framework in which the respective powers and responsibilities are clear may of itself help to deter abuses and encourage a responsive and frank working relationship.

The following issues need to be specified in legislation (See Box No. 21). On the ministerial side, intelligence laws should pronounce upon the allocation of responsibility for formulating policy on security and intelligence matters (within, of course, the legislative mandate of the agencies); a right to receive reports from the agencies; a reservation of the right to approve matters of political sensitivity (for example, cooperation with agencies from other countries)[6] or activities that affect fundamental rights (such as the approval of the use of special powers, whether or not additional external approval is required, for instance, from a judge).[7] On the agency side, the following corresponding duties should be codified: the duty to implement government policy; the duty to report to ministers as well as the duty to seek approval of specified sensitive matters. The following box contrasts the rights of the minister with the corresponding duties of the agencies.

The precise mechanisms for executive control may include the stipulation that directions be given in writing, the formulation of written policies or targets to guide agency priorities, a right to be briefed, the requirement that sensitive matters be approved specifically by ministers, processes of budgetary approval, and regular reporting and audit.

Box No. 21:

Rights of the Minister	Responsibilities of the Agency
✓ the ministerial responsibility for formulating policy on security and intelligence matters; ✓ the ministerial right to receive reports from the agencies; ✓ a reservation of the right to approve matters of political sensitivity (such as cooperation with agencies from other countries) or undertakings that affect fundamental rights (approval of the use of special powers, whether or not additional external approval is required, for instance, from a judge).	✓ the duty to implement government policy; ✓ the duty to report to ministers; ✓ the duty to seek approval of specified sensitive matters.

Canadian legislation lists, for example, the situations in which the Director of the Canadian Security Intelligence Service is required to consult externally with the Deputy Minister (ie the chief departmental official). This is the case when the Director is confronted with decision-making that touches upon the 'the general operational policies of the Service', where the Minister has required consultation under written directions, and before applying for a judicial warrant to authorise surveillance (See Box No. 22 below).

Box No. 22:
Consultation of the Director with the (Deputy) Minister

Section 7.
1. The director shall consult the Deputy Minister on the general operational policies of the Service.
2. The Director or any employee designated by the Minister for the purpose of applying for a warrant under section 21 or 23 shall consult the Deputy Minister before applying for the warrant or the renewal of the warrant.

Source: Canadian Security Intelligence Service Act 1984, Sections 7(1) and (2).

In many countries, the minister is often aided in the task of control by an Inspector-General – an institution most often established by law and endowed with various rights and responsibilities *vis-à-vis* both the executive and the parliament (for more information on the Inspector-General, please consult Section V on the Role of External Review Bodies). In this context, the Inspector-General monitors whether the government's intelligence policies are appropriately implemented by the services.

It is evident that the rights of the executive ought to be counter-balanced to prevent misuse by the executive of the agencies. Various forms of safeguards may be used for this purpose and will be discussed in detail in Chapter 13.

Best Practice

- ✓ Intelligence legislation should contain two distinct rights of access: the right of the executive to relevant information in the hands of the agency and the right of the agency heads to have access to the respective minister;
- ✓ The Minister should be legally responsible for the formulation of policy on security and intelligence matters. He should also be legally entitled to receive agency reports at regular intervals as well as being legally responsible for the approval of matters of political sensitivity.

Chapter 11

Control over Covert Action

Covert action refers to intervention or measures taken by an intelligence agency in the territory or affairs of another country which is unacknowledged. For instance, the US Executive Order 12333, defines the term 'special activities' as follows (see Box No. 23 below):

Box No. 23:
Covert Action Defined (US)

'Special activities means activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence United States political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions.'[8]

Source: US Executive Order 12333, 1981, paragraph 3.4(h).

Covert action raises issues of accountability for at least two reasons. Firstly, since this type of action is secretive it will be difficult for the legislature to control (even if legislators are aware of it). Nevertheless, there is a legitimate parliamentary interest in action taken by the state's employees and using public money. Secondly, there is an ethical dimension. Historically, a number of covert action programmes have involved controversial strategies and techniques. The fact that these are covert and usually illegal according to the law of the state in whose territory they take place makes the temptation to abuse perhaps all the greater. It is therefore all the more important that elected politicians set ground-rules for what is acceptable (for instance, compliance with international human rights law) and are responsible for authorising covert action.

There are few legal precedents to draw on here. One of the few explicit models of this kind is for ministerial authorisation in UK law which, when given, amounts to a statutory defence in UK law for acts committed abroad by the intelligence agencies which breach civil or criminal law (see Box No. 24).

Reflection on two issues that this scheme does not address is instructive. Firstly, there is no legal requirement to obtain ministerial authorisation whenever such acts are committed. A second shortcoming concerns legality. For obvious reasons the state may seek exemption in its own legal system from extra-territorial liability for covert action and, equally obviously, these actions will be in breach of the legal system within which they are committed. Nevertheless, there is a realm of legality which should not be by-passed or ignored – namely international human rights law.

Box No. 24:
Authorisation of Covert Action Abroad (UK)

7(1) If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section (…)
7(3) The Secretary of State shall not give an authorisation under this section unless he is satisfied:
a. that any acts which may be done in reliance on the authorisation or, as the case may be, the operation in the course of which the acts may be done will be necessary for the proper discharge of a function of the Intelligence Service; and
b. that there are satisfactory arrangements in force to secure:
i. that nothing will be done in reliance on the authorisation beyond what is necessary for the proper discharge of a function of the Intelligence Service; and
ii. that, in so far as any acts may be done in reliance on the authorisation, their nature and likely consequences will be reasonable, having regard to the purposes for which they are carried out; and
c. that there are satisfactory arrangements in force under section 2(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained by virtue of anything done in reliance on the authorisation will be subject to those arrangements.

Source: Intelligence Services Act, United Kingdom, 1994, Section 7.

The legal rights and obligations that stem from this body of law are deemed universally applicable, ie their applicability does not alter with a change in domestic settings. International human rights law depicts a body of universal legal guarantees protecting individuals and groups against actions by governments that interfere with fundamental freedoms and human dignity.[9] It is becoming increasingly clear, especially in the case of the ECHR, that states may be liable not only for human rights abuses committed in their own territory, but also in other areas where they exercise jurisdiction, or where the abuse follows from or is a result of acts of their officials, wherever these take place.

As part of the growing body of international human rights law, the International Covenant on Civil and Political Rights (ICCPR)[10] as well as the Convention against Torture and other cruel inhumane and other degrading treatment or punishment (CAT)[11] should be particularly emphasised when it comes to the conduct of covert actions by intelligence services. In particular it is the right to life (Art. 6, ICCPR), the right not to be subjected to torture or to cruel, inhuman or degrading treatment or punishment (Art. 7, ICCPR) as well as the right to liberty and security of person (Art. 9, ICCPR) that could be infringed by covert intelligence action. Two illegal practices should be named that directly relate to the aforementioned, namely extra-judicial killing and torture/degrading treatment.

Whatever the goal and the perceived credibility of a covert action, extra-judicial killing such as the assassination of an enemy by intelligence agents (abroad) are a clear violation of the right to life expressed in the ICCPR. As the right to life is granted to

any human being qua being human, derogations may not be made (Art. 4 (2) ICCPR). At the time of writing, 152 states are parties to this treaty.[12]

The other illegal practice traditionally linked to covert actions concerns interrogation techniques that amount to a violation of the right not to be subjected to torture or degrading treatment (Art. 7, ICCPR).

Box No. 25:
Torture

Article 1 of the Torture Convention defines the crime of torture as follows:
'For the purposes of this Convention, the term 'torture' means any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidation of any kind, when such pain or suffering is inflicted by or at the instigation of a public official or other person acting in an official capacity. It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions'.

Source: The Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, G.A. Res 39/46, 39 U.N. G.A.O.R. Supp. (No. 51) at 197, U.N. Doc. A/39/51 (1984), *entered into force* 26 June 1986.

Examples of interrogation techniques that violate this right have been provided in a famous judgement of the European Court of Human Rights. The court listed:

- *wall-standing*: forcing the detainees to remain for periods of some hours in a 'stress position', described by those who underwent it as being 'spread eagled against the wall, with their fingers put high above the head against the wall, the legs spread apart and the feet back, causing them to stand on their toes with the weight of the body mainly on the fingers';
- *hooding*: putting a black or navy coloured bag over the detainees' heads and, at least initially, keeping it there all the time except during interrogation;
- *subjection to noise*: pending their interrogations, holding the detainees in a room where there was a continuous loud and hissing noise;
- *deprivation of sleep*: pending their interrogations, depriving the detainees of sleep; and
- *deprivation of food and drink*: subjecting the detainees to a reduced diet during their stay at the centre and pending interrogations.[13]

The use for legal purposes of information elicited by torture is clearly prohibited in international law (see Chapter 12).

Normally there are higher standards of legality for domestic operations compared with operations abroad. Irrespective of this, the executive plays a crucial rule in monitoring the legality of intelligence services' covert actions – it should *inter alia* monitor the adherence to basic human rights provisions. The following example from the Australian Intelligence Services Act documents well the importance attached to the

involvement of the executive when it comes to controlling covert actions (see Box No. 26 below).

Box No. 26:
Legalising Ministerial Control Over Covert Action (Australia)

Section 6 Functions of ASIS

1. The functions of ASIS are (…) :
   e. to undertake such other activities as the responsible Minister directs relating to the capabilities, intentions or activities of people or organisations outside Australia.
2. The responsible Minister may direct ASIS to undertake activities referred to in paragraph (1)(e) only if the Minister:
   a. has consulted other Ministers who have related responsibilities; and
   b. is satisfied that there are satisfactory arrangements in place to ensure that, in carrying out the direction, nothing will be done beyond what is necessary having regard to the purposes for which the direction is given; and
   c. is satisfied that there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in carrying out the direction will be reasonable having regard to the purposes for which the direction is given.
3. A direction under paragraph (1)(e) must be in writing.

Section 6A Committee to be advised of other activities

If the responsible Minister gives a direction under paragraph 6(1)(e), the Minister must as soon as practicable advise the Committee of the nature of the activity or activities to be undertaken.

Source: Intelligence Services Act, Australia, 2001, Section 6.

Accepting that these operations are against the law of the country where the operation is taking place, safeguards should apply for the acting state's own citizens that might be affected by covert intelligence operations. Exemplary in this regard is Section 15 of the Australia's Intelligence Services Act 2001 which maintains that the Minister responsible for ASIS 'must make written rules regulating the communication and retention by ASIS of intelligence information concerning Australian persons'. In so doing, the Minister 'must have regard to the need to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper performance by [ASIS of its] functions'.[14]

Best Practice

- ✓ All covert action shall be approved by the responsible member of the executive according to a legal framework approved by parliament. Regular reports shall be made;
- ✓ No action shall be taken or approved by any official as part of a covert action programme which would violate international human rights.

Chapter 12

International Cooperation

One area in which it is especially difficult for national ministers or legislatures to exercise scrutiny lies within the work of international/supra-national bodies and bilateral cooperative arrangements.[15] Post 9/11 these arrangements are increasingly important and widely-used. Even where the interests of two nations do not entirely converge, intelligence often supplies the 'quid' for others' 'quo'. Bilateral cooperation normally involves the sharing of intelligence information and analysis on topics of mutual interest. Such bilateral relations can only be maintained and continued if both parties fully and strictly respect the basic agreement underlying their intelligence sharing: that the origin and details of intelligence provided by the partner service will be protected according to its classification and will not be passed on to third parties.

Indeed, cooperation with foreign agencies is a practical necessity, for example, in combating terrorism. Yet this also bears the risk of at best compromising domestic standards of constitutionalism, legality and propriety through unregulated cooperation and, at worst, consciously using cooperative arrangements to circumvent domestic controls on the obtaining of information or for protection of privacy. It is therefore essential that international cooperation of intelligence services should be properly authorised and subject to minimum safeguards. The box below details more concretely the different activities that make up international intelligence cooperation.

Box No. 27:

Various Practices of Intelligence Cooperation: Bilateral Sharing

The most common form of international intelligence cooperation depicts the bilateral sharing of information and analysis on topics of mutual interest. Beyond such bilateral sharing, other, more intimate, or special relations and cooperative arrangements may also exist which can take any of several forms.

- A state may agree to undertake collection and/or analysis in one area and share it in return for the other state's intelligence reciprocating in another area;
- One state may permit another the use of its territory for collection operations in return for sharing the results of such collection;
- A state may help another acquire a collection capability for its own purposes with the understanding that the providing state will be permitted to share the results;
- Joint collection operations may be undertaken with one state's intelligence officers working side-by-side with, or in a complementary manner to, their foreign counterparts;
- Exchanges of analysts or technicians between two states' intelligence services may occur;
- One state may provide training in return for services rendered by another state's intelligence service, whenever a foreign service can bring unique skills to other endeavours.

The importance of bilateral sharing of intelligence information notwithstanding, its 'quid pro quo' rationale has increasingly found a wider application through multilateral forms of intelligence cooperation. Traditionally the precise details of intelligence cooperation have been secret – the most famous example being perhaps the arrangements for sharing signals intelligence between the US, the UK, Australia, Canada and New Zealand which dates from the Second World War and is allegedly based on an unpublished treaty of 1947.[16] Within the European region, for example, the commitment to move a step further to the pooling of sovereignty and to overcome the mere demonstration of political willingness in this regard has been achieved by the creation of the position of a EU Counter-Terrorism coordinator in March 2004.[17] The single most important task of this new institution is to oversee and coordinate the work of the European Council in combating terrorism – thus making sure that multilateral intelligence-sharing decisions will be implemented.

Yet beyond this regional level, the recent US-EU Declaration on Combating Terrorism[18] does also expressly mention the necessity for multilateral sharing of intelligence information as a capacity-building measure to work effectively against the dangers of terrorism (see Box No. 28 below).

Box No. 28:
Multilateral Sharing of Intelligence: A Renewed EU-US Commitment

3.3 We will work together to enhance, in accordance with national legislation, our abilities to share information among intelligence and law enforcement agencies to prevent and disrupt terrorist activities, and to better use sensitive information as allowed by national legislation in aid of prosecutions of terrorists in a manner which protects the information, while ensuring a fair trial.

Source: US - EU Declaration on Combating Terrorism, Signed in Shannon, Ireland, 26 June 2004.

In general, cooperation with foreign agencies should only take place in accordance with arrangements approved by democratically accountable politicians, usually the executive.[19]

The following are examples of situations where effective ministerial control over intelligence cooperation practices is required in order to abide by the principle of accountability.

- **The issue of 'plausible deniability'**

Plausible deniability is a political doctrine developed in the 1950s and involves the creation of power structures and chains of command loose and informal enough to be denied if necessary. The idea is a product of Cold War strategic planning whereby intelligence services could be given controversial instructions by powerful figures in the executive – but that the existence and true source of those instructions could be denied if necessary; if, for example, an operation went disastrously wrong and it was necessary for the administration to disclaim. A possible present-day application of this doctrine can be seen in situations where a government is held to ransom after a national citizen has been kidnapped. In these situations, governments tend to discard

the option to enter into direct negotiations with terrorists for comprehensible political reasons. Yet, they also do not want to be seen as being indifferent to the fate of the kidnapped person. Often some sort of instruction is given to members of the secret service who, on behalf of the government, get in contact with the hostage-takers. In these situations it is important that a balance is struck between the need for secrecy and the need for state officials to be held accountable for their actions.

- **Cooperation with foreign intelligence services whose practices infringe non-derogable human rights**

Although publicly disputed, in exceptional circumstances it might be tempting for intelligence services to obtain information on pressing issues of national security – irrespective of the original method used for obtaining the information. However international law clearly prevents the use, for example in a terrorist prosecution or in deportation proceedings, of statements obtained in another state through torture.[20] Under Article 15 of the UN Convention against Torture, any statement made as a result of torture is inadmissible in evidence in 'any proceedings', except in proceedings against the alleged perpetrator of the torture. This protection is widened in the Geneva Conventions and some other international standards which also exclude statements obtained as a result of other cruel, inhuman or degrading treatment or punishment, as well as torture.[21]

It can be argued, although admittedly international law is not so specific here, that the same considerations apply even to the indirect use of information obtained by another state's security services through torture.

> [B]y 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.[22]

The usage of information obtained as a result of torture ought to be forbidden per se. It violates fundamental human rights. Again, effective ministerial control of intelligence services can provide the necessary safeguard to ensure that this prohibition is respected at all times.

- **Giving information on national citizens to foreign security services**

Legislation should contain clear safeguards against the avoidance of the controls that apply in domestic law through cooperation with foreign agencies. German legislation (see Box No. 29 overleaf) provides an illustration.

Where information is received from an foreign or international agency, it should be held subject both to the controls applicable in the country of origin and those standards which apply under domestic law. Information should only be disclosed to foreign security and intelligence agencies or to an international agency if they undertake to hold and use it subject to the same controls that apply in domestic law to the agency which is disclosing it (in addition to the laws that apply to the agency receiving it).

Box No. 29:
Giving Information on National Citizens to Foreign Security Services: An Example from German Intelligence Legislation

Art. 19 (3)
The Agency may provide foreign security and other appropriate foreign services, as well as supra and international organisations, with data regarding citizens, provided that the supplying of this data is essential for the pursuit of its duties or because prevailing security interests of the receiving institution necessitate this. The supplying of information ceases when this would run counter to the predominant foreign concerns of the Federal Republic of Germany or where the pre-eminent interests of the affected private persons deserve to be protected.
The supplying of data ought to be recorded in public files. The beneficiary is to be instructed that the information is transmitted on the understanding that the data may only be used for the specific purpose for which it was sent. The Agency reserves the right to request information on the usage of data by the beneficiary.
Source: *Bundesverfassungsschutzgesetz* (BVErfSchG), Germany, November 2002, Art. 19 (*Unofficial translation*).

Notice that international cooperation is not limited only to bilateral/multilateral agreements among national intelligence services but can also involve the duty to cooperate with an international tribunal. Reference is made to the International Criminal Tribunal for the Former Yugoslavia (see Box No. 30 below).

Box No. 30:
The Duty of the Bosnian Intelligence Service to Cooperate with the International Criminal Tribunal for the Former Yugoslavia

Article 6
The Agency shall cooperate with the International Criminal Tribunal for the Former Yugoslavia, *inter alia*, by providing information to the Tribunal concerning persons responsible for serious violations of international humanitarian law in the territory of the former Yugoslavia since 1991 (hereinafter: the International Tribunal).
Source: Law on the Intelligence and Security Agency, Bosnia and Herzegovina, 2004, Art. 6.

Best Practice

- ✓ It is essential that international cooperation should be properly authorised by ministers and should be subject to minimum safeguards to ensure compliance with domestic law and international legal obligations;
- ✓ Legal safeguards should be incorporated to prevent the use of intelligence sharing in a way that circumvents non-derogable human rights standards or controls in domestic law.

Chapter 13

Safeguards against Ministerial Abuse

In the previous chapters, it was argued that executive and ministerial control is one of the essential elements of democratic accountability of the security and intelligence services. However, the danger exists that services can become amenable to political abuse by the executive. Not only transition states, but also Western democracies have witnessed political turmoil because ministers have used the security and intelligence services for personal or political motivations, eg instructing the services to wiretap political opponents or using services' assets for commercial interests. Mainly for these reasons it is vital that safeguards should be in place guaranteeing the impartiality and professionalism of the services. In the following discussion, the focus is on institutional safeguards (see also Chapter Eight on the Internal Direction and Control of the Agency).

Despite being a democratic necessity, executive control of the security sector does carry potential disadvantages. Firstly, there is the risk of excessive secrecy, where the government in effect treats information acquired by public servants as its own property; it may, for example, attempt to withhold information about security accountability or procedures which are legitimate matters of public debate, under the guise of 'national security'. Secondly, there is the temptation to use security agencies or their capacities to gather information for the purposes of domestic politics ie to gather information on or to discredit domestic political opponents. Safeguards for officials to refuse unreasonable government instructions (for example, to supply information on domestic political opponents) are therefore highly desirable.

There is a delicate balance between ensuring proper democratic control of the security sector and preventing political manipulation. We have referred in Chapter 5 to the need to give legal safeguards for the agency heads through security of tenure, to set legal limits to what the agencies can be asked to do, and to establish independent mechanisms for raising concerns about abuses. Where staff from security agencies fear improper political manipulation it is vital that they have available procedures with which to raise these concerns outside the organisation. Whistle-blowing or grievance procedures are therefore significant (see Section II, Chapter Eight on Reporting on Illegal Action)

Safeguards

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. The rights of the executive ought to be counter-balanced to prevent misuse by the executive of the agencies. Various forms of safeguards may be used for this purpose. In Canada, Hungary and Australia there is a requirement that

certain ministerial instructions be put in writing (see Hungarian example in Box No. 31 below).

Box No. 31:
Direction and Control of the National Security Services in Hungary

Section 11
1 (b) The Minister shall determine in writing the topical tasks of the services for the directors general semi-annually; shall give orders in writing for meeting the information requirements received from the members of the Government.

Source: Act on the National Security Services 1995, Hungary, Section 11.

Ministerial instructions may also be required to be disclosed outside the agency. The Canadian law, for example, requires them to be given to the Review body[23] and Australian law requires them to be given to the Inspector-General of Intelligence and Security as soon as practicable after the direction is given (see Box No. 32 below).

Box No. 32:
Duties of the Minister vis-à-vis the Agency (Australia)

Section 32B: Minister to give directions and guidelines to Inspector-General
1. This section applies to any guidelines or directions given by the responsible Minister to the head of ASIS or DSD.
2. As soon as practicable after giving to the head of the agency a direction or guideline issued on or after the commencing day, the Minister must give to the Inspector-General a single copy of the direction or guideline.
3. As soon as practicable after the commencing day, the Minister must give to the Inspector-General a single copy of each direction or Guideline that was issued before that day and is still in operation.

Source: Australian Inspector-General of Intelligence and Security Act, 1986, Section 32B.

Within a wider frame of checks and balances, the Australian intelligence legislation features another safeguarding provision, namely the duty of the Director-General to brief the Leader of the Opposition.[24] Notice that this is also established informal practice in other national settings aiming, *inter alia*, at the prevention of ministerial abuse. 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 one operating within a Westminster-style 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.[25]

The following legislative examples from Bosnia and Herzegovina and the United Kingdom are instructive inasmuch as they include clear provisions that the intelligence/security services shall not be amenable to any attempts that try to undermine their impartiality – be it by furthering the interests of certain political parties or by undermining the credibility of legitimate political movements within the country (see Boxes No. 33 and 34 below).

Box No. 33:
Measures to Safeguard the Impartiality of the Agency

A. Example from Bosnian legislation:
Article 39
Employees shall not be members of political parties, take instructions from political parties or perform any remunerative activity or other public or professional duties incompatible with work in the Agency.
Article 56
1. The Agency shall be apolitical, and shall not be involved in furthering, protecting or undermining the interests of any political party, lawful political organisation or any constituent people.
2. The Agency may not investigate acts of protest, advocacy or dissent that are organised and carried out in a lawful manner.

Source: Law on the Intelligence and Security Agency, Bosnia and Herzegovina, 2004.

B. Example from UK legislation:
Section 2 The Director-General
2.— (1) The operations of the Service shall continue to be under the control of a Director-General appointed by the Secretary of State.
(2) The Director-General shall be responsible for the efficiency of the Service and it shall be his duty to ensure—
(a) that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of preventing or detecting serious crime or for the purpose of any criminal proceedings; and
(b) that the Service does not take any action to further the interests of any political party;

Source: Security Service Act, United Kingdom 1989, Section 2.

A third type of safeguard is the aforementioned 'open-door policy' by which the agency head is granted a right of access to prime minister or president. In the United Kingdom, for example, the agency heads of the Security Service, the Secret Intelligence Service and Government Communications Headquarters, although responsible to the Home Secretary and Foreign Secretary respectively, have a right of access to the Prime Minister.[26]

Box No. 34:
The Head of Agency's Right of Access to the Prime Minister (UK)

The Chief of the Intelligence Service shall make an annual report on the work of the Intelligence Service to the Prime Minister and the Secretary of State and may at any time report to either of them on any matter relating to its work

Source Section 2(4), Intelligence Services Act 1994 United Kingdom

Best Practice

- ✓ Intelligence legislation should include safeguards against ministerial abuse and the politicisation of intelligence services. Various possible safeguarding mechanisms are imaginable, such as the requirement that all ministerial instructions be put in writing and/or disclosed to an external review body as well as the ministerial requirement to brief the Leader of the Opposition;
- ✓ Intelligence Services should not take any action to further the interests of a political party;
- ✓ Intelligence Services should not be allowed to investigate acts of protest, advocacy or dissent that are part of the democratic process and in accordance with the law.

Endnotes Section III – The Role of the Executive

1. Intelligence Service Act, Canada, R.S. 1985.
2. Intelligence and Security Services Act 2002, Netherlands, Art. 2.
3. Law on the Intelligence and Security Agency 2004, Bosnia and Herzegovina, Art. 8 and 9.
4. Law on the Intelligence and Security Agency 2004, Bosnia and Herzegovina, Art. 10
5. Law on the Intelligence and Security Agency 2004, Bosnia and Herzegovina, Art. 27.
6. Canadian Security Intelligence Service Act 1984, s. 13.
7. Australian legislation requires the ministers responsible for ASIS [Australian Secret and Intelligence Services], and the responsible Minister in relation to DSD [Defence Signals Directorate, the Department of Defence], to issue written instructions to the agency heads dealing with situations in which the agencies produce intelligence on Australians: the Intelligence Services Act 2001, s. 8(1).
8. The US Executive order asserts a measure of *Presidential* control: 'No agency except the CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress under the War Powers Resolution [87 Stat. 855]) may conduct any special activity unless the President determines that another agency is more likely to achieve a particular objective'.
9. Condé, H. V., *A Handbook of International Human Rights Terminology*, (Lincoln, NE: University of Nebraska Press, 2004), p. 111.
10. UN GA Res. 2200 A (XXI), 21 UN GAOR Supp. (no 16.) at 52, UN Doc. A /6316 (1966), entered into force 23 March 1976.
11. UN GA RS 39/46, 39 GAOR Supp. (no 51) at197, UN Doc. A/39/51 (1985), entered into force 26 June 1987.
12. Office of the United Nations High Commissioner for Human Rights, *Status of Ratification of the Principal International Human Rights Treaties* (as of 09.06.2004), available online at: <http://www.unhchr.ch/pdf/report.pdf>
13. Ireland v. United Kingdom, Judgement, European Court of Human Rights, p. 96, available at: <http://hudoc.echr.coe.int/Hudoc1doc/HEJUD/sift/91.txt>.
14. These rules made by the ministers have been published and are available online at <http://www.asis.gov.au/rules_to_privacy.html>.
15. Note, for example, Art.85 of the Constitution of Bulgaria which requires parliamentary approval for treaties with military or political implications.
16. See Richelson, J., Ball, D., *The Ties That Bind*, (London: Allen & Unwin, 1990).
17. EU Council Declaration on Combating Terrorism, Brussels, 25 March 2004, p. 13. Available online at: <http://www.delrus.cec.eu.int/en/news_561.htm>
18. US-EU Declaration on Combating Terrorism, Signed in Shannon, Ireland in June 2004, available online at: <http://www.whitehouse.gov/news/releases/2004/06/20040626-5.html>
19. See for example Bosnia and Herzegovina law, Article 64 which requires approval from the Chair, before the Agency enters into an arrangement with intelligence and security services of other countries. (Additionally, the Minister for Foreign Affairs must be consulted before an arrangement is entered with an Institution of a foreign State, an international organisation of states or an institution thereof). The Chair is obliged to inform the Intelligence Committee of all such arrangements.
20. See: the Human Rights Committee interpretation of the International Covenant on Civil and Political Rights: ICCPR General comment 20, para. 12, 10 March 1992, supra, note 188; Guideline 16 of the UN Guidelines on the Role of Prosecutors (Adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, September 1990.)
21. Article 99 of the Third Geneva Convention stipulates: 'No moral or physical coercion may be exerted on a prisoner of war in order to induce him to admit himself guilty of the act of

which he is accused'. Article 31 of the Fourth Geneva Convention: 'No physical or moral coercion shall be exercised against protected persons, in particular to obtain information from them or from third parties'.
See also Article 12, Declaration on the Protection of All Persons from Being Subjected to Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; Article 69(7) of the Rome Statute of the International Criminal Court; Principle 27, UN Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment.

22. Lord Justice Neuberger (dissenting) in *A and others v Secretary of State for the Home Departmen*t, Court of Appeal (Civil Division), [2004] EWCA Civ 1123.
23. See, for instance: CSIS Act 1984, s. 6(2), requiring written instruction issued by the Minister to the Director of CSIS to be given to the Security Intelligence Review Committee. In Australia under the Intelligence Services Act 2001, section 8(2), the ministers responsible for ASIS (Australian Secret and Intelligence Services), and the responsible Minister in relation to DSD (Defence Signals Directorate, the Department of Defence), may give written instructions which must be observed by the agency heads.
24. Intelligence Services Act, Australia 2001, Section 19.
25. Note the example of Bosnia and Herzegovina from Article 6 of the new legislation:
'As necessary to fulfil its duties under this Law, the Agency shall keep the following officials and bodies informed of intelligence matters in a timely manner, both upon its own initiative and upon the request of the latter: the Presidency of Bosnia and Herzegovina (collectively) (hereinafter: the Presidency), the Chair of the Council of Ministers, the Minister of Foreign Affairs, the Minister of Security, Minister of Defence, the Presidents, Vice-Presidents and Prime Ministers of the Federation and Republika Srpska, the Ministers of Interior of the Federation and Republika Srpska, the Chair and Deputy Chairs of the House of Representatives of the Parliamentary Assembly of Bosnia and Herzegovina, the Chair and Deputy Chairs of the House of Peoples of the Parliamentary Assembly of Bosnia and Herzegovina, the Speaker and Deputy Speakers of the Republika Srpska National Assembly, and the Chair and Deputy Chairs of the Federation House of Representatives, the Chair and Deputy Chairs of the Federation House of Peoples, as well as the Security-Intelligence Committee of the Parliamentary Assembly of Bosnia and Herzegovina (hereinafter: Security-Intelligence Committee).
26. Security Service Act 1989, s. 2(4); Intelligence Service Act 1994, s. 2(4), 4(4).

Section IV

The Role of Parliament

Chapter 14

The Case for Parliamentary Oversight

Oversight or scrutiny of the security sector cannot remain the preserve of the government alone without inviting potential abuse. It is commonplace, aside from their role in setting the legal framework, for Parliaments to take on the task of scrutinising governmental activity.

In a democracy no area of state activity should be a 'no-go' zone for parliament, including the security and intelligence sector. Parliamentary involvement gives legitimacy and democratic accountability. It can help to ensure that security and intelligence organisations are serving the state as a whole and protecting the constitution, rather than narrower political or sectional interests. Proper control ensures a stable, politically bi-partisan approach to security which is good for the state and the agencies themselves. The involvement of parliamentarians can help ensure that the use of public money in security and intelligence is properly authorised and accounted for.

There are dangers, however, in parliamentary scrutiny. The security sector may be drawn into party political controversy- an immature approach by parliamentarians may lead to sensationalism in public debate, and to wild accusations and conspiracy theories being aired under parliamentary privilege. As a consequence the press and public may form an inaccurate impression and there may develop a corresponding distrust of parliamentarians by security officials. Genuine attempts at openness or leaks of sensitive material to which legislators have been given privileged access may compromise the effectiveness of military or security operations.

Effective scrutiny of security is painstaking and unglamorous work for politicians, conducted almost entirely behind the scenes. Sensitive parliamentary investigations require in effect a parallel secure environment in parliament for witnesses and papers. The preservation of necessary secrecy may create a barrier between the number of parliamentarians involved and the remainder. Those within the ring of secrecy may be envied or distrusted by colleagues because of privileged access to secret material. It is therefore essential that a cross-section who can command widespread trust and public credibility are involved.

That parliamentary oversight of the security and intelligence services is an accepted phenomenon in democratic societies, is illustrated by Box No. 35. It gives an overview of structure and powers of parliamentary oversight of the services in seven selected democracies in the Americas, Europe, and Africa. Most of the elements of this box will be discussed in the following chapters.

Box No. 35: Comparison of the External and Parliamentary Oversight Bodies in Selected Countries

(1) Country	(2) Mandate of Oversight Body	(3) Budget Control Powers of Oversight Body	(4) Type of oversight body; Membership, Clearance, Appointment of Oversight Body	(5) Subpoena powers	(6) Prior notification requests
(A) Argentina	Reviews legality and effectiveness of the services, including citizens' complaints.	Both scrutiny and authorisation powers.	Parliamentary oversight body of 14 MPs as member, appointed by parliament. There is no security vetting.	No.	Not regulated by the law.
(B) Canada	The SIRC checks legality and efficacy of the agency.	SIRC has no authorisation powers, yet can comment on CSIS's budget.	External independent expert oversight body of max. 5 experts as members, appointed by Prime Minister. Members are under oath.	Yes.	No prior notification required.
(C) Norway	The oversight focuses primarily on legality of the services, including human rights protection.	No budget oversight function.	External expert parliamentary oversight body; max. 7 members (non-MPs) but appointed by parliament.	Yes, all persons summoned to appear before the Committee are obliged to do so.	Agencies are forbidden from consulting with the Committee about future operations.
(D) Poland	Overviews, legality, policy, administration and international cooperation of services. Effectiveness is not checked.	Commission scrutinises the services' draft budget and its implementation.	Parliamentary oversight body; max. 9 MPs as members, appointed by parliament. All members undergo security vetting.	No.	No legal duty.
(E) South Africa	Its oversight purview includes legislation, activities, administration, financial management and expenditure of the services.	The committee does not oversee the intelligence services' budgets per se, but its purview includes financial management of the services.	Parliamentary oversight body; committee consists of 15 MPs, appointed by President. Members are vetted.	Yes	No legal duty.
(F) United Kingdom	Finance, administration and policy of MI5, MI6 and GCHQ with a view on efficiency. It does not check legality.	Committee scrutinises the finance together with the Chairman of the Public Accounts Committee but has no authorisation power.	Parliamentary oversight body of 9 members drawn from both Houses of Parliament, appointed by the Prime Minister.	No.	No legal duty.
(G) United States	Reviews all intelligence agencies. Approves top intelligence appointments. It checks both legality and effectiveness of the services.	Both oversight committees possess budget authorisation powers.	Two Congressional oversight committees, consisting of 20 (House) and 17 (Senate) Congressmen, appointed by House and Senate leaders.	Yes, on both committees.	Yes, except in times of acute emergency, in which the agencies can delay reporting for 2 days.

Source: Born, H., Johnson, L.K., Leigh, I. (eds.), *Who's watching the spies? Establishing Intelligence Service Accountability* (Dulles, VA: Potomac Books, Inc., 2005)

Box No. 35 shows the current state of affairs in those seven selected democracies. It has to be emphasised that parliamentary oversight of the security and intelligence services is a recent phenomenon, even in established democracies.[1] The mid-1970s saw the beginning of exposures concerning abuses by security and intelligence agencies in liberal democratic systems which have proved to be a major catalyst for initiating parliamentary oversight across the globe.[2] Following the US, Australia and Canada legislated for intelligence oversight in 1979 and 1984.[3] Having commenced in the Anglo-Saxon world (though reform did not reach the UK until 1989), a wave of reform spread to Europe in the 1980s and 1990s; with reforms in Denmark in 1988, Austria in 1991, Rumania in 1993, Greece in 1994, Norway in 1996, and Italy in 1997.[4] These developments have attracted support from the Parliamentary Assemblies of the Council of Europe and of the Western European Union.[5] Progress outside Europe has been slower, although there are exceptions, as demonstrated by the cases of Argentina and South Africa.

Chapter 15

The Mandate of Parliamentary Oversight Bodies

The international norm is for parliament to establish an oversight body for all the major security and intelligence agencies (a 'functional approach' to oversight), rather than having multiple oversight bodies for specific agencies (an 'institutional' approach). This 'functional' approach facilitates seamless oversight since in reality different parts of the intelligence machinery work closely with each other. There is a risk that an oversight body established on a purely 'institutional' basis may find that its investigations are hampered if they lead in the direction of information supplied by or to an agency outside the legal range of operation.

There are some significant divergences from this approach, however. In the US there are separate congressional intelligence committees in the House of Representatives and the Senate, each with legal oversight of the agencies. In the UK the Intelligence and Security Committee's (ISC) legal remit covers only part of the intelligence establishment (Defence Intelligence Staff, the Joint Intelligence Committee and National Criminal Intelligence Service are not included in the legal remit of the Committee). In practice, however, and with the cooperation of the government, the ISC has examined their work.

Broadly speaking, there are two ways in which a parliamentary oversight committee's role can be set out in law. The first is to give a wide remit and then to detail specific matters which may *not* be investigated; examples of this approach can be found in legislation from the UK and Australia.[6] The second is to attempt a comprehensive list of functions, as in the example boxed overleaf (taken from United States Rules of the US Senate Select Committee on Intelligence):

A second, and critical, distinction concerns whether the oversight body is envisaged as able to examine operational detail or is limited to questions of policy and finance (see Box No. 37 overleaf). The German *Bundestag* mandated its Parliamentary Control Panel to scrutinise both policies and operations. Policies include the procedures which enable the intelligence service to operate and to fulfil its tasks. The German Parliamentary Control Panel is fully informed about both these procedures and the implementation thereof. In addition, the German Parliamentary Control Panel should be briefed about operations of the intelligence services as well as intelligence related aspects which received media coverage. Furthermore, the Control Panel should be fully informed about major decisions that alter the internal procedures of the agencies.[7]

Box No. 36:
A Comprehensive List of Tasks for a Parliamentary Oversight Body

Section 13 (edited)
(a) The select committee shall make a study with respect to the following matters:
1. the quality of the analytical capabilities of the United States foreign intelligence agencies and means for integrating more closely analytical intelligence and policy formulation;
2. the extent and nature of the authority of the departments and agencies of the executive branch to engage in intelligence activities and the desirability of developing charters for each intelligence agency or department;
3. the organisation of intelligence activities in the executive branch to maximise the effectiveness of the conduct, oversight and accountability of intelligence activities; to reduce duplication or overlap; and to improve the morale of the personnel of the foreign intelligence agencies;
4. the conduct of covert and clandestine activities and the procedures by which Congress is informed of such activities;
5. the desirability of changing any law, Senate rule or procedure, or any Executive order, rule, or regulation to improve the protection of intelligence secrets and provide for disclosure of information for which there is no compelling reason for secrecy;
6. the desirability of establishing a standing committee of the Senate on intelligence activities;
7. the desirability of establishing a joint committee of the Senate and the House of Representatives on intelligence activities;
8. the authorisation of funds for the intelligence activities.

Source: United States Rules of the US Senate Select Committee on Intelligence

Box No. 37:
Elements of Parliamentary Oversight (Germany)

Section 1(1) With respect to the activities of the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*), the Military Counter-Intelligence Service (*Militärischer Abschirmdienst*) and the Federal Intelligence Service (*Bundesnachrichtendienst*), the Federal Government shall be subject to the supervision of the Parliamentary Control Panel (*Parlamentarisches Kontrollgremium*).

Section 2: The Federal Government shall provide the Parliamentary Control Panel with comprehensive information regarding the general activities of the authorities referred to in Section 1 (1) above, as well as regarding operations of special significance. At the request of the Parliamentary Control Panel, the Federal Government must also report on other operations.

Section 2a: As part of its duty to provide information under Section 2 above, the Federal Government must, if so requested, allow the Parliamentary Control Panel to inspect the services' documents and files to speak to the employees of the services as well as arranging for the Panel to visit the services.

Source: Act governing the Parliamentary Control of Intelligence Activities by the German Federation. Parliamentary Control Panel Act (PKGrG), Germany, April 1978 (cited text includes amendments of 1992 and 1999), Section 2, 2a.

A parliamentary oversight body able to examine intelligence operations may have greater credibility and may be given greater powers (for example, to compel the production of evidence). However, it will face inevitable restrictions on how it conducts its investigations and on what can be reported to parliament or to the public. It will operate in effect within the ring of secrecy and that will create a barrier between it and the remainder of parliament. Provided it establishes a reputation for independence and apparent thoroughness this need not affect its legitimacy. However, 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 the supporting evidence being available. A second danger is that an oversight body of this type gets too close to the agencies it is responsible for overseeing. For example, although a legal requirement that it be notified in advance of certain actions by the agency may appear to strengthen oversight, it could also inhibit the oversight body from later criticism of these operational matters.

The alternative approach is to limit the function of the parliamentary oversight body to matters of policy and finance. These are issues which can be more readily examined in the public arena with the need for far fewer restrictions in the national interest on what is disclosed (although the publication of precise budgetary details may be prejudicial to national security). The difficulty of this second approach, however, is that it detracts from one of key tasks of parliamentary scrutiny: to ensure that government policy in a given field is carried out effectively. Without access to *some* operational detail, an oversight body can have or give no assurance about the efficiency of the security and intelligence agency in implementing the published policy. The same applies to auditing issues of legality or the agencies' respect for fundamental rights – tasks which are given to parliamentary oversight bodies in some countries. Such exercises in parliamentary oversight may lack credibility unless founded on some clear evidence about the behaviour of the agency concerned.

It seems, then, that the ring or barrier of secrecy poses a dilemma for the design of parliamentary oversight; within the barrier oversight may be effective but cannot be shown to be so, outside the barrier it may operate in parallel to but never really touch the actions of the agencies concerned.

In practice several strategies can be adopted to overcome this conundrum. One is to create institutions or offices that can go behind the ring of secrecy on parliament's behalf and report to a parliamentary oversight body. In some countries Inspectors-General perform this role (although they also perform a different function of strengthening executive oversight – see Chapter 22).

A second method is to provide for *ad hoc* reference of operational matters to the parliamentary oversight body (as a body with recognised expertise in the field), either by the government or by parliament itself. The following box illustrates how this method is legislated for in Australia.

Box No. 38:
The Provision of *ad hoc* Reference of Operational Matters to the Parliamentary Oversight Body

Section 29 – Functions of the Committee
(1) The functions of the Committee are:
b. to review any matter in relation to ASIO, ASIS or DSD referred to the Committee by:
(i) the responsible Minister, or
(ii) a resolution of either House of the Parliament.
Source: Intelligence Services Act 2001, Australia, Section 29

Ad hoc investigations are most likely to be used where the alleged actions of the agencies cause controversy. Where this happens, access to the necessary information is also likely to be given since the government and agencies will wish to be seen to cooperate. However the oversight body's negotiating position may be strengthened if it can decline to conduct such an *ad hoc* investigation unless assured that it will be given adequate access to information.

Another example of a more narrow mandate is given by the Norwegian parliamentary intelligence oversight committee. This committee, whose members are not parliamentarians but are appointed by and report to parliament, is mandated to scrutinise whether the services respect the rule of law and human rights (see Box No. 39). Within this focused mandate, the committee has far-reaching investigative powers, covering the entire Norwegian intelligence machinery. Its oversight, which is *ex post facto* oversight, might include operations, but only from the point of view of legality.

Box No. 39:
Parliamentary Oversight Focusing on the Rule of Law and Human Rights: The Example of Norway

'Section 2. The purpose of the monitoring is:
1. to ascertain and prevent any exercise of injustice against any person, and to ensure that the means of intervention employed do not exceed those required under the circumstances,
2. to ensure that the activities do not involve undue damage to civic life,
3. to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law (…)'

Source: The Act relating to the Monitoring of Intelligence, Surveillance and Security Services. Act No. 7 of 3 February 1995, Norway

Best Practice

- ✓ Horizontal scope of the mandate: the entire intelligence community, including all ancillary departments and officials, should be covered by the mandate of one or more parliamentary oversight bodies;
- ✓ Vertical scope of the mandate: the mandate of a parliamentary oversight body might include some or all of the following (a) legality, (b) efficacy, (c) efficiency, (d) budgeting and accounting; (e) conformity with relevant human rights Conventions (f) policy/administrative aspects of the intelligence services;
- ✓ All six aspects mentioned above should be covered by either the parliamentary oversight body or other independent bodies of the state, eg national audit office, inspectors-general, ombudsman or court. Overlap should be avoided;
- ✓ The bigger an intelligence community is and the more different intelligence services are involved, the greater is the need for specialised parliamentary oversight (sub)committees;
- ✓ The mandate of a parliamentary oversight body should be clear and specific;
- ✓ The recommendations and reports of the parliamentary oversight body should be (a) published; (b) debated in parliament; (c) monitored with regard to its implementation by the government and intelligence community;
- ✓ The resources and legal powers at the disposal of the parliamentary oversight body should match the scope of its mandate.

Chapter 16

The Composition of a Parliamentary Oversight Body

In order to enjoy legitimacy and command trust it is vital that parliamentary oversight bodies in this area have a broad mandate, are appointed by parliament itself and represent a cross-section of political parties. Although wherever possible members should have some relevant expertise (for example from previous ministerial service), in our view it is also essential that they be civilian – there must be clear demarcation between the oversight body and the agencies overseen in order for oversight to be effective. A particular difficulty arises in transition states – the presence of former members of the security agencies on the oversight body. Where the services were implicated in maintaining a repressive former regime this is bound to undermine confidence in the oversight process and is best avoided, if necessary by a legal prohibition.

Equally, to be effective a parliamentary committee must enjoy a relationship of trust with the agencies it oversees. This suggests that to be effective a relatively small committee (without, however, compromising the principle of cross-party membership) is best.

As the oversight of security and intelligence services requires expertise and time, some parliaments have chosen to set up a committee outside the parliament, whose members are not parliamentarians, but are appointed by parliament and report to parliament (eg Norway; Canada [proposed reforms][8]).

Options for appointing the membership of parliamentary oversight bodies vary from countries where the head of government appoints (after consultation with the Leader of the Opposition, in the case of the UK)[9], to where the executive nominates members but parliament itself appoints (as in Australia)[10], to instances in which the legal responsibility for appointment rests solely with the legislature (as in Germany[11] and Norway[12]). The issue of appointment is plainly connected with that of vetting and security clearance (see Chapter 17): the executive may feel more relaxed about clearance where it has formal responsibility for appointment or has a monopoly over nominations.

The chairman of an oversight body will invariably have an important role in leading it and determining how it conducts its business as well as directing liaison with the services outside formal committee meetings. Traditions within parliamentary systems vary concerning the chairmanship of parliamentary committees. While being sensitive to different traditions, the legitimacy of a parliamentary oversight body will be strengthened if it is chaired by a member of the opposition, or if the chairmanship rotates between the opposition and the government party.

Box No. 40:

Appointing Members of Parliamentary Oversight Bodies: Examples from selected states

Germany:

'Section 4 (1) At the beginning of each electoral period the German *Bundestag* shall elect the members of the Parliamentary Control Panel from amongst its own members; …(3) Those who obtain a majority of the votes of the members of the German *Bundestag* shall be elected.

Source: German Federation Parliamentary Control Panel Act, 1978 amended (PKGrG)

United Kingdom:

'10(2) The Committee shall consist of nine members (a) who shall be drawn both from members of the House of Commons and from members of the House of Lords and (b) none of whom shall be a Minister of the Crown; (3) The members of the Committee shall be appointed by the Prime Minister after consultation with the Leader of the Opposition (…).'

Source: Intelligence Service Act, 1994.

The Netherlands:

'The [Parliamentary Oversight] Committee decided that the legitimacy of its functioning had become too limited and that, therefore, chairpersons of all parliamentary factions should have a seat on the Committee'.

Source: *Report of the Committee for Security and Intelligence Services on its Activities During the Last Five Months of 2003*, 2nd Chamber of Parliament, Session Period 2003-2004, 29 622, nr. 1, 3 June 2004

Argentina:

'The [bi-cameral legislative] Committee includes 14 legislators, seven appointed by the Chamber of Deputies and seven by the Senate. The president, the two vice-presidents and the secretary of the Joint Committee are chosen by simple vote of its members, with a term of office of two years, rotating between each one of the two chambers. (…) There is no special procedure to veto prospective members or to remove members of the Joint Committee other than not having or losing the political confidence of its faction members, particularly the president of the faction. All legislators are eligible to be members of the Joint Committee.'

Source: Estevez, E. 'Argentina's new century challenge: Overseeing the intelligence system' in: Born, H., Johnson, L, Leigh, I. (eds.) *Who's Watching the Spies? Establishing Intelligence Service Accountability*, (Dulles, VA: Potomac Books, Inc., 2005).

Hungary:

'(…) At all times the Chairman of the Committee may only be a member of the Opposition.'

Source: Section 14, 1, Act nr. CXXV of 1995 on the National Security Services, Hungary.

The chairman should be chosen by the parliament or by the committee itself, rather than appointed by the government. Trust in the Chairmanship will be enhanced to the extent that it is seen to be independent of government. The only compelling case for a requirement that a government supporter chair the committee is where this applies to

all other parliamentary committees also. Even in such circumstances it is preferable that the choice of chairman from among those eligible is within parliament or the committee itself and that the chairman holds office at the pleasure of the parliament or the committee.[13]

Best Practice

- ✓ Parliamentary oversight bodies should be clearly 'owned' by parliament;
- ✓ Parliament should be responsible for appointing and, where necessary, removing members of a body exercising the oversight function in its name;
- ✓ Representation on parliamentary oversight bodies should be cross-party, preferably in accordance with the strengths of the political parties in parliament;[14]
- ✓ Government ministers should be debarred from membership (and parliamentarians should be required to step down if they are appointed as ministers) or the independence of the committee will be compromised.[15] The same applies to former members of agencies overseen;
- ✓ Committee members should have security of tenure at the pleasure of parliament itself, rather than the head of government; [16]
- ✓ The chairman should be chosen by the parliament or by the committee itself, rather than appointed by the government.

Chapter 17

Vetting and Clearance of the Oversight Body

Vetting is a process by which an individual's personal background and political affiliation is examined to assess his or her suitability for a position that may involve national security concerns. Whether it is necessary for members of a parliamentary committee to be subject to security vetting or clearance depends on several related factors.

If the appointment or nomination process is in the hands of the government there is likely to be an informal process of vetting in practice prior to nomination or appointment and people who are regarded as security risks are unlikely to be put forward in the first place.Equally the tasks and powers of the committee are relevant in discussing the need for vetting or security clearance. A committee whose task is confined to discussion of policy or which lacks the power to subpoena evidence or to receive sensitive evidence concerning intelligence operations or sources hardly needs to be vetted.

Constitutional differences are relevant also. Where the constitutional tradition is opposed to the vetting of the *ministers* responsible for the security and intelligence services, it would be inappropriate if parliamentarians involved in oversight were to be vetted.

On the other hand, where (as is preferable) the committee has wider functions and powers, it is important that members of the oversight body have adequate access to the information and documents. If members of the oversight body are not trusted with material of this kind (for example, where appropriate, by being given the highest security clearance) oversight will be incomplete at best. Therefore, some parliaments (eg Norway) have enacted legislation that allows members of the oversight body to (immediate) access to all information that is necessary for the proper execution of the tasks of the oversight body.

Box No. 41:
Clearance of the Norwegian Parliamentary Intelligence Oversight Committee

'Those elected [to the Parliamentary Oversight Committee] shall be cleared for the highest level of national security classification and according to treaties to which Norway is a signatory. After the election, authorisation shall be given in accordance with the clearance.'

Source: Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS), Norway, 1995, *Section 1, para. 2:*

Vetting of members of a parliamentary oversight body raises an obvious dilemma: who is to be responsible for the vetting? There is a clear conflict of interest in the overseers being vetted by those they are responsible for overseeing. However, this is to some degree unavoidable. The suspicion that the criteria for vetting may screen out those likely to be hostile to the security and intelligence agencies is best countered by clear public criteria for vetting and the possibility of a challenge being brought to a refusal of clearance. The criteria and the process for vetting should be sufficiently clear, consistent and robust to withstand democratic scrutiny. It should be borne in mind, however, that in many countries the outcome of vetting is merely advisory – in these cases it may be sufficient to merely affirm the ability of the appointing body to continue with the appointment, notwithstanding an adverse report (see Box 42 below).

Box No. 42:
Dealing with Denial of Security Clearances for Members of Parliament of Bosnia and Herzegovina

'(…) In cases where the Agency denies issuance of a security clearance to a nominee, the Collegium of the Parliamentary Assembly may request that the Agency reconsider such denial if it has justified concerns as to its legitimacy. Should the Agency reaffirm the original denial, the Collegium shall either put forward the name of another candidate or confirm its initial proposal (…).'

Source: Art. 18 Law on Intelligence and Security Agencies of Bosnia and Herzegovina, 2004

It is better that vetting of members of a committee takes place formally, rather than through informal processes. This is fairer to the parliamentarians concerned (who will then be aware that vetting is taking place) and allows for proper processes by which an adverse decision can be justified and challenged.

Procedures for challenging vetting refusals are a difficult area since there is a balance to be maintained between fair procedure, national security and the protection of individual privacy. In principle it is best if cases involving parliamentarians can be handled using the normal machinery available to state officials and others denied clearance, so that they do not become matters of public discussion and parliamentary debate.

Members of parliamentary oversight committees should only be vetted where, because of the remit or powers of the committee, they are likely to come into contact with operationally sensitive material. Where vetting is necessary it should be formal: the parliamentarian should be aware that it is taking place, the criteria and process involved should be published, the outcome should be made available both to the appointing body (in a way that respects the privacy of the individual concerned so far as possible) and to the parliamentarian, and there should be an opportunity to challenge the outcome before an independent body.

Best Practice

- ✓ Members of parliament should only be vetted if the committee's mandate includes dealing with operationally sensitive material;
- ✓ Where clearance is denied to members of parliament by the security and intelligence services, procedures should be established to deal with disputes authoritatively, giving the final decision to the parliament or its presidium;
- ✓ The criteria for vetting should be clear, public, consistent and robust in order to withstand democratic scrutiny.

Chapter 18

Parliamentary Powers to Obtain Information and Documents

The parliament, and particularly the oversight body, needs to have sufficient power to obtain information and documents from the government and intelligence services. The precise extent that a parliamentary oversight body requires access to security and intelligence information and the type of information concerned depends on the specific role that it is asked to play. An oversight body whose functions include reviewing questions of legality, effectiveness and respect for human rights will require access to more specific information than one whose remit is solely policy. Similarly, it will have a stronger case for a right of access to documents (rather than information or testimony from identified witnesses).[17] Clearly, however, an oversight body should have unlimited access to the necessary information in order to discharge its duties.

Box No. 43:
The Argentinean Joint Committee's Right to Information

Art. 32
The Joint Committee [for the Oversight of Intelligence Services and Activities] shall have full authority to control and investigate by its own. Upon its request, and in accordance with the provisions established by article 16, the agencies of the National Intelligence System shall submit the information or documentation that the Committee requests.

Source: National Intelligence Law, No. 25520 of 2001, Art. 32.

The differences in role explain some of the variations in the extent to which oversight bodies are given access to operational detail in different constitutional systems. Some countries, e.g. the US, provide that the executive has the responsibility to keep the oversight body informed.

Box No. 44:
Duty to keep the Congressional Committees Fully and Currently Informed about Intelligence Activities (US)

1. The President shall ensure that the intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this subchapter (…).
   (b) Reports concerning illegal intelligence activities. The President shall ensure that any illegal intelligence activity is reported promptly to the intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity.

Source: United States Code, Title 50, Section 413 (a)

Additionally, the US Congressional Oversight Provisions demand that the President keeps the Congressional intelligence committees informed about covert operations (see Chapter 11). The box below illustrates executive duties in this respect.

Box No. 45:
Reporting of Covert Action to the US Congressional Intelligence Committees

'(…) (b) Reports to intelligence committees; production of information
To the extent consistent with due regard for the protection from unauthorised disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of Central Intelligence and the heads of all departments, agencies, and entities of the United States Government involved in a covert action:

1. shall keep the intelligence committees fully and currently informed of all covert actions which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including significant failures; and
2. shall furnish to the intelligence committees any information or material concerning covert actions which is in the possession, custody, or control of any department, agency, or entity of the United States Government and which is requested by either of the intelligence committees in order to carry out its authorised responsibilities.

(c) Timing of reports; access to finding

1. The President shall ensure that any finding approved pursuant to subsection (a) of this section shall be reported to the intelligence committees as soon as possible after such approval and before the initiation of the covert action authorised by the finding, except as otherwise provided in paragraph (2) and paragraph (3).'

Source: United States Code, Title 50, Section 413b.

Systems vary in how they handle reporting of sensitive material. In the US, the onus of *being informed* not only rests with the oversight body, but with the executive as well. In Australia, on the other hand, the Parliamentary Committee is forbidden from requiring 'operationally sensitive information' from being disclosed;[18] requests for documents cannot be made be made by the Committee to agency heads or staff members or to the Inspector-General, and ministers may veto evidence from being given.[19] A power of veto of this kind effectively returns disputes over access to information to the political arena. What is important is that powers to obtain information match the parliamentary oversight body's mandate.

Various countries have stipulated that the oversight body is also entitled to obtain information and documents from experts of both the services as well as civil society, eg think tanks or universities. Such a provision guarantees that the parliament is able to receive alternative viewpoints, in addition to the position of the government. These provisions will be more powerful if the oversight body is able to subpoena witnesses and to receive testimony under oath.

Box No. 46:

Consulting External Expertise (Luxembourg)

'When the [parliamentary] control concerns a field that requires special knowledge, the [Parliamentary Control] Committee can decide, with two-thirds majority vote and after having consulted the Director of the Intelligence Service, to be assisted by an expert.'

Source: Art. 14 (4), Loi du 15 Juin portant organisation du Service de Renseignement de l'Etat, Memorial-Journal Officiel du Grand-Duché de Luxembourg, 2004, A-No. 113 (unofficial translation)

However, as often the information and documents are related to sensitive issues (about persons) and/or about national security, oversight bodies of various countries have made great efforts to protect information from unauthorised disclosure. There is a case for clear prohibitions governing the unauthorised disclosure by members of the parliamentary oversight body or their support staff. Unauthorised disclosure of information may not only harm national security interests, but may also harm the trust which is necessary for an effective relationship between the oversight body and the services. This is partly a matter of legislation (see the US[20] and in Norway[21]), and partly a matter of proper behaviour of the members of the oversight body to deal with classified information with care and attention.

Best Practice

- ✓ The oversight body should have the legal power to initiate investigations;
- ✓ Members of oversight bodies should have unrestricted access to all information which is necessary for executing their oversight tasks;
- ✓ The oversight body should have power to subpoena witnesses and to receive testimony under oath;
- ✓ Where relevant to the oversight body's remit, the executive should have responsibility for keeping the oversight body informed;
- ✓ The oversight body should take appropriate measures and steps in order to protect information from unauthorised disclosure;
- ✓ Disputes over access to information between the agencies and the oversight body should be referred in the last analysis to the Parliament itself.

Chapter 19

Reporting to Parliament

Reports from parliamentary committees are the main process by which public confidence in the process of parliamentary oversight is instilled. In some countries the committee may report to the entire parliament, to a group of deputies representing the various political parties, or to the presidium, without this report being published. Other countries have the tradition that all reports to parliament are public documents.

Inevitably, in order to protect security, there is a limit to what can or should be reported publicly. Nevertheless, unless the committee itself is responsible for such decisions the oversight system will lack credibility and will be capable of being abused in order to cover inefficiency or malpractice.

There should be a legal duty on a parliamentary oversight committee to report at least annually (see Box No. 47 below). Primary responsibility for the timing and a form of a parliamentary committee's report and any decision to publish evidence should lie with the committee itself. It is best if a parliamentary oversight body reports directly to parliament rather than through the government since this enhances the parliamentary 'ownership' of the committee. It is good practice, however, to give sufficient advance notice of a final report to the government so that it can make a response on publication. Where reporting takes place through the government there should be clear legal duty on government ministers to lay the report in full before parliament within a stipulated time.

Box No. 47:
Informing Legislature and Executive about Committee's Activities and Recommendations (South Africa)

1. The Committee shall, within five months after its first appointment, and thereafter within two months after 31 March in each year, table in parliament a report on the activities of the Committee during the preceding year, together with the findings made by it and the recommendations it deems appropriate, and provide a copy thereof to the president and the minister responsible for each service.
2. The Committee may at the request of parliament, the president or the minister responsible for each service or at any other time which the Committee deems necessary, furnish parliament, the president or such minister with a special report concerning any matter relating to the performance of its functions; and shall table a copy of such report in parliament or furnish the president and the minister concerned with copies, as the case may be.

Source: Intelligence Services Control Act 1994 (2002)

Concerns over disclosure of sensitive information by the committee can be met by imposing a legal duty to consult the agencies over material derived from them that is

included in reports or evidence (which is good practice in any event), or by prohibiting very limited categories of information from being published (for instance, the identity of intelligence operatives), but the government or the agencies should not enjoy a veto.

Box No. 48:
Restrictions on Disclosure to Parliament (Australia)

The Committee must not disclose in a report to a House of the Parliament:
a. the identity of a person who is or has been a staff member of ASIO or ASIS or an agent of ASIO, ASIS or DSD; or
b. any information from which the identity of such a person could reasonably be inferred; or
c. operationally sensitive information or information that would or might prejudice:
   (i) Australia's national security or the conduct of Australia's foreign relations; or
   (ii) the performance by an agency of its functions.

Source: Intelligence Services Act, 2001, Schedule 1, Part 1, Clause 7,1

Absence of a government veto on publication is the better practice. In states that do incorporate a veto, however, the government or agencies should, nevertheless, be required by law to state in general what is omitted from the published report and the reason for omission. This enables political scrutiny of such decisions to take place through the normal parliamentary process.

Best Practice

- ✓ Primary responsibility for the timing and form of the Parliamentary Committee's Report and any decision to publish evidence should lie within the committee itself;
- ✓ The committee should report to parliament at least yearly or as often as it deems necessary;
- ✓ The parliamentary oversight body should have the final word on whether it is necessary to remove material from a public report for security reasons;
- ✓ The government and the agencies should be given prior sight of the draft report so that representations about necessary security deletions can be made.

Chapter 20

Budget Control

Budget control is at the heart of parliamentary control. Most countries have developed or are developing a systematic approach to the evaluation and approval of budget proposals. In every country, parliament fulfils a different role in the budgeting and accounting procedures for the security and intelligence services, for example, in terms of the scope of budget control, the power to amend budgets, the power to approve supplementary budget requests, access to classified information (see Chapter 18) and the disposition of independent financial auditors (see Chapter 23). The greater the parliament's powers in these areas the more effective it will be in debates with the government. Concerning the power of the purse, three types of parliaments exist, in descending order of influence:

- *Budget-making parliaments*: parliament has the capacity to amend or to reject the budget proposal for the security and intelligence services as well as the capacity to formulate its own alternative budget proposal;
- *Budget-influencing parliaments*: parliament can amend or reject the budget, but lacks the capacity to put forward its own proposals;
- *Parliaments with little or no effect on budget formulation*: parliament lacks the capacity either to amend or to reject the budget or to come forward with its own proposals. At best, they limit their role to assenting to the budget as proposed by the government.[22]

In any case, it is a minimum requirement that parliament has a say in budget issues as the security and intelligence services are financed with taxpayers' money. From this point of view, parliaments around the world have claimed a role in the budgeting and accounting process of the security and intelligence services.

The power of the purse as exercised by parliament has to be seen within a dual context – that of the entire budget process, as well as the mandate of the parliamentary body charged with oversight of these specific activities of government.

The Budget Process

Parliament can be attentive to issues related to the security and intelligence services in all phases of the budget cycle for which most countries have adopted a planning, programming and budgeting system:[23]

Budget-preparation: generally speaking, this phase is for the executive to propose allocations of money for several purposes but parliament and its members can contribute to the process through different formal and informal mechanisms.

Budget-approval: in this phase the parliament should be able to study and determine the public interest and suitability of the money allocation and may in certain contexts complement security-related appropriations with specific guidelines. An example of specific guidelines can be found in the case of the US Congress where the Congress designates the financial ceiling (including the budget from research and development to operations) and sets personnel ceilings for the maximum number of officials to be hired by the services in the upcoming fiscal year.[24]

Execution or spending: in this phase, parliament reviews and monitors government spending and may strive to enhance transparency and accountability (see corresponding section below). In the case of supplementary budget requests, parliament monitors and scrutinises these demands to prevent cost overruns. In some countries, for example in the US, the relevant intelligence oversight committees of the US Congress and the relevant subcommittees of the Appropriations Committee must be informed if elements of the intelligence community shift money from one account to another. [25]

Audit or review: in this phase, parliament determines whether there was misuse of the money allocated by the government. Additionally, parliament periodically evaluates the entire budget and audit process to ensure accountability, efficiency and accuracy. The role of audit offices is discussed in Chapter 23.

Budget Control and the Mandate of the Parliamentary Oversight Body

Budget control has also to be understood in the context of the mandate of the parliamentary intelligence oversight body. In some countries, this body clearly has the power of the purse as the embodiment of the people's voice. In other countries, for example in Norway, parliament has chosen not to give the power of purse to the (independent expert) oversight committee, but kept that power for the plenary or the parliamentary budget committee. The reason behind this practice is that budget control would make the oversight committee co-responsible for government policy. Therefore in Norway the parliamentary intelligence oversight committee focuses on whether the services comply with the rule of law and respect human rights only and leave budget oversight to other bodies of the parliament. In doing so, the intelligence committee can maintain independence in scrutinising the services.

In other parliaments, however, such as in Argentina, the Netherlands, Germany or the US, the parliamentary oversight committee has the power of the purse, giving those parliaments better insights about how money is spent by the services. To be more precise, in the US, as well as, for example, in Germany, the power of the purse is often divided between the budget committee and the intelligence oversight committee. The former committee focuses on appropriations; the latter committee focuses on the policy aspects of the services and authorises funds.

Box No. 49 overleaf illustrates the practice in Germany.

Box No. 49:
Financial Auditing by the German Parliamentary Control Panel

Section 2e
1. The Chairman, his deputy and an authorised member may take part, in an advisory capacity, in the meetings of the Confidential Committee *(Vertrauensgremium,* whose members also sit on the *Bundestag's* Budgetary Select Committee*)*, which acts pursuant to Section 10a of the Federal Budget Code *(Bundeshaushaltsordnung)*. Equally the Chairman of the Confidential Committee, his deputy and an authorised member, may also take part in the meetings of the Parliamentary Control Panel in an advisory capacity.
2. Draft copies of the annual economic plans of the services shall be transmitted to the Parliamentary Control Panel for co-deliberation. The Federal Government shall provide the Panel with information regarding the implementation of economic plans during the budgetary year. During discussions relating to the services' economic plans and their implementation, the members of both authorities may take part in each other's meetings in an advisory capacity.

Source: Act governing the Parliamentary Control of Intelligence Activities, Germany, April 1978 (amended in 1992 and 1999)

In accordance with section 2(e) para. 2 of the law on German Parliamentary Control Panel (PKGr), the services' draft annual budgets are forwarded to the PKGr for consultation. However, the consultation does not mean that the PKGr scrutinises these draft budgets in the manner of a budget committee. Instead, PKGr subjects the overall activities of the intelligence services to a political analysis on the basis of the budgets and the extensive data these contain – with respect to the structure, the personnel, the projects and the activities of the services. After the consultations have been completed, an assessment is forwarded to the German Bundestag's Confidential Forum of the Budgetary Select Committee, which is actually in charge of reviewing the draft budgets. The federal government also keeps the PKGr informed about the execution of the budgets during the budget year.[26]

Transparency and Accountability

Accountability and transparency are essential conditions for effective budgeting. The best way to realise accountability is through a transparent process of budget-making. Proper accountability and transparency can be developed from the following principles of effective budgeting:[27]

Prior authorisation – The parliament should authorise the executive to carry out expenditure.

Unity – All expenditure and revenue should be presented to parliament in one single consolidated budget document.

Regularity – The executive is expected to respect a regular time-frame to present the budget every year to the parliament (instead of, for example, every five years).

Regularity also involves the need for specifying the time-frame during which the money allocations will be spent.

Specificity – The number and descriptions of every budget item should result in a clear overview of the government's expenditure. Therefore the description of the budget items should not be vague and the funds related to a budget item should not be too large. Giving the parliament only the grand totals of the yearly budget for the security and intelligence services would clearly violate the principle of specificity.

Legality – All expenditures and activities should be in keeping with the law. In this context, the services are not allowed to acquire funds outside the state budget (for example, through commercial activities).

Accessibility – The executive is expected to acquaint the parliament with a plan of estimated expenditure that is manageable and understandable to the wide and diverse audience that is usually present in parliament.

Comprehensiveness – The state budget concerning the different aspects of the security sector has to be all-inclusive and complete. No expenditure should go unaccounted for. In this context, 'black' programmes or secret budgets – inaccessible for members of the parliamentary intelligence oversight committee – would be clearly in violation of this principle. Parliamentarians of the intelligence oversight committee and the budget committee should have access to all classified information. Section 14, para. 4.9 of the Hungarian Law illustrates how the comprehensiveness of budget control can be legislated.

Box No. 50:
Comprehensive Budget Control by Parliament (Hungary)

'While exercising parliamentary control, the committee (…) shall give its opinion on the detailed draft budget of the national security services, the items of the budget of other organisations entitled to gather intelligence related to such activities, and the draft of the detailed report on the execution of the Act on the Budget of the year, and shall make a proposal during the debate on the bills to Parliament to adopt the bill in question(…).'

Source: Article 14, 4g of the 1995 Act on the National Security Services of Hungary.

Consistency – Clear links should be established between policies, plans, budget inputs and performance outputs.

Effectiveness – The budget explanation should be able to communicate clear understandings of the aims of the budget in terms of a) resource inputs; b) performance or capacity objectives to be achieved, and c) measurable results on plans. A flexible budget should allow changes in any of these three parameters.

These principles may in fact be considered to be quality criteria for proper modern budgeting. They imply that the normal principles of good governance (see Introduction) which govern other activities of government, should also apply to the

security and intelligence services. Exceptions in terms of, for example, secrecy, should be legally limited.

Where parliamentarians lack appropriate information on the security sector, they are unable to raise issues concerning the budget of the services. As in other branches of the state, safeguards can be put into place in order to avoid improper disclosure of classified information. This issue is discussed in Chapter 18 on access to classified information by parliamentarians. Concerning public access to budget information, in some countries the grand totals of the security and intelligence services' budget are available to the public. This is the case, for example, in the United Kingdom.[28]

Best Practice

- ✓ The oversight body should have access to all relevant budget documents, provided that safeguards are in place to avoid leaking of classified information;
- ✓ The oversight of the budget of the security and intelligence services should be governed by the same principles of good governance which regulate other activities of government. Exceptions should be regulated by law. From this point of view, the oversight of the budget should be a shared power between the appropriations committee and the intelligence oversight committee;
- ✓ Powerful parliaments should have the right to authorise the budget;
- ✓ Intelligence Agencies should only use funds for activities if those funds were specifically authorised by the legislative branch for that purpose;
- ✓ The intelligence services should not be allowed to transfer funds outside the agency without the authorisation of the legislature.

Endnotes Section IV – The Role of Parliament

1. The following text is based on Leigh, I., 'Three Decades of Oversight', in Born, H Johnson, L., Leigh, I. (eds.), *Who's Watching the Spies? Establishing Intelligence Service Accountability*, (Dulles, VA: Potomac Books, Inc., 2005).
2. Some countries have institutionalised and legalised parliamentary oversight before the mid 1970s, such as the US, Germany and the Netherlands.
3. Australian Security Intelligence Organisation Act 1979 (Cth) and Canadian Security Intelligence Service Act 1984, respectively. Lustgarten, L, Leigh, I., *In from the Cold: National Security and Parliamentary Democracy* (Oxford: Clarendon Press, 1994).
4. For other comparative reviews see: Brodeur, J-P., Gill, P., Töllborg, D., *Democracy, Law and Security: Internal Security Services in Contemporary Europe* (Aldershot: Ashgate, 2003); Assembly of the WEU, *Parliamentary oversight of the intelligence services in the WEU countries – current situation and prospects for reform* (Document A/1801, 4 December2002);<http://assemblyweu.itnetwork.fr/en/documents/sessions_ordinaires/rpt/2002/1801.html>
5. Council of Europe, Parliamentary Assembly, *Recommendation 1402/1999*; Western European Union Assembly*, Resolution 113*, adopted on 4 December 2002 (9th sitting).
6. Intelligence Services Act 2001 No. 152, 2001**,**Sections 28 and 29 (Committee on ASIO, ASIS and DSD). Note in particular: Section 30.
   3. The functions of the Committee do not include:
   (a) reviewing the intelligence gathering priorities of ASIO, ASIS or DSD; or
   (b) reviewing the sources of information, other operational assistance or operational methods available to ASIO, ASIS or DSD; or
   (c) reviewing particular operations that have been, are being or are proposed to be undertaken by ASIO, ASIS or DSD; or
   (d) reviewing information provided by, or by an agency of, a foreign government where that government does not consent to the disclosure of the information; or
   (e) reviewing an aspect of the activities of ASIO, ASIS or DSD that does not affect an Australian person; or
   (f) reviewing the rules made under section 15 of this Act; or
   (g) conducting inquiries into individual complaints about the activities of ASIO, ASIS or DSD.

   Intelligence Services Act 1994, s. 10 (UK) establishing the Intelligence and Security Committee with jurisdiction to investigate the policy, administration and finance of the Security service (MI5), the Secret Intelligence Service (MI6) and GCHQ.
7. German *Bundestag*, Secretariat of the Parliamentary Control Commission, *Parliamentary Control of the Intelligence Services in Germany*. (Berlin: Bundespresseamt, 2001)
8. Until 2004 there was no oversight committee in the Canadian Parliament although the Security Intelligence Review Committee (a statutory body composed of Privy Counsellors) was established under the Canadian Security Intelligence Service Act 1984. A parliamentary oversight committee is soon to be established: see Farson, S., 'The Delicate Balance Revisited: Parliamentary Democracy, Intelligence, and the War against Terrorism in Canada', in: Born, H. et al, *Who's Watching*.
9. Intelligence Services Act 1994, s. 10.
10. Intelligence Services Act 2001, s. 14. The Prime Minister is required to consult the leaders of all other parliamentary parties before making the nominations: s. 14(2).
11. Law on the Parliamentary Control of Activities of the Federal Intelligence Services (PKGrG) (1978; 1992, 1999 and 2001 amended version). The PKGrG stipulates that at the beginning of each legislative period the German *Bundestag* shall elect the members of the PKGr from amongst its midst (§4 para 1 PKGrG), and that the number of the PKGr's

members, its composition and its working practices shall be laid down in a resolution of establishment (§4 para 2).
Composition: The amendment of the Parliamentary Commission Regulation Act (1995) increased the number of members to nine. To get elected, each member of the PKGr needs the support of a majority of members of the Bundestag (§4 para 3 PKGrG).

12. Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS), 1995, Section 1.
'The Committee shall have seven members including the chairman and vice-chairman, all elected by the Storting, *on the recommendation of Presidium of the Storting,* for a period of a maximum of five years. Steps should be taken to avoid replacing more than four members at the same time.'
13. For example, see Intelligence Services Act 2001, s. 16 (Australia).
14. Intelligence Services Act 2001, s. 14(5) (Australia);
15. For examples see Intelligence Services Act 2001, s. 14(6) (Australia);
16. See for example Intelligence Services Act 2001, s. 15(1) (Australia);
17. For examples of powers to obtain documents see Intelligence Services Act 2001, s. 30.2; (4) (Australia).
18. Intelligence Services Act 2001, s. 30 (Australia); nor must it require to be disclosed 'information that would or might prejudice Australia's national security or the conduct of Australia's foreign relations'.
Under Section 29 of same Act: 'operationally sensitive information' means information:
(a) about sources of information, other operational assistance or operational methods available to ASIO, ASIS or DSD; or
(b) about particular operations that have been, are being or are proposed to be undertaken by ASIO, ASIS or DSD; or
(c) provided by, or by an agency of, a foreign government where that government does not consent to the public disclosure of the information.
'responsible minister', in relation to the review of a matter, means the minister responsible for the agency concerned in relation to that matter.
19. Intelligence Services Act 2001, s. 32 (Australia). These certificates cannot be challenged in court but must be deposited in Parliament. Although this restricts the powers of the oversight body it also places the refusal of information firmly into the political arena, where it can be justified or challenged.
20. United States Code Section 413. General Congressional Oversight Provisions, (d).
21. The Act relating to the Monitoring of Intelligence, Surveillance and Security Services, 1995, *Section 9,* (Norway) requiring the Committee and its secretariat to observe a duty of secrecy and comply with regulations for the handling of documents.
22. Adapted from Norton, P., *Does Parliament Matter?, (*New York*:* Harvester Wheatsheaf, 1993)
23. Born, H., Fluri, Ph., Johnsson, A. (eds.), *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices (Handbook Nr. 5 for Parliamentarians),* (Geneva: IPU-DCAF), p. 130.
24. Intelligence Authorisation Act for Fiscal Year 2004 , Sec. 102.
25. See eg section 414 and 415 of the US Code.
26. German *Bundestag*, Secretariat of the Parliamentary Control Commission (PKGr), *Parliamentary Control of the Intelligence Services in Germany*, July 2001.
27. Born, H. et al., *Parliamentary Oversight*, pp. 131-132.
28. Appropriation Act 2004, Chapter 9, Schedule 2, Part 48 'Security and Intelligence Agencies, available at: <http://www.legislation.hmso.gov.uk/acts/acts2004/40009-az.htm#sch2pt48>

Section V

The Role of External Review Bodies

Chapter 21

Resolving Citizens' Grievances

Security and intelligence agencies are often trusted with exceptional powers, such as surveillance or security clearance, which, if used incorrectly or mistakenly, carry the risk of serious injustice to individuals. It is therefore important that some avenue of redress should be open to people who suspect that they may have been the victim of an injustice, for example those whose private life may have been intruded upon or whose career may have been affected. Moreover, in a security or intelligence agency, as with any large body, complaints can highlight administrative failings and lessons to be learned, leading to improved performance. However, precisely because of the secret nature of the processes involved, difficulties in obtaining evidence, and the legitimate need of these agencies to protect sensitive information from public disclosure, redress through public hearings in the regular courts is rarely effective or appropriate. There is also the need to ensure that any system for redress cannot be used by the legitimate targets of a security or intelligence agency to find out about the agency's work. Achieving a balance in any complaints system between independence, robustness and fairness, on the one hand, and sensitivity to security needs on the other is challenging but not impossible.

The essential distinction in these different systems is between:

- Non-judicial processes (ombudsmen or parliamentary committee);
- Judicial-type procedures (courts and tribunals).

Non-Judicial Handling of Complaints

Different oversight systems handle complaints in a variety of ways. An independent official, such as an ombudsman, may have power to investigate and report on a complaint against an agency (this is the case in the Netherlands, see Box No. 51 overleaf). In some countries an independent Inspector-General of security and intelligence deals with complaints against the services as part of the office's overall oversight remit in a rather similar way (see Chapter 21). This is the case in New Zealand and South Africa for example. In addition, specific offices established under freedom of information or data protection legislation may have a role in investigating complaints against the agencies.

Ombudsman-type systems place reliance on an independent official investigating on behalf of the complainant. They usually exist to deal with an administrative failure rather than a legal error as such. They give less emphasis to the complainant's own participation in the process and to transparency. They typically conclude with a report, and (if the complaint is upheld) a recommendation for putting matters right and future action, rather than a judgement and formal remedies.

Box No. 51:
Handling of Complaints: the Dutch National Ombudsman

Article 83
Each person is entitled to file a complaint with the National Ombudsman on the actions or the alleged actions of the relevant Ministers, the heads of the services, the coordinator and the persons working for the services and for the coordinator, with respect to a natural person or legal entity in the implementation of this act or the Security Investigations Act.

Source: Intelligence and Security Services Act 2002, The Netherlands, Art. 83.

Complaints and grievances of citizens can also be dealt with by the parliamentary intelligence oversight committee, as is the case in, for example, Germany and Norway (see Box No. 52 below).

Box No 52:
Handling of Complaints: the Norwegian Parliamentary Intelligence Oversight Committee

'On receipt of complaints, the Committee shall make such investigations of the administration as are appropriate in relation to the complaint. The Committee shall decide whether the complaint gives sufficient grounds for further action before making a statement.

Statements to complainants should be as complete as possible without revealing classified information. Statements in response to complaints against the Security Service concerning surveillance activities shall, however, only declare whether or not the complaint contained valid grounds for criticism. If the Committee holds the view that a complainant should be given a more detailed explanation, it shall propose this to the Ministry concerned.

If a complaint contains valid grounds for criticism or other comments, a reasoned statement shall be addressed to the head of the service concerned or to the Ministry concerned. Statements concerning complaints shall also otherwise always be sent to the head of the service against which the complaint is made.'

Source: Instructions for monitoring of intelligence, surveillance and security services (EOS), Section 8, pursuant Section 1 of the 1995 Act on Monitoring of Intelligence, Surveillance and Security Services, Norway.

Although handling complaints is separate from parliamentary oversight, there is a connection. Parliamentarians are often called on to represent the grievances of individual citizens against government departments. There may be a benefit also for a parliamentary oversight body in handling complaints brought against security and intelligence agencies since this will give an insight into potential failures – of policy, legality and efficiency. On the other hand, if the oversight body is too closely identified with the agencies it oversees or operates within the ring of secrecy, there may also be disadvantages in it handling complaints. The complainant may feel that the

complaints process is insufficiently independent. In cases where a single body handles complaints and oversight it is best if there are quite distinct legal procedures for these different roles. On the whole it is preferable that the two functions be given to different bodies but that processes are in place so that the oversight body is made aware of the broader implications of individual complaints.

In some countries not only citizens but also members of the services are permitted to bring service-related issues to the attention of an ombudsman or parliamentary oversight body**.** For example, in Germany officials may raise these matters with the Parliamentary Control Panel 'although not when acting in their own interest or in the interest of other members of these authorities, insofar as the head of the service has failed to look into matters in question. Members of staff may not be cautioned or penalised for doing so.'[1]

Judicial Handling of Complaints

Alternatively, a specialist tribunal may be established to deal with complaints either against a particular agency or in relation to the use of specific powers, as in the United Kingdom. Or complaints may be handled by a specialist oversight body, as in Canada (see example in Box No. 53 below).

Box No. 53:

Handling of Complaints: the Canadian Security Intelligence Review Committee

Under the Canadian Security Intelligence Service Act 1984 the Security Intelligence Review Committee ('SIRC'), the statutory oversight body composed of Privy Counsellors, is also responsible for investigating complaints brought by individuals 'with respect to any act or thing done by the Service' (section 41) as well as challenges brought to denials of security clearance (section 42). Complainants using these provisions must first raise the matter with the government department concerned and must complain to SIRC in writing. Investigations take place in private, although the complainant is given an opportunity to make representations (s. 46) and to be represented by counsel. Neither the complainant nor the Service is entitled to see the representations of the other. SIRC possesses powers of subpoena and to hear evidence on oath (s. 50). Concerning the report of findings, the Review committee shall:

(a) on completion of an investigation in relation to a complaint under section 41, provide the Minister and the Director with a report containing the findings of the investigation and any recommendations that the Committee considers appropriate; and

(b) at the same time as or after a report is provided pursuant to paragraph (a), report the findings of the investigation to the complainant and may, if it thinks fit, report to the complainant any recommendations referred to in that paragraph.

Source: Canadian Security Intelligence Service Act, 1984.

Judicial procedure does not always involve court hearings. A tribunal has some advantages over a regular court in dealing with security – and intelligence-related complaints: it can develop a distinct expertise in the field of security and intelligence,

judges and lawyers can be vetted as necessary, and specific procedures can be devised for handling sensitive information. In view of the nature of the subject matter these are unlikely to involve a full public legal hearing. On the other hand, while some tribunals may give the complainant a hearing, he or she is likely to face 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. These counsel have the task of challenging security-related arguments, especially those aspects not disclosed to the complainant. This can help the tribunal reach a more objective assessment of the evidence and the arguments.

The ECHR and the Handling of Complaints

For states which are signatory to the ECHR there are considerations about the requirements of different Convention rights under Articles 6, 8 and 13 which need to be observed in designing complaints mechanisms. Article 6 gives the right to a fair trial by an independent and impartial tribunal in criminal matters and in the determination of a person's civil rights and obligations. Article 6 has been taken to apply, for example, to procedures governing evidence from informants and undercover state officials in a criminal trial,[2] and to rules restricting the treatment and disclosure of evidence in the public interest, both in criminal and civil trials.[3] The use of special security-cleared counsel has been commended by the European Court of Human Rights as a way of meeting the requirements of the right to a fair trial Article 6 of the ECHR.[4]

However, even where Article 6 does not apply, procedural protections may be required in complaints processes, because of Articles 8 and 13. These articles impose some *ex post facto* controls in the case of security measures which intrude upon privacy, such as surveillance and security vetting. There is, however, no European Convention blueprint (for example, a person subject to surveillance need not always be informed after the event).[5] Article 13 recognises the right to an effective remedy before a national authority for violation of a Convention right. This need not be a court in every case and in security-related issues the European Court of Human Rights has found that a combination of different oversight and complaints mechanisms may be adequate.[6] As a Council of Europe Working Party put it:

> On the basis of the Court's case-law on Articles 8 and 13 of the Convention it can be concluded that whether the requirement of an effective remedy is satisfied, does not depend only on the mere existence of access to a court, but on the entire arsenal of oversight mechanisms and their effectiveness.[7]

The key criteria of a credible complaints system are that it should:

- Be clearly independent of the security or intelligence agency,
- Have the necessary powers and access to information in the hands of the agency for resolving the complaint
- Be able to award effective remedies in the event of upholding a complaint, and an adequate explanation of the reasons for refusing a complaint.

It is useful if some form of assistance is available to complainants unfamiliar with legal process to help them in lodging a complaint. It should also give an opportunity for the complainant to participate sufficiently in the investigation or proceedings so that the process is seen to be fair, whether or not a formal hearing is given. The process of investigation may need to restrict the information or reasons made available to a complainant for reasons of national security. However, this should be to the minimum extent necessary, it should always be the decision of the person or body handling the complaint, rather than of the agency under investigation, and should be compensated for by other procedural protections (for example, the use of Special Counsel to challenge the agency's case).

Best Practice

- ✓ The official or tribunal hearing the complaint should be persons who fulfil the constitutional and legal requirements to hold an office at this level and should enjoy legal security of tenure during their term of office;
- ✓ As much of the process as possible should be completed in public. Even where the process is closed to the public as much of it as possible should be open to the complainant and his or her legal representatives;
- ✓ There should be a power to dismiss without investigation complaints that the official or tribunal concludes are vexatious or frivolous;
- ✓ If it is necessary for reasons of national security to restrict the participation of a complainant in the review process then the decision to do should be in the hands of the reviewing official or tribunal alone and compensating safeguards (such as the use of a 'Devil's Advocate' or 'Special Counsel') should be provided to ensure that proceeding are fair and impartial;
- ✓ The tribunal or official should have power to make legally binding orders which provide an effective remedy to a complainant who has a justifiable case. These may include the award of compensation and the destruction of material held by the security or intelligence agencies;
- ✓ The scope of review and grounds of review should be clearly established in law and should extend to the substance (rather than merely procedural aspects) of the actions of the security or intelligence agencies.

Chapter 22

Oversight of Agencies within the Administration by Independent Authorities

If, to avoid the dangers of political manipulation, security agencies are given some constitutional 'insulation' from political instructions, how can the government be assured that it has all the relevant information and that secret agencies are acting according to its policies?

For this reason a number of countries have devised offices such as Inspectors-General, judicial commissioners or auditors to check on the activities of the security sector and with statutory powers of access to information and staff.[8]

The idea was first devised in the US intelligence community, which now has around a dozen inspectors-general. All are independent of the agencies concerned. There are, however, significant variations: some of these offices are established by legislation (for example, the Inspectors-General for the Central Intelligence Agency and the Department of Defense), others rest solely on the administrative arrangements established by the relevant Secretary (for example, with regard to the Defense Intelligence Agency and the National Reconnaissance Office). Irrespective of this distinction some report to Congress as well as to the executive branch. A number of these offices have a remit that extends to efficiency, avoiding waste and audit, as well monitoring legality and policy compliance.

Inspectors-General of this kind are within the ring of secrecy: their function is not primarily to provide public assurance about accountability, rather it is to strengthen accountability to the executive. Canadian legislation contains a clear illustration of this type of office.

The Canadian Inspector-General has unrestricted access to information in the hands of the Service in order to fulfil these functions.

Box No. 54:
The Functions of the Canadian Inspector-General

The Inspector-General is responsible to the official in charge of the relevant government department (the Deputy Solicitor-General) and has the role of

(a) monitoring the compliance by the Service with its operational policies;
(b) reviewing the operational activities of the Service; and
(c) submitting an annual certificate to the Minister stating the extent to which the Inspector General is satisfied with the annual report of the Service and whether any of the Service's actions have contravened the Act or ministerial instructions or have involved an unreasonable or unnecessary exercise by the Service of any of its powers.[9]

Source: Canadian Security and Intelligence Service Act, 1984, Sections 30 and 32.

Similarly, in Bosnia and Herzegovina the Inspector-General is responsible under Article 33 of the Law on the Intelligence and Security Agency for providing 'an internal control function'. To this end, the Inspector-General may review the Agency's activities, investigate complaints, initiate inspections, audits and investigations on his or her own initiative, and issue recommendations. The Inspector-General has a duty of reporting at least every six months to the Security Intelligence Committee and of keeping the main executive actors informed of developments in a regular and timely fashion. The powers of the Inspector-General include questioning agency employees and obtaining access to agency premises and data.

Other countries – notably South Africa[10] – have created Inspectors-General to report to Parliament. In these cases the office in effect bridges the ring of secrecy ie it is an attempt to assure the public through a report to Parliament that an independent person with access to the relevant material has examined the activities of the security or intelligence agency. However, inevitably most of the material on which an assessment of the agency's work is made has to remain within the ring of secrecy, although it may be shared with other oversight bodies.

Even some inspectors-general whose statutory brief is to report to the executive may maintain an informal working relationship with parliamentary bodies, this is so in Australia for instance and, as noted above, a number of the US inspectors-general report periodically to Congress.

Whether an office of this kind reports to the government or to Parliament, in either case, careful legal delineation of its 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 any instance, however, the office will need unrestricted access to files and personnel in order to be able to come to a reliable assessment. In practice an independent official is unlikely to be able to scrutinise more than a fraction of the work of an agency. Some of these offices work by 'sampling' the work and files of the agencies overseen – this gives an incentive for the agency to establish more widespread procedures and produces a ripple effect. Some also have jurisdiction to deal with individual complaints (as under the Australian scheme).[11]

Best Practice

- ✓ Review of the functions of the security and intelligence agencies affecting individuals should be by independent and impartial officials (such as Ombudsmen, or Inspectors-General) and comply with the following standards;
- ✓ The official who acts as a reviewer should be a person who fulfils the constitutional and legal requirements to hold an office at this level and should enjoy legal security of tenure during their term of office;[12]
- ✓ The scope of review and grounds of review should be clearly established in law and should extend to the substance (rather than merely procedural aspects) of the actions of the security or intelligence agencies;
- ✓ The official should have sufficient legal powers to be able to review matters of fact and evidence relating to the use of powers of the security or intelligence agencies;
- ✓ The official should have ultimate authority to determine the form and scope of any order or report or decision which results from the process.

Chapter 23

Independent Audit Offices

The executive's and parliament's financial oversight responsibility is far from finished once the intelligence service's budget has been adopted. Not only the executive, but also parliament has to enforce its oversight and audit functions, keeping in mind that the presentation of fully audited accounts to parliament is part of the democratic process and that the auditing process should entail both the auditing of accounts and the auditing of performance. The accounts and annual reports of the security and intelligence services are an important source of information for parliaments to assess how public money was spent in the previous budget year.

Guaranteeing Independence

In most countries the national audit office, (sometimes called the Auditor-General, National Audit Office, Budget Office or Chamber of Account) is established by constitutional law as an institution independent of the executive, legislative and judicial branches. In order to guarantee its independence, the Auditor-General:

- ✓ Is appointed by parliament and has a clear term of office;
- ✓ Has the legal and practical means and resources to perform his/her mission independently;
- ✓ Has the independent authority to report to parliament and its budget committee on any matter of expenditure at any time.

Parliament should see to it that judicial sanctions are provided for by law and are applied in cases of corruption and mismanagement of state resources by officials and the political body. Parliament should also see to it that remedies are applied in case of fault.

Auditing Security and Intelligence Services

The objective of audit of the security and intelligence services is to certify that the expenditure is in compliance with law in an effective and efficient manner. To this extent, it is essential that the services are open to full scrutiny by the Auditor-General apart from limited restrictions to protect the identities of certain sources of information and the details of particularly sensitive operations.[13]

Precisely because the services function under the protection of secrecy, shielded from public scrutiny by the media and civil society watchdogs, it is important that the auditors have wide access to classified information. Only in this way, it can be certified whether the services have used public funds within the law or whether illegal practices, eg corruption, have occurred.

Box No. 55:
The Auditor General

"Regardless of whether it falls under the Executive, the Legislature or the Judiciary, it is imperative for the Audit Office to be completely independent and truly autonomous. It should also dispose of adequate resources to accomplish its mission. Its function is three-fold:

Financial Oversight
The Audit Office must verify the accuracy, reliability and thoroughness of the finances of all organs of the Executive and public departments. It must verify that all financial operations are carried out in accordance with the regulations on public funds. Within the context of this oversight function, the Audit Office must fulfil a mission of jurisdiction with regard to public accountants and officials who authorise payments. They must all be made accountable for the money they handle save in the case of a discharge or release of responsibility. In cases of misappropriation or corruption, the Audit Office is duty-bound to report its findings to the Judiciary.

Legal Oversight
The Audit Office must verify that all public expenditure and income are conducted in accordance with the law governing the budget.

Ensuring Proper Use of Public Funds
A modern Audit Office which functions in the interest of good governance should ensure the proper use of public funds on the basis of the three following criteria :

(i) *Value for money*: ensure that the resources used were put to optimal use, both qualitatively and quantitatively;
(ii) *Effective*: measures to what extent objectives and aims were met;
(iii) *Efficient*: measures whether the resources used were used optimally to obtain the results obtained.

This *ex-post* oversight is conducted on the initiative of the Audit Office or at the request of Parliament.

Excerpts from: General Report on the IPU Seminar on Parliament and the Budgetary Process, (Bamako, Mali, November 2001)

As a matter of a general principle of good governance, the normal rules of auditing which apply to other activities of government, should also apply to the audit of the expenditures of the services with some limited restrictions as mentioned above. What makes auditing security and intelligence services different from regular audits, are the reporting mechanisms. In order to protect the continuity of operations, methods and sources of the services in many countries special reporting mechanisms are in place. For example, in the UK, as far as the parliament is concerned, only the Chairman of the 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 expenditures, occurrence of possible irregularities, and whether the services have operated within or have exceeded the budget. In the case of Germany, the control of the accounts and the financial management of the intelligence services is carried out by a special institution (i.e. *Dreierkollegium*) within the national audit office (*Bundesrechnungshof*). The *Bundesrechnungshof* reports its

secret findings on the control of the accounts and the financial management of the intelligence services to a special sub-committee of the Parliamentary Budget Control Committee (i.e. the Confidential Forum), the Parliamentary Control Panel for intelligence oversight, the Federal Chancellery (*Bundeskanzlerarmt*) as well as to the Finance Ministry.[14] The parliament (i.e. not the intelligence services) decides which elements of the intelligence services' budget need to be secret.[15]
Furthermore, in many countries, the public annual reports of the security and intelligence service (eg in the Netherlands) or of the parliamentary oversight body (eg in the UK) include statements about the outcome of the financial audits.[16]

The box below illustrates how the disclosure of information about the services to the auditor can be arranged.

Box No. 56:
Statutory Disclosure of Information of the Services to the Auditor (UK)

'[T]he disclosure of information shall be regarded as necessary for the proper discharge of the Intelligence Service if it consists of (…) the disclosure, subject to and in accordance with arrangements approved by the Secretary of State, of information to the Comptroller and Auditor General for the purposes of his functions.'

Source: Intelligence Services Act 1994, Section 2(3)b, United Kingdom

It also happens in many countries that the audit office investigates the legality, effectiveness and efficiency of particular projects, such as the building of a new headquarters (eg in Canada and the UK) or the purchase of new SIGINT (Signal Intelligence) systems (eg in the UK) or the exchange of information between the services for coordinating anti-terrorism policy (the Netherlands). Box No. 58 gives an example of the mandate and scope of an investigation by the Canadian Auditor-General.

The national audit office does not function in a vacuum, but is embedded in an existing system of financial accountability procedures, provided for by law. Normally, laws on financial accountability in general and laws on intelligence services in particular, specify which normal and special accountability provisions apply. Box No. 57 gives an example of some of the financial accountability procedures of the Luxembourg intelligence services. The Luxembourg illustrates three significant elements of financial auditing systems. Firstly, the special accountant of the intelligence services is appointed by the relevant minister, and not by the director of the intelligence service. This provision puts the accountant in a strong position within the service and contributes to the independence of his office. Secondly, the mandate of the national audit office is to check periodically the way in which the services are managed from a financial point of view. This implies that the mandate goes beyond accessing and accounting for the legality of the expenditure and also includes consideration being given to the performance, efficiency and efficacy of the services in question.

Thirdly, the law stipulates that the Law on State Budget, Accountability and Treasury also applies to the intelligence services (except for some specific exemptions). Therefore, the objective of the law is to reach a situation where the normal practices of good financial management are applied as much as possible.

Box No. 57:

Financial Accountability (Luxembourg)

'(1) The expenditures of the Intelligence Services are carried out by the special accountant of the Intelligence Service, who is appointed by the minister in charge of the budget in accordance with the provisions of article 68 of the amended 8 June 1999 Law on State Budget, Accountability and Treasury.
(2) Exceptions to the provisions of article 68 - 73 of the aforementioned law are:

- The periodical control of the management of the Intelligence Service is done by the National Audit Office;
- The funds that are received by the special accountant are allocated to the payment of the expenditures of the Intelligence Service; and are recorded in the accounts of the special accountant;
- At the end of each trimester, the special accountant reports on the use of the funds to the official who has the power to authorise expenditures, within the timeframe that is indicated in the decision to allocate the funds;
- The funds which are not used for paying the expenditures during the fiscal year for which they are allocated, are not returned to the State Treasury. Instead, these funds are recorded in the Intelligence Service's attributes for the following fiscal year;
- The official who has the power to authorise expenditures, submits the special accountants' financial records to the National Audit Office for its approval;
- The National Audit Office submits the accounts, together with its observations to the Prime Minister, Minister of State;
- At the end of each fiscal year, the Prime Minister, Minister of State, offers the minister to whom the responsibility for the budget has been attributed, the option of discharging the special accountant from his functions. The discharge should be decided upon before 31 December of the fiscal year following the fiscal year to which the accounts of the special accountant refer to.'

Source: Loi du 15 juin portant organisation du Service de Renseignement de l'Etat, Article 7, Memorial - Journal Officiel du Grand-Duché de Luxembourg, A-No. 113 (unofficial translation)

Box No. 58:

Independent Audit of Projects: the Example of the National Headquarters Building Project of the Canadian Security and Intelligence Services (CSIS) by the Auditor General of Canada

'**Objectives:** The objectives of the audit were to determine whether the constructed national headquarters facility would meet the CSIS-stated objectives and the Treasury Board approvals, and whether the project was implemented with due regard to economy and efficiency.

Criteria: Our audit criteria were derived from our guide for auditing capital asset projects, as well as the appropriate Treasury Board policies and guidelines.

Scope: The audit examined all the major stages of this major Crown project. Specifically, we reviewed the needs definition, the options analysis, the project definition, the design and review process, the contracting process, change orders, project management, environmental assessment, commissioning and post-project evaluation. Our audit commenced in November 1995 and was completed in March 1996. Given the size and complexity of this project and the limited time available, we did not audit detailed financial records. (…) The audit did not address the CSIS mandate. However, in acquiring an understanding of the requirements for the facility, we confirmed that they were based on the existing mandate and were appropriate.

Approach: Audit evidence was collected through extensive interviews with the building project staff, and with CSIS staff as users of the building. We reviewed planning documents, submissions to the Treasury Board, project briefs, minutes of the Senior Project Advisory Committee meetings and project management meetings, correspondence, contract documents and annual reports. We inspected the building, from the roof to the basement, including the office space, special purpose space and building services space. We received a high level of cooperation (…). The level of cooperation is particularly noteworthy given the security considerations relative to CSIS operations and the facility itself.'

Source: 1996 Report of the Auditor General of Canada, available at http://www.oag-bvg.gc.ca

A cautionary note, however, is important. Security and intelligence services are not entirely comparable to other the business of government. For a number of reasons, the work involves a higher degree of risk, and, therefore, investments may go wrong due to factors outside the responsibility of the service. Elected representatives should treat the outcomes of the audits with great care. An unbalanced response to the reports of the auditor general or the leaking of its results could hurt the operations, harm the services' functioning, and, last but not least, might damage the trust between the political leadership and the leadership of the services.

Best Practice

- ✓ In order to guarantee the independence of the audit office, its operation should be based on law, it should report to parliament and the director of the audit office should be appointed or confirmed by parliament;
- ✓ The law on audit offices should include provisions on the office's mandate, reporting mechanisms, the appointment of the director as well as on access to classified information;
- ✓ The auditor-general should have full access to classified information, with specific restrictions in order to protect the identity of sources and sensitive operations;
- ✓ The statutory audit offices should be able to conduct not only financial audits but also performance audits of specific projects in detail;
- ✓ As the audit offices are dealing with classified information, safeguards should be put in place to avoid unauthorised publication of (parts of) audits.

Endnotes Section V - The Role of External Review Bodies

1. German *Bundestag* Secretariat of the Parliamentary Control Commission (PKGR), *Parliamentary Control of the Intelligence Services in Germany*,(Berlin: *Bundespresseamt*, 2001), pp. 19-20.
2. *Windisch v Austria*, (1991) 13 European Human Rights Reports 291; *Van Mechelen v Netherlands*, (1998) 25 European Human Rights Reports 647, *Teixeira de Castro v Portugal*, European Court of Human Rights, Judgment of 9 June 1998.
3. *Rowe and Davis v UK*, (2000), 30 European Human Rights Reports 1; *Tinnelly and McElduff v UK*, E Ct HR, Judgment, 10 July 1998.
4. *Chahal v UK,* (1997) 23 E.H.R.R. 413; *Tinnelly and McElduff* v *UK*, (1999) 27 E.H.R.R. 249.; *Edwards and Lewis v UK*, European Court of Human Rights, Judgment 22 July 2003 and 27 October 2004.
5. *Klass v Germany*, para. 15 (as regards Art. 8); *Leander v Sweden*, para. 68 (as regards Art. 13).
6. *Leander v Sweden, para. 78.*
7. **'**Report on the Feasibility of Recommendations on Internal Security Services', adopted by the *PC-S-SEC* at its second meeting (9 - 11 October 2002), p. 15.
8. For comparison of the powers of Inspectors-General in different countries, see: Intelligence and Security Committee (UK), *Annual Report for 2001-2*, Cm 5542, Appendix 3.
9. CSIS Act, s. 33.2. Both the Service's Annual Report and the Inspector-General's certificate are required to be sent to the oversight body, SIRC.: s. 33.3 CSIS Act 1984.
10. Office of the Inspector General of Intelligence.
11. Inspector-General of Security and Intelligence Act 1986, sections 10-12.
12. See, for example, Law of the Intelligence and Security Agency of Bosnia Herzegovina, Article 32:
    'An Inspector General shall be appointed and dismissed by the Council of Ministers upon the proposal of the Chair. The Inspector General shall serve a four-year term, which may be renewed once. The Inspector General may be dismissed before the expiration of his/her mandate upon his/her own request; if s/he permanently loses the capacity to execute his/her duties; fails to comply with applicable legislation or regulations; fails to implement measures for supervision of the Agency; if criminal proceedings for the criminal offences of abuse of office or disclosing a State, military or official secret have been instituted against him/her; if a final imprisonment sentence for a criminal offence which makes him/her unworthy of executing such duties is rendered against him/her; or if s/he fails to conduct an investigation, inspection or audit in a timely and lawful manner.'
13. These restrictions apply to the UK Comptroller and Auditor-General, see Report by the Comptroller and Auditor-General, *Thames House and Vauxhall Cross,* HC Session 1999-2000, 18 February 2000, point 8. Available at:
    http://www.nao.org.uk/publications/nao_reports/9900236.pdf
14. German *Bundeshaushaltsordnung* (BHO) (1969), Para. 10a (3); Secretariat of the German Parliamentary Control Panel, *Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland – Materialien*, (Berlin: Bundestag, 2003), p. 42; Website of the German Intelligence Service (*Bundesnachrichtendienst*) at:>http://www.bundesnachrichtendienst.de/auftrag/kontrolle.htmBundeshaushaltsordnung>.
15. German Bundeshaushaltsordnung (BHO) (1969), Para. 10a (2).
16. See, for example, Annual Report of the General Security and Intelligence Services of the Netherlands (2003), available at:
    <http://www.minbzk.nl/contents/pages/9459/annual_report_2003_aivd.pdf>, pp. 69-70; Intelligence and Security Committee Annual Report 2002-2003, presented to parliament by the Prime Minister by Command of Her Majesty, June 2003, London, pp. 8-13.

Overview of Best Practice

The Agency

Defining the Mandate

- ✓ The role of a security or intelligence agency should be clearly defined and limited to matters which should be specified in detail and involve serious threats to national security and the fabric of civil society;
- ✓ The concepts of threats to national security and the fabric of civil society should be legally specified;
- ✓ The territorial competence of a security or intelligence agency should be clearly defined and any powers to act outside the territory should be accompanied by safeguards;
- ✓ The tasks and powers of the agency within its mandate should be clearly defined in legislation, enacted by parliament;
- ✓ Especially in post-authoritarian states, it is important to have legal and institutional safeguards in place, preventing the misuse of security and intelligence against domestic political opponents.

Appointing the Director

- ✓ Legislation should establish the process for the appointment of the Director of a security or intelligence agency and any minimum qualifications or any factors which are disqualifications from office;
- ✓ The appointment should be open to scrutiny outside the executive, preferably in parliament;
- ✓ Preferably, the opposition in parliament should be involved in appointing the Director;
- ✓ Legislation should contain safeguards against improper pressure being applied on the Director and abuse of the office (for example provisions for security of tenure, subject to removal for wrongdoing);
- ✓ The criteria for appointment and dismissal should be clearly specified by the law;
- ✓ Preferably, more than one cabinet member should be involved in the process of appointing a Director, eg the head of state/prime minister and the relevant cabinet minister.

Authorising the use of special powers

- ✓ It is a requirement of the rule of law that any special powers that the security or intelligence services possess or exercise must be grounded in legislation.
- ✓ The law should be clear, specific and also comprehensive, so that there is no incentive for an agency to resort to less regulated means;
- ✓ The principle of proportionality should be embedded in legislation governing the use and oversight of special powers;
- ✓ There should be controls against the misuse of special powers involving persons outside the agency, both before and after their use;
- ✓ All actions taken by security and intelligence services to fight terrorism should respect human rights and the principle of the rule of law. Whatever the acts of a person suspected or convicted of terrorist activities, intelligence services may never derogate from the right to life as guaranteed by the ECHR and the International Covenant of Civil and Political Rights (ICCPR);
- ✓ In order to safeguard against arbitrary use of special powers and violations of human rights, the agency's actions must be subject to appropriate supervision and review.

Information and Files

- ✓ The legislative mandate of the security and intelligence agencies should limit the purposes and circumstances in which information may be gathered and files opened in respect of individuals to the lawful purposes of the agency;
- ✓ The law should also provide for effective controls on how long information may be retained, the use to which it may be put, and who may have access to it and shall ensure compliance with international data protection principles in the handling of disposal information. There should be audit processes including external independent personnel to ensure that such guidelines are adhered to;
- ✓ Security and intelligence agencies should not be exempted from domestic freedom of information and access to files legislation. Instead they should be permitted, where relevant, to take advantage of specific exceptions to disclosure principles referring to a limited concept of national security and related to the agency's mandate;
- ✓ The courts or whatever other independent mechanism is provided under the legislation should be free to determine, with appropriate access to sufficient data from the agency's files, that such exceptions have been correctly applied in any case brought by an individual complainant;
- ✓ Where information is received from an overseas or international agency, it should be held subject both to the controls applicable in the country of origin and those standards which apply under domestic law;
- ✓ Information should only be disclosed to foreign security services or armed forces or to an international agency if they undertake to hold, and use it subject to the same controls as apply in domestic law to the agency which is disclosing it (in addition to the laws that apply to the agency receiving it).

Internal Direction and Control of the Agency

- ✓ Intelligence services should not be beyond the law. Therefore staff who suspect or become aware of illegal actions and orders within the services should be under a duty to report their suspicions;
- ✓ A codified practice should be in place which guarantees appropriate support and security for whistleblowers;
- ✓ Intelligence Services staff should be trained to a code of conduct which includes consideration of the ethical boundaries to their work. This training should be kept up to date and available to staff throughout their tenure;
- ✓ Internal administrative policies should be formalised with a clear legal status.
- ✓ Matters too detailed or sensitive to appear in legislation should be governed by formal internal administrative policies with a clear legal status.

The Role of the Executive

Ministerial Knowledge and the Control of Intelligence

- ✓ Intelligence legislation should contain two distinct rights of access: the right of the executive to relevant information in the hands of the agency and the right of the agency heads to have access to the respective minister;
- ✓ The Minister should be legally responsible for the formulation of policy on security and intelligence matters. He should also be legally entitled to receive agency reports at regular intervals as well as being legally responsible for the approval of matters of political sensitivity.

Control over Covert Action

- ✓ All covert action shall be approved by the responsible member of the executive according to a legal framework approved by parliament. Regular reports shall be made;
- ✓ No action shall be taken or approved by any official as part of a covert action programme which would violate international human rights.

International Co-operation

- ✓ It is essential that international cooperation should be properly authorised by ministers and should be subject to minimum safeguards to ensure compliance with domestic law and international legal obligations;
- ✓ Legal safeguards should be incorporated to prevent the use of intelligence sharing in a way that circumvents non-derogable human rights standards or controls in domestic law.

Safeguards against Ministerial Abuse

- ✓ Intelligence legislation should include safeguards against ministerial abuse and the politicisation of intelligence services. Various possible safeguarding mechanisms are imaginable, such as the requirement that all ministerial instructions be put in writing and/or disclosed to an external review body as well as the ministerial requirement to brief the Leader of the Opposition;
- ✓ Intelligence Services should not take any action to further the interests of a political party;
- ✓ Intelligence Services should not be allowed to investigate acts of protest, advocacy or dissent that are part of the democratic process and in accordance with the law.

The Role of Parliament

The Mandate of Parliamentary Oversight Bodies

- ✓ Horizontal scope of the mandate: the entire intelligence community, including all ancillary departments and officials, should be covered by the mandate of one or more parliamentary oversight bodies;
- ✓ Vertical scope of the mandate: the mandate of a parliamentary oversight body might include some or all of the following (a) legality, (b) efficacy, (c) efficiency, (d) budgeting and accounting; (e) conformity with relevant human rights Conventions (f) policy/administrative aspects of the intelligence services;
- ✓ All six aspects mentioned above should be covered by either the parliamentary oversight body or other independent bodies of the state, eg national audit office, inspectors-general, ombudsman or court. Overlap should be avoided;
- ✓ The bigger an intelligence community is and the more different intelligence services are involved, the greater is the need for specialised parliamentary oversight (sub)committees;
- ✓ The mandate of a parliamentary oversight body should be clear and specific;
- ✓ The recommendations and reports of the parliamentary oversight body should be (a) published; (b) debated in parliament; (c) monitored with regard to its implementation by the government and intelligence community;
- ✓ The resources and legal powers at the disposal of the parliamentary oversight body should match the scope of its mandate.

The Composition of a Parliamentary Oversight Body

- ✓ Parliamentary oversight bodies should be clearly 'owned' by parliament;
- ✓ Parliament should be responsible for appointing and, where necessary, removing members of a body exercising the oversight function in its name;
- ✓ Representation on parliamentary oversight bodies should be cross-party, preferably in accordance with the strengths of the political parties in parliament;
- ✓ Government ministers should be debarred from membership (and parliamentarians should be required to step down if they are appointed as ministers) or the independence of the committee will be compromised. The same applies to former members of agencies overseen;
- ✓ Committee members should have security of tenure at the pleasure of parliament itself, rather than the head of government;
- ✓ The chairman should be chosen by the parliament or by the committee itself, rather than appointed by the government.

Vetting and Clearance of the Oversight Body

- ✓ Members of parliament should only be vetted if the committee's mandate includes dealing with operationally sensitive material;
- ✓ Where clearance is denied to members of parliament by the security and intelligence services, procedures should be established to deal with disputes authoritatively, giving the final decision to the parliament or its presidium;
- ✓ The criteria for vetting should be clear, public, consistent and robust in order to withstand democratic scrutiny.

Parliamentary Powers to Obtain Information and Documents

- ✓ The oversight body should have the legal power to initiate investigations;
- ✓ Members of oversight bodies should have unrestricted access to all information which is necessary for executing their oversight tasks;
- ✓ The oversight body should have power to subpoena witnesses and to receive testimony under oath;
- ✓ Where relevant to the oversight body's remit, the executive should have responsibility for keeping the oversight body informed;
- ✓ The oversight body should take appropriate measures and steps in order to protect information from unauthorised disclosure;
- ✓ Disputes over access to information between the agencies and the oversight body should be referred in the last analysis to the Parliament itself.

Reporting to Parliament

- ✓ Primary responsibility for the timing and form of the Parliamentary Committee's Report and any decision to publish evidence should lie within the committee itself;
- ✓ The committee should report to parliament at least yearly or as often as it deems necessary;
- ✓ The parliamentary oversight body should have the final word on whether it is necessary to remove material from a public report for security reasons;
- ✓ The government and the agencies should be given prior sight of the draft report so that representations about necessary security deletions can be made.

Budget Control

- ✓ The oversight body should have access to all relevant budget documents, provided that safeguards are in place to avoid leaking of classified information;
- ✓ The oversight of the budget of the security and intelligence services should be governed by the same principles of good governance which regulate other activities of government. Exceptions should be regulated by law. From this

point of view, the oversight of the budget should be a shared power between the appropriations committee and the intelligence oversight committee;

- ✓ Powerful parliaments should have the right to authorise the budget;
- ✓ Intelligence Agencies should only use funds for activities if those funds were specifically authorised by the legislative branch for that purpose;
- ✓ The intelligence services should not be allowed to transfer funds outside the agency without the authorisation of the legislature.

The Role of External Review Bodies

Resolving Citizens' Grievances

- ✓ The official or tribunal hearing the complaint should be persons who fulfil the constitutional and legal requirements to hold an office at this level and should enjoy legal security of tenure during their term of office;
- ✓ As much of the process as possible should be completed in public. Even where the process is closed to the public as much of it as possible should be open to the complainant and his or her legal representatives;
- ✓ There should be a power to dismiss without investigation complaints that the official or tribunal concludes are vexatious or frivolous;
- ✓ If it is necessary for reasons of national security to restrict the participation of a complainant in the review process then the decision to do should be in the hands of the reviewing official or tribunal alone and compensating safeguards (such as the use of a 'Devil's Advocate' or 'Special Counsel') should be provided to ensure that proceeding are fair and impartial;
- ✓ The tribunal or official should have power to make legally binding orders which provide an effective remedy to a complainant who has a justifiable case. These may include the award of compensation and the destruction of material held by the security or intelligence agencies;
- ✓ The scope of review and grounds of review should be clearly established in law and should extend to the substance (rather than merely procedural aspects) of the actions of the security or intelligence agencies.

Oversight of Agencies within the Administration by Independent Authorities

- ✓ Review of the functions of the security and intelligence agencies affecting individuals should be by independent and impartial officials (such as Ombudsmen, or Inspectors-General) and comply with the following standards;
- ✓ The official who acts as a reviewer should be a person who fulfils the constitutional and legal requirements to hold an office at this level and should enjoy legal security of tenure during their term of office;
- ✓ The scope of review and grounds of review should be clearly established in law and should extend to the substance (rather than merely procedural aspects) of the actions of the security or intelligence agencies;
- ✓ The official should have sufficient legal powers to be able to review matters of fact and evidence relating to the use of powers of the security or intelligence agencies;
- ✓ The official should have ultimate authority to determine the form and scope of any order or report or decision which results from the process.

Independent Audit Offices

- ✓ In order to guarantee the independence of the audit office, its operation should be based on law, it should report to parliament and the director of the audit office should be appointed or confirmed by parliament;
- ✓ The law on audit offices should include provisions on the office's mandate, reporting mechanisms, the appointment of the director as well as on access to classified information;
- ✓ The auditor-general should have full access to classified information, with specific restrictions in order to protect the identity of sources and sensitive operations;
- ✓ The statutory audit offices should be able to conduct not only financial audits but also performance audits of specific projects in detail;
- ✓ As the audit offices are dealing with classified information, safeguards should be put in place to avoid unauthorised publication of (parts of) audits.

Contributors

Authors

Dr. Hans Born
Senior Fellow, Geneva Centre for the Democratic Control of Armed Forces, Geneva, Switzerland.

Professor Ian Leigh
Professor of Law, Co-Director of the Human Rights Centre, Durham University, Durham, United Kingdom.

Editorial Assistants

Mr. Thorsten Wetzling
Research Assistant, Geneva Centre for the Democratic Control of Armed Forces, Geneva, Switzerland.

Ms. Ingrid Thorburn
Research Assistant, Geneva Centre for the Democratic Control of Armed Forces, Geneva, Switzerland.

Members of the Advisory Board
(in their private capacity)

Dr. Fredrik Sejersted
Attorney at Law, Office of the Attorney-General, Oslo, Norway.

Mr. Fred Schreier
Senior Consultant, Geneva Centre for the Democratic Control of Armed Forces, Geneva, Switzerland.

Consultees
(in their private capacity)

Dr. Andrew Butler
Crown Law, Wellington, New Zealand.

Ms. Marina Caparini
Senior Fellow, Geneva Centre for the Democratic Control of Armed Forces, Geneva, Switzerland.

Dr. Richard B. Doyle
Associate Professor of Public Budgeting, Naval Postgraduate School, Monterey, USA.

Dr. Willem F. van Eekelen
President of the Advisory Board of the Centre for European Security Studies at the University of Groningen, Member of the Advisory Boards of the Geneva Centre for the Democratic Control of Armed Forces and of the Stockholm Institute Peace Research Institute, former Member of the Netherlands' Senate, former Minister of Defence of the Netherlands and former Secretary-General of the Western European Union.

Prof. Dr. Peter Gill
Professor of Politics and Security at Liverpool John Moores University, United Kingdom.

Mr. George B. Lotz II
Assistant to the Secretary of Defense for Intelligence Oversight, Washington DC, USA.

Dr. Barry R. Wickersham
Director of Training, Office of the Assistant to the Secretary of Defense for Intelligence Oversight, Washington DC, USA.

Glossary

Accountability
The liability of representatives, whether elected or appointed, to be called to account in the exercise of their powers and duties. This applies equally for employees of intelligence and security services. It has the political purpose of checking the power of the executive and therefore minimising any abuse of power and the operational purpose to help to ensure that governments operate effectively and efficiently.

Checks and Balances
This concept describes constitutionally and legally derived mechanisms applied to the process of decision-making which are aimed at preventing one-party domination. With regard to the oversight of intelligence services, it means that the executive, the judiciary and the legislature each play their distinct role in the process of intelligence accountability. *See Democratic Control of the Security Services.*

Civil Society
Civil society refers to the set of institutions, organisations and behaviour situated between the state, the business world, and the family. Specifically, this includes voluntary and non-profit organisations, philanthropic institutions, social and political movements, other forms of social participation and engagement, and the values and cultural patterns associated with them.

Classified Information
A category to which national security information and material is assigned to denote the degree of damage that unauthorised disclosure would cause to national defence or foreign relations, and to denote the degree of the protection required. The desired degree of secrecy about such information is known as its sensitivity. It is often the case that sensitive information is disseminated on a need-to-know basis. The following US example demonstrates a formal hierarchy of classification for information: (i)*Top secret* – this is the highest security level, and is defined as information which would cause 'exceptionally grave damage' to national security if disclosed to the public; (ii) *Secret* – the second highest classification may include, for example, details of other security measures and procedures. It is defined as information which would cause 'serious damage' to national security if disclosed; (iii) *Confidential* – is the lowest classification level. It is defined as information which would "damage" national security if disclosed. Additional categories might be added such as (iv) *Sensitive but unclassified (SBU)* – data which is not related to national security but whose disclosure to the public could cause some harm; (v) *Unclassified* – not technically a 'classification', this is the default, and refers to information that is not sensitive and can be freely disclosed to the public. *Declassification* of information can happen if information becomes out of date or if an authorised body demands declassification for reasons of public interest.

Complaint
An individual or collective communication to a control body drawing attention to an alleged violation of human rights.

Democracy
Representation of the people, by the people and for the people. Marked by free elections, the rule of law, separation of power and respect for basic human rights. *See Human Rights.*

Democratic Accountability of Intelligence Services
Although secrecy is a necessary condition of intelligence services' work, intelligence in a liberal democratic state needs to work within the context of the rule of law, checks and balances, and transparent lines of responsibility. Democratic accountability of intelligence services thus identifies the propriety and determines the efficacy of intelligence services under these parameters. This involves five distinct yet interdependent pillars: (1) executive control; (2) parliamentary oversight; (3) judicial review; (4) independent oversight on behalf of the general public; and (5) internal control by the intelligence services.

Director of Intelligence
Tasked by the relevant minister, the director of an intelligence service is responsible *inter alia* for the control and management of the service, the timely fulfilment of its missions, the provision of leadership and political guidance for the services.

Executive Control / Ministerial Control
The executive exercises direct control over the intelligence services from the central, regional or local levels of government. It determines the budget, general guidelines and priorities of the activities of the intelligence services. In order to guarantee effective executive control, ministers need access to relevant information in the hands of the agency or to assessments based upon it through intelligence assessments and to be able to give a public account where necessary about the actions of the intelligence services. The exercise of external control is facilitated by the work of special offices or bodies such as Intelligence Coordination Commissioners, Intelligence Supervisory Boards, Policy Review Committees and Audit Offices who report directly to the responsible ministers.

Good Governance
The core elements of 'good governance' necessitate that government is people-centred, equitable, accountable, transparent, engenders participation and consultation in planning and decision-making, is effective and efficient in public sector management, and actively seeks and facilitates the involvement of civil society (World Bank).

Human Rights
Any basic right or freedom to which all human beings are entitled and in whose exercise a government may not interfere (including rights to life and liberty, freedom of thought and expression and equality before the law such as are contained in the main International Human Rights treaties eg the Universal Declaration on Human

Rights (UNDHR), The International Covenant on Economic, Social and Cultural Rights (ICESCR), The International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights (ECHR) and other regional schemes eg the African Charter on Human and Peoples' Rights., the American Convention on Human Rights and Asian Human Rights Charter.

Independent Oversight
One of the five distinct pillars of intelligence accountability is independent oversight. Within the framework of this publication, independent oversight over the intelligence services is carried out by institutions whose independence is secured by law as well as special reporting and appointment mechanisms. Examples of independent oversight institutions are national audit office, ombudsman, tribunals or independent inspector-generals. *See Civil Society and Think Tank.*

Intelligence
Governments collect, process and use information. Part of statecraft is 'the central importance of knowing, both in general and in particular' (John Keegan). Intelligence in government usually has a restricted meaning – it has particular associations with international relations, defence, national security and secrecy, and with specialised institutions labelled 'intelligence' (Michael Herman). Intelligence can be described as 'a kind of knowledge', 'the type of organisation which produces the knowledge' and the 'activity pursued by the intelligence organisation' (Sherman Kent). Intelligence in government is based on the particular set of organisations with the name: the 'intelligence services'. Intelligence activity is what they do, and intelligence knowledge is what they produce (Michael Herman).

Intelligence Control versus Intelligence Oversight versus Intelligence Review
To have control means to be in charge, responsible, capable of managing and influencing a given intelligence task. Oversight is a more general concept than control as it does not imply that a supposed 'overviewer' is in charge or has the capacity to affect either decision-making or outcomes. Review is done by *ex post facto* monitoring the intelligence services' work and the legal status of their actions.

Inspector-General
In general, the term Inspector-General is used for a military or civilian government official responsible for investigations. Within the realm of intelligence, the Inspector-General is appointed and entrusted by the executive to perform a broad range of different tasks such as to monitor compliance by the intelligence services with the law and government policies and priorities as well as to review the activities of the intelligence services; and to submit regular reports to the executive (or in some schemes, to Parliament).

Internal Control
To ensure the compliance of intelligence service officers with the standards of democratic rule, a complex system of safeguard mechanisms within the intelligence services should be in place. A Code of Conduct and a book of rules should apply to intelligence officers. Furthermore, in order to prevent the abuse of intelligence, every employee should be trained in how to deal with an illegal order by a superior. A

special body within the intelligence services should coordinate and control the proper functioning of internal control of intelligence.

Judicial Review
Judicial review is understood differently within various constitutional systems. Within legal systems possessing a Constitutional Court and a written constitution it frequently includes the power of a court to review a law or an official act of a government employee or agent for constitutionality. The court has the power to strike down that law, to overturn the executive act or order a public official to act in a certain manner if it believes the law or act to be unconstitutional. Within the UK it refers to the ability of the courts to declare actions of governmental bodies to be contrary to law or in violation of the European Convention on Human Rights. It is used here in the narrower sense of the ability of the courts to judge the legality of the actions of intelligence agencies or ministers including, where this applies, their constitutionality.

Law Enforcement Surveillance versus Intelligence Surveillance
Law enforcement surveillance is primarily perceived as a mechanism for obtaining evidence of criminal activities by identified suspects, whereas intelligence surveillance is primarily seen as a mechanism for gathering intelligence on more nebulous threats to national security not necessarily connected to criminal activities, or at least, specific criminal offences. The mandate of the intelligence agencies to engage in surveillance is usually framed in a less clear way and with more room for speculative 'fishing expeditions' and correspondingly less protection of the human rights of the targets. The time limits are usually more lenient, with most intelligence operations being conducted for much longer periods than law enforcement operations (Cameron, I.; see also Brodeur, J-P. and Gill, P.).

Legality
Nullum crimen, nulla poena sine lege, also known as the principle of legality, stipulates that certain criminal conduct is punishable only: (i) if at the time of that conduct there was a valid rule characterising the conduct as criminal, and (ii) if, at that time, there existed rules establishing, in relation to such conduct, a reasonably precise scale of punishments.

Legitimacy
The legitimacy of a rule, or of a rule-making or rule-applying institution, is a function of the perception of those in the community concerned that the rule, or the institution, has come into being endowed with legitimacy, that is, trusted, valued and respected.

Ombudsman
An institution whose function is to examine and report on complaints made by ordinary people about the government or public authorities. In order to guarantee its independence from the executive and its secret services, in many countries the ombudsman is appointed by and reports to parliament.

Parliamentary Oversight
The legislature exercises parliamentary oversight by passing laws that define and regulate the intelligence and security services and their powers and by adopting the corresponding budgetary appropriations. At the legislative level there should exist

mechanisms by which parliamentarians can call to account the officials in charge of the intelligence services. These mechanisms should include:

(i) a well-functioning parliamentary committee for intelligence oversight;
(ii) the possibility to control the budget of the services;
(iii) powers to retrieve (classified) information from the government and services;
(iv) access to classified information;
(v) the possibility to commission experts from civil society;
(vi) clear and effective reporting mechanisms between parliament, government, services, and society at large;
(vii) the possibility to initiate hearings;
(viii) the possession of investigative powers

Proportionality
The proportionality requirement has three aspects: (i) the existence of a rational connection between the impugned measure and the objective; (ii) minimal impairment of the right or freedom, and; (iii) a proper balance between the effects of the limiting measure and the legislative objective (Supreme Court of Canada). The European Convention on Human Rights uses the principle of proportionality as an interpretive device designed to restrain the power of state authorities and to provide greater protection to individual autonomy.

Quality of Law Test
In a democratic society, some human rights such as the right to privacy, freedom of thought, conscience and religion, freedom of expression, and the freedom of assembly and association can be limited, among others, in the interest of national security and public order. As regards the European context, the European Convention on Human Rights (ECHR) prescribes that these limitations have to be made in 'accordance with the law'. Case law of the European Court of Human Rights (ECtHR) says, *inter alia*, that security and intelligence services can only exercise their special powers if they are regulated by the law. The following conditions must be fulfilled to qualify as 'law' under the quality of law test:
(i) a norm must be adequately accessible and formulated with sufficient precision to enable the citizen to regulate his conduct;
(ii) a rule needs to possess the essential characteristics of foreseeability and must not allow the exercise of unrestrained discretion;
(iii) a rule must at least set up the conditions and procedures for interference.

Rule of Law
Legislation – including human rights legislation – must be created and mandated by a democratically legitimate government and enforced and systematically applied by an independent judiciary with coercive powers. The rule of law is an essential precondition for accountability in both the public and the private sectors. The establishment and persistence of the rule of law depends on clear communication of the rules, indiscriminate application, effective enforcement, predictable and legally enforceable methods for changing the content of laws and citizens who perceive the set of rules as fair, just and legitimate, and who are willing to follow them.

Security
Security is often thought of in the sense of national security, ie the absence of threats or perceived threats to specific values of a nation. In addition, according to both 'critical' and 'human' security approaches, security is about attaining the social, political, environmental and economic conditions conducive to a life of freedom and dignity for the individual.

Subpoenas
If a parliamentary oversight committee is vested with subpoena powers it possesses the authority to compel the attendance of a person before it (in a hearing).

Think Tanks
A think tank is an organisation that serves as a centre for research and/or analysis of important public issues. As civil society institutions, think tanks play a number of critical roles, including:
(i) playing a mediating role between the government and the public;
(ii) identifying, articulating, and evaluating current or emerging issues, problems or proposals;
(iv) transforming ideas and problems into policy issues;
(v) serving as an informed and independent voice in policy debates;
(vi) providing a constructive forum for the exchange of ideas and information between key stakeholders in the policy formulation process (James McGann).
Basically, think tanks provide the public with alternative information to that provided by the government.

Transparency
The construction of institutions, networks and routines in government and government agencies which lend themselves to systematic scrutiny by parliamentary and other institutions and individuals diffused across the social and economic spectra of civil society.

Vetting & Clearance
Vetting is required for people that may take certain jobs or carry out particular tasks that need security clearance. These jobs and tasks can be found at all governmental levels and the entire national security decision-making apparatus including the intelligence services, the ministries of defence and the armed forces. In addition, it might include the members of a Parliamentary Oversight Committee. Notably, not all parliaments make their members of intelligence oversight committee subject to vetting procedures by intelligence services, as it might signify the subordination of parliament to the executive branch of government. Clearance refers to the outcome of a successful vetting process, which clears an individual to different levels of classified information. See *classified information.*

Whistle-Blowing
Whistle blowing takes place when an employee discloses that an employer is breaking the law, acting unethically or contrary to an announced policy. Many countries have recognised the importance of such disclosures and have adopted legal protections for whistle-blowers to protect them from sanctions, whether in their employment or by prosecution. To whistle blow, an employee must tell of the illegal or

unethical act to someone outside the agency. Usually it must be a government or law enforcement agency. If the employee merely complains to someone inside the company or agency, that is not whistle blowing, and the employee is not protected by the whistleblower laws. Disclosures direct to the news media are usually not protected. Disclosures to relevant parliamentarians may be.