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.