Strasbourg, 15 December 2015

CDL-AD(2015)010
Or. Engl.

Studies no. 388 / 2006 and no.719/2013

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

REPORT
ON THE DEMOCRATIC OVERSIGHT OF THE SECURITY SERVICES

Adopted by the Venice Commission
at its 71st Plenary Session
(Venice, 1-2 June 2007)

On the basis of comments by

Mr Iain Cameron (Substitute member, Sweden)
Mr Olivier Dutheillet de Lamothe (Substitute member, France)
Mr Jan Helgesen (Member, Norway)
Mr Valery Zorkin (Member, Russian Federation)
Mr Ian Leigh (Expert, United Kingdom)
Mr Franz Matscher (Expert, Austria)

Updated by the Venice Commission
at its 102nd Plenary Session
(Venice, 20-21 March 2015)

On the basis of comments by

Mr Iain Cameron (Member, Sweden)

TABLE OF CONTENTS

Executive Summary

The need to control security services

1. The maintenance of the internal and external security of the State is vital and essential for the protection of the other values and interests of the State. In order to anticipate, prevent or protect itself against threats to its national security, a State needs effective intelligence and security services: intelligence is thus an inescapable necessity for modern governments.

2. Security agencies are expected to collect as much information as possible on threats to the State; this involves collecting information on individuals. Security services therefore, by their very nature, impinge on individual rights. It is therefore essential that there be internal limits as well as external limits to their activities.

3. In addition, the terrorist threats of the post 9/11 era have brought about new security challenges. Intelligence is one of the main weapons the State has in the struggle against terrorism and the spread of weapons of mass destruction. A transnational and network-based response from the States is necessary, and inter-agency co-operation must be enhanced. A tighter democratic control, and a different kind of control, is nowadays necessary.

4. Security services naturally receive instructions from the government. They need to be adequately *controlled* by the executive in order to avoid that they develop a "State within the State" mentality. Indeed, they are, and must be, equipped with considerable technological tools and enjoy exceptional powers. They have a natural tendency to over-collect information, and the individuals must be protected against an abusive or illegitimate use of the information collected about them.

5. Security services have inbred in them a potential of abuse of State power. The subjectivity and flexibility of the notion of "national security", combined with its vital importance to the State, mean that governments have a wide margin of manoeuvre in this area. They could be tempted to use the security services to pursue illegitimate aims. It is thus necessary to establish mechanisms to prevent political abuse, while providing for effective governance of the agencies.

Accountability

6. Security services must be "accountable". A working definition of accountability is "being liable to be required to give an account or explanation of actions and, where appropriate, to suffer the consequences, take the blame or undertake to put matter right, if it should appear that errors have been made".

7. In simplified form, four different forms of State accountability can be identified:
   - parliamentary accountability
   - judicial accountability
   - expert accountability
   - complaints mechanisms.

   The latter two forms are supplements or replacements for the first two forms of accountability.

8. Making secret services accountable presents special problems. A large degree of secrecy must accompany national security policy and operations, which increases the government control at the expense of the legislative power, and insulates the former from criticism.

9. Control even by government is made difficult by the very nature of the work of the secret services: the government is dependent on the special knowledge of the experts.

10. Control by the courts becomes then even more important, but the ordinary courts, to the extent their formal competence to review decisions in this field is not blocked by procedural devices (immunity, secrecy of documentation etc), are often faced with great difficulties reviewing in practice the large discretion which is given to the government in this area.

11. Monitoring the assessment of intelligence is a difficult exercise in itself, given that what needs to be checked is not only hard data (purely factual information) but also and more importantly subjective assessments as to whether facts or people constitute a present or future threat to national security.

12. A variety of patterns for organizing the internal security function exists. A single agency can be given this function or it can be split between different agencies and/or the police. The organisational context determines the actual power or influence of the agency.

13. As concerns the form of the mandate, it is greatly preferable that the primary rules be in statute form. It is essential, at any rate, that the norms concerning the internal security services be as clear and concise as possible and that they be kept secret only to the extent that it is absolutely necessary.

14. The content of the mandate can vary considerably from State to State, depending on the security priorities, determined by socio-political factors, and the character, more or less "proactive", of the tasks allocated to the security services.

15. Internal control of security services is exercised by the security agency over itself and by the way of the administrative control exercised by the hierarchical superior permanent civil servants in government departments to which the agency is subordinated. Internal control is the primary guarantee against abuses of power, when the staff working in the agencies is committed to the democratic values of the State and to respecting human rights. Different mechanisms exist for strengthening internal control, e.g. the quality of the staff (which can be improved by e.g. recruitment and training); the existence of an independent official designed to oversee the agency on the behalf of the government (an Inspectors-General), clear internal rules on delegation of, and responsibility for, decision-making and expenditure, financial auditing.

16. A precondition of effective parliamentary oversight is adequate governmental control. However, strengthening governmental control over an agency carries with it the risk of political manipulations and abuse. Certain mechanisms may lower this risk, e.g. security of tenure of the agency head; legal limits to what agencies can do, independent mechanisms for raising concerns about abuses, proper documentation of political directives ("paper trails").

17. International cooperation between Intelligence Agencies is increasingly necessary to fight terrorism, but often involves even more secrecy, hence raising issues of accountability. International exchanges of intelligence can escape the existing national mechanisms of control.

Parliamentary Accountability

18. The ultimate legitimacy and authority of security agencies should be derived from legislative approval of their powers, and parliamentary accountability is designed to avoid political abuse and ensure the appropriate use of public money. Parliamentary oversight also carries with it dangers: lack of expertise and professionalism on the part of parliamentarians; leaks to the press or the public of sensitive material. The possibility for the security agency to withhold or conceal information from an "amateur" investigator means that parliamentary questions or ad hoc parliamentary commissions of inquiry usually are only of limited efficacy in this field.

19. In presidential regimes, where the President has control over internal security matters, an antagonistic relationship with the parliament may arise.

20. The remit of a parliamentary oversight body may vary (policy, operations, questions of legality, effectiveness, respect for human rights). When it extends to operations, however, the oversight body must refrain from disclosing certain operational detail to the rest of the parliament and to the public. Access to operational details will often be "ex post", but it is difficult to establish when the operation has ceased, and the ongoing nature of intelligence operation may be used as an excuse if mutual trust is lacking between the agency and the oversight body. When its remit extends beyond mere policy, the oversight body should have at least a residual investigative capability of its own, (meaning that it should have some staff) and should also have access to information and documents from experts.

21. As concerns the staff of the oversight body, these need to possess adequate expertise. This means that these will normally have previously served in intelligence-related functions.

22. Additionally or alternatively, the oversight body might be assisted by an Inspector General to investigate a particular issue and report back to it.

23. An oversight body which reports to parliament should be able to decide when and how often to report. It should also be able to decide the content of the report, but should be sensitive to the secrecy needs. Different procedures can be designed to reconcile openness with the need for security.

24. As far as membership is concerned, the leading principle should be autonomy: parliament should be free to make appointments. There should be cross-party representation. There must be a clear demarcation between the oversight body and the agencies overseen. It is important that members should sit on the body long enough to acquire the necessary expertise (intelligence has a long learning curve). Vetting of members could be desirable in order to have an enhanced access to confidential information, although parliament may not allow the vetting of its members. A tailor-made parliamentary committee would therefore be preferable.

25. International cooperation raises specific problems. Engaging in international networking of security agencies is certainly the adequate response to the recent terrorism threats. However, it is necessary to create a legal framework in which cooperation with foreign agencies is only permissible according to principles established by law (including human rights safeguards) authorised according to strict routines (with proper paper trails) and controlled or supervised by applicable parliamentary or expert bodies.

26. Other roles for parliament in securing better accountability of secret services can exist e.g. as concerns the appointment of the Head of the agencies and the auditing of the services.

Judicial review and authorisation

27. There are different forms of judicial control of the security services.

28. First, prior authorisation in a pre-trial phase or post ad hoc review of special investigative measures. Secondly, control in court cases concerning security issues (particularly in criminal cases on security-related offences). Thirdly, investigating magistrates, often specialists in security issues, may be given a general supervisory control over ongoing security investigations. Judges may also be given a role in chairing ad hoc commissions of inquiry, or serving or retired judges may sit on expert bodies, but this should be regarded as a form of expert rather than judicial control.

29. Judicial authorisation protects individual cases. Much security work is not directed towards pre-trial legal procedures (e.g. data-mining). This kind of security work thus tends to escape judicial control.

30. In order for judicial control to be effective, the judges must be independent and possess the necessary expertise. Considerable experience and specialist training is advisable as otherwise they may not be able in practice to question the experts' threat assessments. However, case-hardening" (a tendency of the specialised judges to identify with the security officials) must be, avoided which means that judges should not serve for too long periods in this role.

31. Special security-cleared advocates may in some cases serve the need to balance open justice (fair trial) with security interests.

Expert bodies accountability

32. These can replace or supplement a parliamentary body or judicial accountability. Expert bodies can allow for greater expertise and time to be devoted to oversight, and do not present the same risks of political division as a parliamentary body. However, they do not have the same legitimacy as a parliamentary body. Different methods exist for strengthening their legitimacy.

33. Their mandate can be agency-specific or field-specific (e.g. only over databanks or surveillance) however, nowadays the integrated approach to security issues means that such specific forms of oversight miss other important parts of the security spectrum. Like parliamentary bodies the focus can be on different things. They can supervise certain aspects of the security work (legality, efficacy, efficiency, budgeting, conformity with human rights, policy), or certain activities (e.g. as regards security data banks). Such bodies can also be given certain control functions, e.g. as regards approving surveillance.

34. Their members should be legally trained if the mandate is review of legality, or a more varied background if the mandate is broader. Expert bodies need the trust of parliament and the public. Parliament involvement is thus necessary in establishing the expert body, in choosing its membership and in receiving its reports. An alternative to a purely expert body which combines expertise with legitimacy is to have part of the membership consist of serving or retired politicians (a "hybrid body"). Expert bodies should be able to present special reports as well as an annual report. As regards the content of the report, different methods exist for reconciling government concerns for secrecy with the need for the expert body to provide plausible reassurance to parliament and the public. However, the government should not normally be able to control whether a report is published at all, and when it is published.

Complaints mechanisms

35. It is clearly necessary for individuals who claim to have been adversely affected by security services to have avenues of redress before an independent body. This strengthens accountability and leads to improved performance through highlighting administrative failings.

36. The capacity of ordinary courts to serve as an adequate remedy in security fields is limited, Alternative, specialist tribunal or ombudsman-like systems exist in some States. In some cases, parliamentary bodies also deal with individual complaints. The ECHR requires that control and remedies functions are performed by different bodies.

I. Introduction

37. In its Recommendation 1713(2005) "on democratic oversight of the security sector in member States", the Parliamentary Assembly recommended "(…) that the Committee of Ministers prepare and adopt guidelines for governments setting out the political rules, standards and practical approaches required to apply the principle of democratic supervision of the security sector in member States (…)". It further identified certain principles in some areas including the Intelligence Services.

38. On 7 July 2005, the Committee of Ministers of the Council of Europe decided to request an opinion of the Venice Commission on PACE Recommendation 1713 (2005), which was subsequently adopted by the Commission on 21-22 October 2005.

39. In its opinion (CDL-AD(2005)033), the Commission recalled that, in 1998, it had examined, at the request of the Committee on Legal Affairs of the Parliamentary Assembly, the question of the constitutional relations between internal security services and other organs of the State and had reached certain conclusions in respect of the need of ensuring close control of the security services by the Executive, Parliament and the Judiciary (CDL-INF(1998)006). The Commission also noted that, after 9/11, the need to increase the efficacy of ISS had become apparent, while the parallel strengthening of democratic intelligence oversight had to be seen as necessary and a priority. The Commission accordingly recommended a comparative study of the legislation and practice in respect of democratic oversight of national security in the Council of Europe member States.

40. On 21 June 2006, the Committee of Ministers invited the Venice Commission to carry out the aforementioned comparative study, giving special emphasis to the role of parliaments and their specialized committees as well as to that of national courts in overseeing internal security services.

41. A working group was subsequently set up within the Venice Commission, composed of Messers Iain Cameron, Olivier Dutheillet de Lamothe, Ian Leigh, Jan Helgesen, Franz Matscher and Valery Zorkin. The working group met in Venice on 12 October 2006 and in Paris on 1 December 2006 and 26 March 2007.

42. The present report, which was prepared on the basis of the contributions of the members of the working group, was discussed within the sub-Commission on Democratic Institutions on 31 May 2007 and was subsequently adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007).

43. An update of this report on the basis of the contribution of Mr Iain Cameron was subsequently adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015) (CDL-AD(2015)006). The most significant post-2007 development, the issue of improved democratic oversight over signals intelligence, is now set out in a separate report, CDL-AD(2015)011. This report follows the same general structure as the present report, and should be seen as a supplement to it. In the present, consolidated, report, new paragraphs have been added regarding certain more important developments in democratic oversight of security services. Otherwise, the text of the original 2007 report has been left unchanged except for some minor amendments, mainly cross-referencing.

II. Previous Council of Europe work in this area

a. The Venice Commission study[1]

44. In 1998, the Venice Commission was requested by the Committee on Legal Affairs of the Parliamentary Assembly to examine the question of the constitutional relations between internal security services and other organs of the State.

45. The Commission came to the following main conclusions:

- internal security services by their own nature sometimes have to act outside the accepted standards of an ordinary police force;

- whatever their position in respect of the Executive, they must be made accountable for their actions with the provisions of the laws which regulate them;

- the role, functions, powers and duties of the internal security services must be clearly defined and delimited by the legislation setting them up or by the Constitution;

- rules concerning internal security services should be laid down in the legislation or even in the constitution; at any rate, the legal basis should be clear and concise as to their tasks and in harmony with the constitution and the international obligations, in particular those on human rights protection;

- the norms applicable to internal security services should only be kept secret to the extent that it is absolutely necessary;

- the budget allocated to internal security services must be appropriately monitored, and there should be at least one Government member responsible for it;

- internal security services must only be used in the national interest;

- a close control of internal security services is necessary, be it by the Executive, or by Parliament and/or the judiciary;

- the administrative/legal structures of internal security services must allow for an adequate judicial control of their activities;

- in order to allow for pursuing the overriding State interest when necessary, provision should be made to ensure confidentiality, lack of publicity, protection of preserved information and data, protection of witnesses and so on;

- access from other State authorities to the information held by internal security services must be regulated in detail;

- the possibility for internal security services to monitor persons belonging to other State services must be duly regulated by law;

- in the operation of security services, derogations of fundamental rights and freedoms must be kept to a minimum, and accountability of security services for undue infringements of human rights must be stated;

---

[1] See Venice Commission, Internal Security Services in Europe, Report adopted at the 34th Plenary meeting (Venice, 7 March 1998), CDL-INF(1998)006.

- the use by security services of extraordinary measures must be proportionate to the danger incurred and must not be unduly prolonged in time.

46. The Venice Commission has looked at the issue of security agencies in the context of country studies, notably as regards Moldova and Bosnia and Herzegovina.[2]

b. The Group of Specialists on Internal Security Services (PC-S-SEC) of the European Committee on Crime Problems (CDPC)

47. In 2002, the European Committee on Crime Problems set up a Group of Specialists on Internal Security Services, which carried out a research on the legal basis, the structure, the modalities of work of security services and the modalities of control of these services in Council of Europe member States.[3]

48. In 2003, the CDPC, due to significant differences between national legislations in this respect and diverging opinions as to the usefulness of elaborating recommendations on the subject, which could only touch upon certain fundamental and general principles concerning internal security services, considered that this matter was not a priority.

c. The Council of Europe Secretary General's supplementary report under Article 52 of the European Convention on Human Rights on the question of secret detention and transport of detainees suspected of terrorist acts, notably by or at the instigation of foreign agencies

49. On 7 March 2006, the Secretary General of the Council of Europe, with a view to supplementing his report under Article 52 of the ECHR on the question of secret detention and transport of detainees suspected of terrorist acts, notably by or at the instigation of foreign agencies, sent a second series of questions to 36 Council of Europe member States.

50. He sought information and clarification on certain specific points, including on control mechanisms (administrative, judicial, parliamentary or other) in respect of the activities of foreign, as well as national, intelligence services. All requested States replied to the Secretary General's queries.[4]

III. The scope of the present study

51. This study does not aim at producing a survey, let alone an exhaustive one, on the security services of the Council of Europe member States. Such a study would require extensive research, thus an extended timeframe and significant resources.

---

[2] See Venice Commission, Opinion on the Law on the Information and Security Service of the Republic of Moldova, CDL-AD(2006)011; Opinion on the Law on the Agency of Bosnia and Herzegovina for Information and Protection, CDL(2002)006 and 005.

[3] 17 countries provided replies to the questionnaire prepared by the Group of experts: see PC-S-SEC(2002)06rev, Summary of replies to the questionnaire.

[4] See SG/Inf(2006)013 (hereinafter, Secretary-General's report) and the replies made available on the Council of Europe's website.

52. It is difficult to obtain useful information from State authorities on the key issues of the security services. What can of course be obtained is information on the constitutional and legal provisions governing them. By their own nature, however, these services are also governed by unpublished rules and by classified policy decisions, which would not and could not be brought to the attention of the public or of the Commission. Deficient legal provisions might well have been corrected in practice or, vice-versa, good legal provisions might not be applied in the intended way in practice. The mere collection of constitutional and legal provisions would not seem to have any added value at this stage. However, in a number of States, official commissions of inquiry into different aspects of security and intelligence matters have produced considerable material both on law and practice. Members of the Commission were requested to provide the working group with references to recent commissions of inquiry in their respective States, and a number of replies were received. The examples chosen in the present study tend to come from the States whose members replied to the working group. Where necessary, these have been supplemented with other examples of law and practice from different academic studies. On occasion, the present report refers to material from non-Council of Europe States, such as Canada and the United States, States with long experience of democratic control over security agencies.

53. The Commission has therefore decided to proceed instead with the identification of forms and models of accountability[5] for security services, in order to identify the strengths and weaknesses of each of them and possibly best practices of democratic oversight of security services in Europe. In order to do so, the Commission will build upon the case law of the European Court of Human Rights (ECtHR) and previous work carried out in this field and rely on the information on the constitutional and legal regulations already collected, *inter alia* by the Secretary General in spring 2006. Although the study is on "internal security services", it is important to point out at the outset that the study is directed at the *function* of internal security, rather than the mandate of a specific State agency, which a State may or may not have chosen to call an "internal security service".[6] As will be explained below, this function can be, and is in many States, split between several different agencies.

IV. Is there a need for (improved) democratic control?

54. The maintenance of the internal and external security of the State is vital and often claimed to be the primary duty of the State. Without security, the protection of the other values and interests of the State is not possible. Indeed, only a strong State can ensure a satisfactory level of law and order and the full protection of human rights.

55. In order to anticipate, prevent or protect itself against threats to its national security, a State needs effective intelligence and security services: intelligence is thus an inescapable necessity for modern governments. Few States take the view that they can dispense with an intelligence service (against foreign threats) and none is sufficiently immune from terrorism or the inquisitiveness of its neighbours to forego a security service.

---

[5] As for the meaning of accountability in this report, see below paras 72-83.

[6] In this study, the term "internal security service" and "internal security agency" are used as synonyms. Security can be defined as a state of being "secure" i.e. free from fear, damage etc., in other words, a (negative) state of there being an absence of threats. Security in a broader sense can also have the positive element of being in a position to advance one's goals. See generally on the concept of security and "securitisation" Bigo D. et al The Changing Landscape of European Liberty and Security, CHALLENGE Research Paper 4, 2007, www.libertysecurity;org. "Internal" security has traditionally been contrasted with "external" security, meaning threats of "foreign" origin. Nowadays, however, "internal" and "external" threats to the State can naturally be linked in a number of ways (see below paras 58-59). The present report does not deal with the important issues of the democratic oversight of the armed forces, of foreign intelligence services or of military intelligence services, except insofar as these perform internal security functions. The diffuse boundary between these services and the function of internal security, especially as regards the fight against terrorism, merits further study. As regards regulating signals intelligence services, see now CDL-AD(2015)011.

56. Internal security services are designed to enable governments to protect national security. Effectiveness often requires flexibility and secrecy. Undoubtedly, a variety of internal and external situations may arise in which the executive organ of the State must act quickly and decisively to protect the fundamental interests of the State and society. This may justify diverging from the ordinary standards of accountability for other types of public service. However, the very secrecy which is necessary in this field means that it cannot be subject to informal scrutiny by the media and other public watchdogs to the same extent as most areas of public administration. In this respect, improved democratic scrutiny of the security sector serves the dual purposes of ensuring efficiency and legitimacy.[7]

57. The protection of internal security must include the protection of the fundamental values of the State which, for a liberal democratic State, means *inter alia* democracy and human rights: However, in practice, the values of freedom and security can easily be perceived as opposing values. It is widely recognized that security and intelligence agencies can potentially threaten as well as protect democracy. The subjectivity and flexibility of the term "national security" combined with its vital importance to the State means that it provides a government with a large potential for abuse of power. Moreover, as explained below, internal security services themselves have inbred in them a potential for abuse of State power. [8]

58. Globalization and the complexity of modern societies increases their vulnerability to national and transnational terrorism. Industrial and technologically based economies require a relatively high level of order and stability and a small group of determined people can do a vast amount of damage to the communications, transport or power networks. The potential for terrorists making or obtaining weapons of mass destruction (WMD) increases with the spread of technology – a process which can only be delayed, not stopped, by the plethora of international agreements on non-proliferation.

59. Bearing in mind the scale of the dangers, a security agency has very good reasons for collecting as much information as it can on real threats to the State. Intelligence is one of the main weapons the State has in the struggle against terrorism and the spread of weapons of mass destruction. This involves collecting information on individuals which immediately raises the issue of respect for individual rights. The vulnerability of democratic societies combined with the diffuse nature of the threats against them means that intelligence is wanted on everything which is, or can become, a danger. Unless external limits are imposed, and continually re-imposed, then the natural tendency on all agencies is to over-collect information. Internal limits will not suffice because, while the staff of a security agency should set limits on the collection of data, it is not primarily their job to limit themselves and think about the damage which over-collection of intelligence can do to the vital values of democratic societies, in particular, the enjoyment of the rights of freedom of expression, association, privacy and to personal integrity. Physical and administrative capacities may previously have set limits on the extent to which a security agency could interfere with peoples' human rights. However, major technological advances, particularly in data collection, processing and analysis and in surveillance, have dramatically increased the capacity of a security agency in this respect. Moreover, it is, obviously, not simply a question of collecting intelligence. Intelligence is collected in order to be used in a number of ways, e.g. in as regards security screening and in relation to decisions to grant citizenship or to deport aliens.

[7] Cf. Müller-Wille, B., Improving the Democratic Accountability of EU Intelligence, 21 Intelligence and National Security, 100-128 (2006) at p. 108.

[8] See Venice Commission, CDL-INF(98)6, p. 4.

60. Security agencies must be equipped with considerable technological tools and must enjoy exceptional powers. Governments could easily be tempted to use them to pursue illegitimate aims: for this reason, in order to prevent them from becoming an oppressive instrument for party politics, security agencies must be insulated to some degree from day-to-day political/governmental control, (see below para 85). This risk is particularly present in a crisis; when there is pressure to produce quick results. In States where State institutions are relatively weak, the interests and activities of State security agencies and private security organizations interests can be intermingled. Developments in technology, and the relatively free availability of this technology in the private sector, have placed powerful surveillance tools even in the hands of private security organizations.[9] In States where organized crime has heavily penetrated the administration, officials in the security agency can obviously be corrupted and the extensive powers and capabilities of the agency used for criminal purposes. The State security agency must thus also be kept clearly separate from private interests and protected from organized crime.

61. At the same time, this necessary insulation of security services carries with it dangers. While this should not be exaggerated, experience shows that security agencies can develop a "State within a State" mentality. A culture of regarding any non-mainstream political movement as a threat to the State can emerge. In extreme cases, an agency can manipulate the political process by infiltrating political movements, pressure groups, and trades unions, and engage in "psychological operations" and disinformation.[10] This is a danger which is more present in some States than others. Nonetheless, a problem for the personnel of any security agency is that they can develop a "security mindset". Improved democratic scrutiny is thus not simply to protect against abuse of human rights but also to expose the intellectual assumptions and work practices of security personnel to informed criticism.[11]

62. Governmental control of Internal security services is therefore essential to avoid a "State within the State" mentality. It must not however be too tight – or the services may be abusively used to attain illegitimate aims.

63. The need for democratic oversight of the security services has been recognized and has inspired reforms at first, in the 1980's, in several Western European States, and afterwards, in the post-Cold War era, also in Eastern Europe, notably in former States of the Warsaw Pact and the Soviet Union.

64. In the majority of Eastern European States partial reforms were made of internal security services in the extremely difficult context of the post-1989 transition from Communist government. The new political regimes and institutions, along with the democratic values and norms that underpinned them, were fragile. Resources and expertise were scarce. Foreign control was still heavily present. The existing institutions and personnel were perceived by many as "the enemy" and criminals from whom an accounting was demanded.[12] Following lustration processes, non-professional staff were recruited, including at the top level, and a specific focus was put on the loyalty to the post-communist authorities (or at least on the emphasized hostility to the previous regime). This led in many cases to a loss of institutional

[9] See below, para 212.

[10] Even the existence of files gathered in the past can cause problems for people today. In many Eastern European States, files were gathered on dissidents by the former Communist security apparatuses which had extensive networks of informers. Where the content of an individual file is leaked, or a person is, correctly or incorrectly, identified as an informer, this can wreck a person's career.

[11] Lustgarten, L. Accountability of security services in western democracies in Töllborg, D. (ed), *National Security and the Rule of Law*, (Gothenburg University, 1997) at p. 88.

[12] See Watts, L., Intelligence Reform in Europe's Emerging Democracies, Conflicting paradigms, Dissimilar Contexts, 48 Studies in Intelligence, 2004.

memory, internally divided agencies and the deep and often unconstructive politicization of the new staff members. In order to provide rapidly for a legislative basis for the services, legal provisions were copied, often in an uncritical, unsystematic and even contradictory manner, from developed democracies or were improvised. These problems were aggravated by the lack of democratic culture.[13] Former staff on occasion sought employment in the private sector where they could use their technological and other capabilities, leading in some States to the growth of a parallel security sector, unaccountable to the State, but linked through continued personal contacts with the police and officials in the State security agencies. Removing the anti-Communist opposition from the mandate of the internal security service led, in some States, to the service attempting to expand into areas of crime control previously the preserve of the police, resulting in "turf battles" and duplication of efforts.

65. The terrorist attacks of 9/11 have urged new changes and brought new challenges. The new threats of terrorism and the activities whereby it can be funded (drug trafficking, money laundering and organized crime) require greatly enhanced inter-agency communication, co-operation and intelligence sharing at the national and international level. This has inspired another wave of reforms of the security services, which has not focused on control *per se*, but rather on effectiveness and functional coordination. And yet, expanded inter-agency co-operation poses problems not only in terms of effectiveness, but also in terms of the control of the security services.[14] In a number of States, there has been a great expansion of the number of staff of the security agency. This, too, affects the institutional memory of the agency, its awareness of past abuses of power and the need for internal controls.

66. New, and greater, powers of intelligence gathering have also been given to the security agency in a number of States.[15] It should also be remembered that in many States , the rationale for giving the security agency exceptional powers not available to the ordinary police has been the limited size and mandate of the agency (concentrating on counter-espionage) and the fact that its intelligence-gathering was not primarily intended to lead to prosecutions and convictions, but rather preventing security threats from materialising. In some States , barriers to transfer of data between the police and the security agency were deliberately created in order to emphasize that the targets of the latter were (primarily) "foreign" and these powers were not a danger to "ordinary citizens".

67. However, the growth of terrorist "networks" organized transnationally, in a non-hierarchical fashion, requires a transnational and network-based response from the State. This involves proactive and operational cooperation between the security agency and the police, customs, coast guard, tax authorities and other State bodies. From the perspective of effectiveness, barriers to intelligence cooperation are difficult to justify and should be dismantled. But where the State security apparatus is working, as it should be, as a coordinated entity, then the institutional safeguard of locating exceptional powers in only one – small, especially well monitored and controlled – part is no longer so much of a safeguard. Moreover, existing control mechanisms not only tend to be institutional, focusing on a single agency, but are nationally limited, as each State looks exclusively at its own agencies, and none looks at the international network of cooperation as a whole. The transnational nature of threats to States in fact increase the risk for a "State within a State" mentality: in order to obtain information which is in the hands of foreign agencies, a national agency will have to cooperate with foreign agencies in information exchange. The administrative need for good relations with powerful foreign friendly agencies carries with it a number of risks and dangers, notably that of the agency disobeying

[13] See Zorkin, V., Democratic Oversight of Special Services in Eastern Europe, CDL(2007)051.

[14] See Watts, L., op. cit.

[15] See, e.g., the summary of developments in this area for EU States contained in the EU Network of Independent Experts in Fundamental Rights report, the Balance between Freedom and Security within the EU (March 2003).

the will of the government of the day or of the agency harming the interests of the citizens or residents of the State, by transferring information on them to foreign agencies.

68. The recent problems in connection with extraordinary renditions are a clear example of how international cooperation in intelligence operations may affect human rights protection.[16]

69. A tighter democratic control, and a different kind of control, appear therefore necessary in a democratic society in the post 9/11 era. The changed powers and functions of the domestic security services and the international co-operation in the fight against terrorism require an improved control over the manner in which these powers are used and their acceptability in a democratic society.

70. Generally one can say that developments since 2007 have only strengthened the case for better democratic oversight of internal security agencies.[17] The case law of the ECtHR set out in paragraph 133 below – in particular that concerning the involvement of certain European states in the US rendition programme - is very good evidence that there have been serious structural failings in oversight in a number of states. Parliamentary oversight which might exist on paper cannot be taken for granted to work in practice. The US Senate Select Committee on Intelligence Study of the Central Intelligence Agency's Detention and Interrogation Program, made public in a declassified version in 2014,[18] is also evidence that, even in the state which started the modern trend of oversight, misuse of power and serious violations of human rights can occur.

71. The threat which terrorism poses to democratic societies waxes and wanes, or is perceived by public opinion as waxing and waning, depending upon its perception of other threats. At the present time, the conflicts in Iraq and Syria are generating fears over returning "foreign fighters". Radicalisation in the direction of violent extremism undoubtedly continues to be a threat. In the wake of a financial austerity measures, xenophobic extremism can thrive. Minorities - immigrants, Muslims etc. – can be blamed and alienated communities can become even more alienated. If one is no longer concerned about attacking a target which has some, at least, control over the political agenda (governments, parliaments), and instead is prepared to attack any target of symbolic significance then the targets are endless. "Lone wolf" terrorism is impossible to guard against. All of this creates much more work for internal security agencies, and understandably, calls for greater powers. But the need for any new powers for dealing with extremism and terrorism must be convincingly demonstrated, and if granted, must go hand in hand with improved controls and oversight.

---

[16] See below, Section V.C.f.

[17] As regards new standards of oversight, see in particular the Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, The Role of Intelligence Agencies and their Oversight in the Fight Against Terrorism, A/HRC/14/46 17 May 2010, the Ottowa Principles on anti-terrorism and human rights 2006, and as regards fair trial, Open Society Foundation, the Global Principles on National Security and the Right to Information,

http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf.

See also the report of the Commissioner for Human Rights, Oversight of National Security Services, April 2015 (forthcoming) and Marty, D., "Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations", report for the Committee of Legal Affairs and Human Rights, PACE Doc. 12714.

[18] www.intelligence.senate.gov/study2014.html.

V. Accountability

A. The notion and forms of accountability

72. The present study concerns improved democratic control over security agencies. However, it is important to see this as one element of a broader, overarching concept of "accountability". A working definition of accountability is "being liable to be required to give an account or explanation of actions and where appropriate, to suffer the consequences, take the blame or undertake to put matters right, if it should appear that errors have been made".[19]

73. As far as security agencies are concerned, there can be said to be different types of "accountability", to the executive, judiciary, parliament and independent bodies. One can also see the monitoring role of civil society (NGOs, think tanks etc.) and the media as a form of accountability. In the delicate area of alleged wrongdoing by government or security personnel, the attitudes to investigative reporting held by the press and the public, and the degree of obstruction from government and administration may well be as important as any formal safeguards which may exist. An aggressive investigative press, and a government which refrains from threatening it with prosecution under the applicable secrecy legislation, or otherwise gagging it, is also a form of accountability, even if this is not a substitute for State accountability mechanisms.

74. In addition, there is a degree of international accountability to international and supranational monitoring mechanisms, such as (for Council of Europe members) the European Court of Human Rights (ECtHR).

75. Accountability may exist *ex ante* (authorization or control), during the operations (control or monitoring of the activities) or *ex post* (review of the activities). It can concern general operations or specific acts.

76. Different terms can be used for these different forms of accountability, and the terms used vary from State to State. Different terms can be used to refer to the same thing, and the same term can be used for different things. The *executive* can be said to exercise a power of "control" over the security agency, meaning the power to direct the agency in general, or even in specific operations. The *judiciary* may "authorize" the use of special powers by the agency, meaning that permission must be sought before a particular power, such as electronic surveillance, is employed against an individual. The *parliament* or an independent expert body may have a power of "review" or "oversight" of the work of the agency, meaning a power to supervise the work of the agency, either in general or in specific operations. This may be simply a recommendatory power, or it may involve some kind of a power to follow-up on recommendations made. A *judicial, or independent expert body*, may have the power to hear complaints of wrongdoing by the agency.

77. Depending on a number of factors, in particular the constitutional structure and history of the State, and its legal and political culture, there can be overlaps (and gaps) in the types of accountability exercised by the different branches of government. For example, a body responsible to the parliament may have a power of authorization over the use of special powers, or (very commonly) over the budget of the agency. A judicial body may have a power of "review" meaning that it is only informed of specific operations (possibly involving special powers) after these have been initiated.

---

[19] See Oliver, D., Government in the United Kingdom: the search for accountability, effectiveness and citizenship, Open University Press, 1991 p. 22. See also the discussion of the concepts of review, accountability and oversight in the context of security in Arar Commission, A New Mechanism for the RCMP's National Security Activities, 2006, pp. 456-463 and generally, in Behn, R., Rethinking Democratic Accountability, Washington, Brookings Institute, 2001, especially chapter 1.

78. Hybrid forms of accountability can also exist. For example, an independent expert body can be given powers of authorization, or a parliamentary body can be given the power to hear complaints.

79. Accountability can have different modes. It can be backward looking, to apportion responsibility. It can be forward looking, to encourage learning. The primary purpose of accountability is the avoidance of misuse of power. In a democracy, public power comes from the people and the exercise of executive power must, directly or indirectly, be answerable to the representatives of the people. Agencies and officials who carry out the vitally important task of maintaining the internal security of a democratic State must be accountable not only to themselves.

80. Sensitive accountability structures attempt to insulate security and intelligence agencies from political abuse without isolating them from executive governance. On the whole the solutions adopted by democratic States deal with this paradox in two ways. Firstly, by balancing rights and responsibilities between the agencies and their political masters and, secondly, creating checking mechanisms outside the executive branch.

81. In simplified form, four different forms of State accountability can be identified:

a. parliamentary accountability
b. judicial accountability
c. expert accountability
d. complaints mechanisms.

82. The internal security function is an executive function. Thus, the first two accountability forms correspond to the traditional separation of state powers (the legislature and judiciary holding the executive accountable). The second two are accountability forms which have emerged to supplement or replace the traditional forms. Within these forms, different models of accountability have emerged in different States. It is obviously the overall blend of mechanisms, the assessment of the accountability system as a whole, which is important.

83. Before looking at the different forms of accountability (see Sections VIII, IX, X and XI below), more needs to be said about the background. First general problems in ensuring accountability are discussed, followed by the constitutional and organisations contexts that affect accountability. Discussion then moves to international aspects, in particular the questions of accountability where international co-operation between security and intelligence agencies is involved, and the impact of the jurisprudence of the European Court of Human Rights in this field.

B. General problems in ensuring accountability

84. In the light of the importance and nature of the interests at stake, security intelligence-gathering is one of the main areas of national decision-making which a government is most unwilling to submit to national legislative scrutiny and judicial review and, a fortiori, to international supervision and control.

85. For a variety of reasons, there can be tension as regards national security policy, not only between the governing party and the political opposition in a State, but also constitutional tension between the executive and the legislative power, tension within a government (especially a coalition government), and tension between political masters and the staff of security intelligence agencies. A large degree of secrecy must accompany national security policy making and operations. However secrecy also has the effect of increasing the government's control over policy at the expense of the legislative power, and of insulating the

former from criticism. This is exacerbated by the fact that nowadays, there is a link between "external" and "internal" threats to the State. Accordingly, security and intelligence information tend to forms an indivisible whole.

86. Even the government may lack adequate knowledge of what the security intelligence agencies are doing, and adequate mechanisms for administrative, and budgetary, control over them. The complexity of modern society means that there are often problems for elected governments in properly steering the work of government departments and administrative agencies in general, let alone in security matters. Experts have special knowledge, and government is largely dependent upon these experts. In ordinary areas of administration, e.g. education, environmental control etc. various mechanisms exist for improving governmental control over the bureaucracy. But the necessary secrecy which surrounds the area of security can make this considerably more difficult.

87. The normal legislative mechanisms for controlling the administration work by ensuring accountability of the executive for the actions of the administration. These will obviously not function when the executive itself lacks control. Even where the executive is in control, the parliament may not have its own sources of information to check on the legitimacy of a particular claim made by the executive, and so it will seldom be in a position to challenge it.

88. Where the parliament is not in a position to hold the executive accountable, it becomes even more important that the national courts are able to perform this function effectively. But, for a variety of reasons the ordinary courts are often in poor position to perform adequately this task in the area of national security.[20] Unlike other government authorizations to limit human rights, powers granted governments in this area are often wholly discretionary. Useful statutory definitions of what is meant by the term "national security" often do not exist in domestic legal systems, making it very difficult for the judiciary to rule that an exercise of power fell outside the scope of "national security".[21] Courts may moreover lack the procedural competence (e.g. jurisdictional obstacles) or the will to intervene. Even if they have both, they may feel constrained not to do so. They may feel that, constitutionally, this area belongs to the executive. Or even if this is not formally so, they may consider that the policy element looms large in national security decision making, outweighing the adjudicative element. Or they may reason that they have neither the access to all the relevant information nor the training and experience necessary to evaluate this information properly, if they had it. Or they may feel that the public nature of the judicial process is inappropriate for matters which should be kept secret. Even if they have the jurisdiction, the competence and the will to intervene, they can only exceptionally act *proprio motu* and so must usually wait for an appropriate case to present itself.

89. It is particularly important, as regards the limited scope of parliamentary and judicial control, to note the special nature of security intelligence. The heart of a security agency is its intelligence files. "Hard" data, purely factual information, is insufficient for a security agency, or for that matter, any police organization. It also needs to gather *speculative* intelligence in order to determine which people are, or are probably or possibly, threatening national security. This information can be obtained in different ways. A large proportion of non-open source internal security information comes from informants.[22] Like factual information, such "soft intelligence" can, and must if the agency is to do its job properly, be collated to produce a personality profile of a suspect or an analysis of a suspected activity. This means that the filing system must be

[20] See below, paras 216-218.

[21] See below paras 127 and 133, regarding the ECtHR position on defining national security.

[22] Commission of Inquiry into certain activities of the Royal Canadian Mounted Police. 2nd Report, Freedom and Security under the Law (1981) ("McDonald Commission Report"), p. 536, US Congress, Senate, Select Committee to Study Governmental Activities. Final Report, Book II: Intelligence Activities and the Rights of Americans (1976) ("Church Report"), pp. 227-228.

constructed in such a way as to facilitate linking of information on the same subject matter filed after considerable lapses of time, as well as allowing synthesis of (apparently) unrelated information, e.g. to discern patterns of activity. The entries must also be graded to indicate their reliability, and the grading periodically reassessed. It should be noted here that files are obviously not simply person files, but can be a file on a particular phenomenon, event or place (e.g. a suspected meeting place for terrorists or foreign intelligence officers). The data system must also allow all operators to obtain quick overviews of large quantities of data. However, even in the IT society it is reasonable to assume that not all, or even the bulk of, the files are computerised. A standard system would rather be a computerised central register, searchable on a large number of different variables, which in turn refers to paper files containing more details. Security intelligence is often "compartmentalized", meaning that the databases are not automatically accessible to every security official, in order to minimize damage if a security breach occurs. Only those with the correct security clearance will have access to a particular investigation. This can even apply to more senior officials, who may not necessarily have automatic access to all the materials filed by, or used by, junior officials (a factor which has important implications for internal controls, see below para 135).

90. Basically, however, security officials make a value judgment on the available information as to whether a particular person is a security risk, and if so, what exactly he or she is up to. It is a question of risk assessment, and this inevitably involves a large degree of subjectivity. Obviously, it takes a long time for any external monitoring body to penetrate the arcane world of intelligence, to understand what is a "reliable" intelligence assessment, and why this is so. Unless and until they are in a position to make a reasonably informed "second assessment", a monitoring body is not a real safeguard.

C. Constitutional and Organizational Contexts

a. In general

91. The lines of accountability and control of security agencies will depend upon the constitutional structure of the State.

92. In many States, the constitution is firmly based on the separation of powers, which in turn means that the conduct of foreign and defence policy is often the exclusive or primary preserve of the executive.

93. A variety of patterns for organizing security and intelligence exists. *Internal* security agencies can be distinguished from *external* security (or intelligence) agencies, even if the boundary lines between them can at times be difficult to draw. *Military* agencies can be distinguished from *civilian* agencies. The principal mandate of the first may be confined to intelligence collection relating to military threats to the State, and the security/loyalty of the armed forces, although again the boundary line between this and the mandate of a civilian agency may be difficult to draw.[23] Where a security agency is located organizationally within the military command structure, this can give rise to special problems of accountability.[24] Lastly, *communications* intelligence agencies should be mentioned. Having grown out of the

[23] For example, where the State sends troop contingents to peace-keeping operations in areas heavily penetrated by organised crime, the military may want to know about the links which exist between crime in the host area and its own State, and the present and future threats contacts with organised crime can pose to the safety of its personnel, the integrity of the military command structure etc.

[24] The Parliamentary Assembly has expressed the view in Recommendation 1402 (1999) Control of internal security services in Council of Europe member States, guideline A(iv) that "Internal security services should preferably not be organised within a military structure. Nor should civilian security services be organised in a military or semi-military way". See further the Parliamentary Assembly, Committee on Legal Affairs and Human Rights, Control of Internal Security Services in Council of Europe Member States, Doc. 8301, 21 January 1999.

decryption and signals intelligence agencies of the Cold War period, these agencies now monitor the content and patterns of global telecommunications traffic, so called "strategic surveillance". They may also have responsibility for developing and maintaining communications security, e.g. defensive measures against computer network attacks. Communications intelligence agencies have in many States have become large and organizationally independent from the other agencies.

94. It should be noted that the organizational context also determines the actual power or influence of the agency. This will depend partly upon the threats facing the State How pressing are these? How dependent is the State on its security agency? How strong is the political and/or administrative control exercised over it? How large is the budget of the agency? How large is the agency vis-à-vis the police, and other "competing" agencies? To what extent is it dependent on the police and other government agencies and private bodies (e.g. telecommunications companies) for technical and logistical support?

b. The organisation of the security services

95. Some States (for example, Bosnia and Herzegovina, Spain and Turkey) have a single agency for security and intelligence (both domestic and external). Others have distinct agencies for internal and external intelligence and security, with either separate or overlapping territorial competences, as in Hungary, Germany, Poland, Romania and the United Kingdom. More rarely, a State may have a domestic security agency but no acknowledged or actual foreign intelligence agency, such as Sweden, although Sweden has a communications intelligence agency. A security agency may also be organized as a legal entity or be part of a government department.[25]

96. A State may naturally have more than one agency exercising internal security functions. For example, there may be both a military and civil agency and their mandates may overlap.[26] Or there may be a civilian agency, a military agency and a paramilitary/gendarmerie agency. The advantage of parallel agencies is that they can keep an eye on each other. The disadvantages - which will usually outweigh the advantage - are naturally "turf battles", duplication of work and greater, or much greater, difficulties in monitoring and controlling the agencies. While having parallel agencies with overlapping functions is seldom a good idea, dividing functions between agencies e.g. in the field of surveillance, whereby one agency is responsible for requesting surveillance and the other for carrying it out, can have advantages for ensuring strict compliance with authorisation procedures.[27]

97. A basic difference should be mentioned between European States which grant their internal security agencies police powers, and those which do not. Some European States, such as the Netherlands, Slovenia, the Czech Republic and Germany, have separate security agencies with primary responsibility for security crimes. Such agencies might also be given strategic responsibility for terrorism. These agencies have no police powers. If they wish to make arrests, interrogate suspects etc. they must act through the police, usually a special section of the police.

---

[25] E.g. the Spanish National Intelligence Center (Centro Nacional de Inteligencia, CNI), regulated by the law 11/2002 of 6 May, provides that CNI constitutes a corporate body under public law and a department of the Ministry of Defense. The French internal intelligence agency (Direction de la Surveillance du Territoire) is a department of the Ministry of the Interior.

[26] E.g. in Austria there is a special department (Bundesamt für Verfassungsschutz as a part of the ministry for the interior with branches in the regional police commands (Landesämter für Verfassungsschutz) for the civil sector and two separate departments for the military intelligence (Heeresnachrichtenamt and Heeresabwehramt) as a part of the ministry of defence.

[27] See also below, Section VII.

98. Other States, such as Denmark, Finland, France, Ireland, Norway, Sweden and Switzerland, have security police, either fully integrated into the command structure of the ordinary police, or as a separate police unit.[28] Some States have security agencies separate from the police, but authorize these to arrest and interrogate suspects (e.g. Russian Federation).

99. Aside from constitutional traditions, there are a number of reasons for establishing a separate civilian agency. Without going into these more deeply, the main reasons can be listed as prevention of abuse of power (separation of power), the possibility for a civilian agency to develop greater analytical and other expertise, particularly in political matters and the greater scope for governmental control of the agency, as compared to control over the police (which, depending on the constitutional structure of the State, will usually be less appropriate).[29]

100. However, there is no natural dividing line between security matters and crime, especially in the case of what is generally perceived to be the major security threats to most European States today, namely terrorism. The need for a closely coordinated police-security response to terrorism and the links which can on occasion exist between organized crime and terrorism are, in fact, strong arguments for having a security police. There can thus be problems caused by overlapping competences between police and security agencies in States where there is a separate security agency, and even, it must be said, in States where the security agency is part of the police, between the ordinary and security police.

101. The Parliamentary Assembly of the Council of Europe previously expressed a clear preference for having separate civilian security agencies.[30] Undoubtedly, police powers of arrest, search and seizure can, when combined in the same organization with the powers and capabilities of a security agency, create a very powerful institution. However the acceptability of such an institution from the perspective of accountability and the protection of individual rights, depends upon the adequacy of the control structure created to prevent abuse, or overuse, of power. A strong security police which is subject to tight internal controls and control by independent prosecutors, and, when authorizing special investigative measures, control by judges, cannot be said to be incompatible with Council of Europe principles in general, or the ECHR in particular.[31]

c. The form of the mandate of the security services

102. The legal status of the mandate of internal security agencies also depends upon the constitutional structure of the State.

103. In most European States, there are no constitutional rules specifically regulating the relations between internal security services and other organs of the State. These relations are however affected by constitutional rules on the organisation and functioning of the highest State organs, determining how and by whom the organisation, functioning and powers of Government organs, including security organs, are set, and on fundamental and human rights, limiting the competence of the highest State organs to grant powers to other Government organs, including security organs. Especially in the latter respect, constitutional rules are to a

[28] E.g. in Sweden, the security department, RPS/SÄK is an integral though autonomous part of the national police force. The same applies to the French Direction de la Surveillance du Territoire, DST.

[29] One of the best discussions of the need for a separate civilian agency can be found in the McDonald Commission report, (at pp. 413-421) although it should be noted that this was written as part of the justification for removing security competence from the police (RCMP).

[30] Parliamentary Assembly, Control of internal security services in Council of Europe member States, Recommendation 1402 (1999), point 6.

[31] See Venice Commission, CDL-INF(98)6 p. 5.

large extent supplemented and reinforced by international agreements and by international organs monitoring the application of these agreements.[32]

104. In most States, the tasks and the extent of the exceptional powers of the internal security services are set out in parliamentary legislation, either organic laws (e.g. Spain) or ordinary legislation (e.g. Norway).

105. In those countries in which the security services are part of the general police, the legislation concerning police in general is also applicable to them, in addition to whatever special legislation exists, granting other powers and duties.[33]

106. In addition to legislation, more detailed norms, or guidelines, are normally set out in subordinate legislation promulgated by the executive (which, if in the form of executive orders will usually be published) or by the Head of the security service in question (which will usually be secret).

107. Where defence or foreign policy matters are, according to the constitution, the primary responsibility of the president, this will have implications for the legal status of the norms regulating the agency (as well as the accountability arrangements). In France, for example, there is no parliamentary legislation on the internal security services, the whole organizational structure and powers of these services being set out in executive decrees.

108. The Venice Commission has previously expressed the view that this latter model is undesirable from the perspective of democratic legitimacy; indeed, if it is only "preferable" that the rules concerning the internal security services be enshrined in the laws of Parliament, it is "absolutely essential" that norms concerning the internal security services be as clear and concise as possible so that the tasks they can lawfully engage in are clearly defined and that the regulations should only be allowed to be kept secret to the extent that it is absolutely necessary.[34]

d. Security priorities

109. The content of the mandates given to security agencies in terms of tasks will obviously vary considerably, largely depending upon the priority of threats, and perceived threats, faced by the State.[35]The priorities of the security agency may be set in different ways.

110. While the threats will of course, in turn, vary considerably, there is a common European core. Without trying to be exhaustive, the following (at times overlapping) factors will influence the roles and priorities of the security agency:

- ethnographic factors (the existence of violent groups within ethnic minorities which possess both the willingness and capability to pose a separatist threat, first and second generation immigrant communities which can be threatened by foreign interests and who need to be protected from these, or from which threats can emerge),
- military/political factors (is the State neutral or a member of a military alliance? has it foreign bases? are the internal or foreign policies perceived as hostile to the fundamental values of a group in the State, providing a base for recruitment of terrorist

[32] See Venice Commission, CDL-INF(98)6, p. 2.

[33] E.g. Denmark, Finland, France, Ireland, Norway, Switzerland. In Austria a special law governs the security police (the Sicherheitspolizeigesetz).

[34] See Venice Commission, CDL-INF(98)6, p.7 and below, paras 128 and 237.

[35] See PC-S-SEC(2002)06rev, Summary of replies to the questionnaire.

cells? What important military or political information needs to be protected from espionage),
- "pure" political factors relating to the nature of the State itself (does political power change hands frequently, or does one group dominate permanently? where is the State on the spectrum of liberalism – authoritarianism?),
- economic and technological factors (what wealth generating activities need most protection/promotion? what technologies or goods are being produced which should be subject to tight export controls to prevent proliferation of WMD capabilities),
- criminological factors, the extent of threat posed to the State by international terrorism or organized crime,
- historical factors (an imperial past, dictatorships in living memory and so a history of abuse of power by the internal security agency), and
- geographical factors (proximity of unfriendly or unstable States, strategic significance).

111. The content of the mandate can also vary in that the security agency may have either a more pro-active mandate, e.g. to "counter" security threats, or it may be restricted to the gathering and analysis of information.

e. Internal control

112. Internal controls consist of two elements. First, there is the control exercised by the security agency over itself, by means of decision-making structures designed to make sure that measures and policies are properly authorized, procedures are followed etc. Second, internal controls mean those controls which operate within the executive itself, i.e. administrative control exercised by the hierarchical superior permanent civil servants in government departments to which the agency may be subordinate, or to which it may report, or, where the agency is involved in investigating security crime, prosecutors.

113. There can obviously be an overlap between "governmental" and "administrative" control in States where the permanent civil service, or the upper ranks of it, are "politicized". Similar considerations apply as regards prosecutors. Depending upon the constitutional structure and legal culture of the State, prosecutors possess varying degrees of independence from both the agency and government direction and can be a useful control over the security agency, to the extent that its work involves gathering evidence for prosecution. However, prosecutors in a State which are not, formally and in practice, a part of the independent judicial branch are nonetheless a part of the executive and as such can only be seen as an "internal" control.[36]

114. Where, for some reason, governmental control is weak, this may operate to strengthen the administrative control. On the other hand, a formal control structure on paper may naturally conceal a large degree of autonomy for the agency in practice. In one sense, a large degree of administrative control can be seen as a safeguard against dangers that the security agency becomes a tool in the hands of the government of the day.

f. Governmental control

115. As government departments are both "taskmasters" and "consumers" of intelligence, they cannot either be seen as an "external" control over a security agency.[37] A variety of factors influence the form and degree of ministerial or governmental control, i.e. to which Minister(s) the agency reports and how tight the governmental control which is exercised. The fact that

[36] See, *inter alia,* Recommendation Rec (2000) 19 of the Committee of Ministers of the Council of Europe on the role of public prosecution in the criminal justice system.

[37] See Lustgarten, L. and Leigh, I., *In From the Cold: National Security and Parliamentary Democracy*, (Oxford UP, 1994), p. 314.

intelligence cannot be neatly sorted into “internal”, “external”, “military” etc. can mean that an agency may have a right of access to, or a reporting responsibility to the Head of State /Head of government, in addition to, or instead of, the Ministers of Defence or the Interior.

116. Where there are different agencies with overlapping functions in internal security matters, e.g. where there is a civilian agency with no police powers, a police force with a degree of responsibility in security crime (e.g. as regards terrorism) and a paramilitary/gendarmerie force, parallel lines of responsibility may exist, to the head of government, the ministry of justice, and the ministry of defence. This, combined with the already mentioned integrated nature of security threats nowadays can cause problems of lack of transparency, overlapping responsibilities, and avoidance of responsibility.[38]

117. The degree of governmental control exercised depends upon a number of factors which can vary from State to State and from time to time in the same State. An agency may deliberately have been given a statutory, or even constitutional, degree of insulation from day to day governmental or ministerial control. Independence in practice can also arise in particular, where the government in the State is weak for some reason (e.g. governmental power in the State is continually changing hands because of political instability, or voting preferences and the electoral system often result in weak coalition governments). In most, if not all, States, the monopoly of specialist knowledge possessed by the agency will itself grant the agency a considerable degree of autonomy in practice from governmental control. There are examples in the past of agencies more or less setting their own security agendas, despite, in theory, strong governmental control.[39]

g. Particular accountability problems relating to International Co-operation between Intelligence Agencies

118. Treaties on mutual assistance between police, customs and judicial authorities are nowadays an important feature of the fight against transnational organised crime. Similarly, as already mentioned, improved international intelligence cooperation is necessary to combat terrorism in particular. However, this necessary improved cooperation can cause problems as far as concerns accountability for security services. Accountability arrangements tend to track the policies or actions of national security and intelligence agencies. Frequently, the legislation contains either express or implied limitations that inhibit oversight or review of arrangements made with the intelligence agencies of other countries.

119. The detention and interrogation of “enemy combatants” in Afghanistan and at Guantanamo Bay, extraordinary renditions, alleged secret detention centres, torture or the use of information obtained by torture in third countries have led to a growing number of inquiries and reports by national and international bodies.[40] Where foreign agencies operate without

[38] For a recent official inquiry identifying some such problems see the Dutch *De AIVD in beweging* (“The changing AIVD”) from the *Commissie Bestuurlijke Evaluatie AIVD* November 2004.

[39] See, e.g., the Swedish report Personalkontroll, Rapport till regeringen av Registernämnden beslutad den 16 December 1998, p. 75. In practice the question of which individuals had “leading positions” in an organization regarded as undemocratic – which would justify registering the individual in question in the security files – was delegated to the security police, with the result that very many members of the organization were registered. This security police reaction was understandable in a sense: the result was more or less inevitable once the government had identified a particular organization as dangerous to the State. For similar criticisms that policy making in the past has been made at a very junior level see Zybertowicz, A. An Unresolved Game: the Role of the Intelligence Services in the Nascent Polish Democracy, in Born, H., Johnston, L. and Leigh, I. (eds) Who’s Watching the Spies, Potomac, Washington, 2005.

[40] See, e.g. Venice Commission, Opinion on the International legal obligations of Council of Europe member States in respect of secret detention facilities and inter-State transport of Prisoners, CDL-AD(2006)009; Bericht der Bundesregierung (Offene Fassung) gemäß Anforderung des Parlamentarischen Kontrollgremiums vom 25. Januar 2006 zu den Vorgängen im Zusammenhang mit dem Irakkrieg und der Bekämpfung des Internationalen Terrorismus, at http://www.bundesregierung.de/Anlage965868/Bericht+der+Bundesregierung+-

permission in another State, then this will be in violation of the national sovereignty of this State, and depending on national law, may give rise to criminal responsibility. Leaving aside this extreme case, it is becoming clear that even collaboration between agencies in different States can give rise to serious concern. National systems of oversight or accountability were designed for a different era and to guard against different dangers of abuse (for instance, interference in domestic politics or civil society by the agencies). They do not address this concern.

120. Concrete examples of abuses involving international exchanges of intelligence are unlikely to come to light, although the recent Maher Arar case is in Canada is an exception.[41] The main obstacles that national accountability bodies face in this task are a combination of "plausible deniability" and lack of powers to supervise such arrangements. Where a security agency merely receives "anonymized" intelligence from an overseas agency with which it has an arrangement, it can argue that it is not responsible for how the information was obtained. A security agency might accept responsibility in theory where it had actively requesting a foreign agency to obtain information from a suspect by means which are not lawful in the receiving agency's State. The problem will be that this level of involvement can rarely, if ever, be substantiated. The receiving agency will almost invariably be able to argue that it had no knowledge of that illegitimate measures have been used to obtain the intelligence, and no reason to suspect that such measures were used. Allegations of illegal or unethical behaviour can be "plausibly denied" since the receiving agency was not responsible for them. A truthful but incomplete denial can therefore be given to any suggestion that the information was improperly obtained by the receiving agency.

121. Moreover, there can be strong incentives for the receiving agency not to inquire into how information was obtained. An agency in a country with limited foreign intelligence gathering capability may be dependent on friendly foreign agencies providing it with intelligence. If the receiving agency asks too many questions, it may well receive embarrassing answers, namely that the material was indeed obtained by unethical means. One could argue that the receiving agency should try to insist that the supplying agency certifies compliance with human rights standards, but the supplying agency may simply refuse.

122. The exercise of police power is primarily national. That means that whatever national restrictions which apply to obtaining information tend only to apply to actions within the territory or to direct actions by State officials. This leaves the clear possibility that an agency may benefit from intelligence collected overseas by another country's agency through means that it would not be legally permitted to use.

123. In so far as one agency supplies information to another country's agency, again accountability is flawed since the information is unlikely to result in a decision that can be directly traced to the supplying agency. Information may be supplied on terms that the source is not revealed to any other body, including the courts or whatever the oversight bodies exist in the receiving State. Even where this is not so the confidentiality of the source of the information may be protected either under legislation in the receiving country or through the actions of its courts in the name of not harming international relations. Where the legal systems of both the supplying and receiving agencies protect the secrecy of international relations in this way, the result is a vacuum of accountability. The supply of information to multi-lateral bodies- for example to the UN Sanctions Committee or, for EU States, under the EU Third Pillar bodies may also suffer from comparable defects of accountability.

+offene+Fassung.pdf; Parliamentary Assembly of the Council of Europe, Alleged secret detentions and unlawful inter-State transfers of detainees involving Council of Europe member States, report of the Committee on Legal Affairs and Human Rights, 12 June 2006, Doc. 10957; European Parliament resolution on the alleged use of European Countries by the CIA for the transportation and illegal detention of prisoners (2006/2200(INI)).

[41] The Commission of Inquiry into the actions of Canadian Officials in Relation to Maher Arar, Report of the Events Relating to Maher Arar, 3 volumes, 2006, http://www.ararcommission.ca/.

124. The case-law of the ECtHR is still developing in the area of the extent to which a State can, and should, bear responsibility for acts with an extraterritorial dimension. It is, however, already evident that a vacuum of accountability is not acceptable.[42]

VI. Accountability and the case-law of the European Court of Human Rights

125. The European Court of Human Rights has scrutinized parts of systems of accountability in a number of cases.[43]

126. The particular facts of the case provide a strict procedural framework for the Court and this means that it is limited to examining systems of accountability as indirect components of the requirements that a limitation on a given human right be for the "protection of national security", "in accordance with the law", "necessary in a democratic society" and accompanied by "effective remedies" at the national level. The Court is not therefore able to scrutinize the overall accountability system applicable in a State, in the same way as can a national commission of inquiry considering law reform.

127. The Convention institutions have been reluctant to give abstract definitions of Convention terms, and this has also been the case with national security.[44] The Court naturally refuses to accept that issues of security are "outside of the law", although it has also stressed that the Convention is not neutral as regards "enemies of democracy".[45] The Court is prepared to take a wide view of national security, holding e.g. that the German system of loyalty tests for teachers[46] and the Greek government's protection of "national cultural and historical symbols" fall within the concept.[47]

128. "Accordance with the law" means that the exercise of State power, in particular coercive power, must have support in statute law, subordinate legislation or case law. The Court has increasingly stressed the need for the law to satisfy qualitative criteria, in particular, minimum standards of foreseeability and for discretionary powers to be drafted carefully, identifying the addressees, the objects of the exercise of power, the limits, temporal and otherwise on its exercise etc. The problem in this area is reconciling the need for flexibility (above para 55) and the need for foreseeability. The "necessity" requirement is essentially a test of the proportionality of an infringement, and involves looking at the control system for preventing abuse of discretionary powers. Where the Court finds that a measure complained of is not "in accordance with the law", then it does not proceed to examine whether the measure satisfies the requirements of "necessity in a democratic society". The majority of cases relating to

---

[42] See, in particular, ECtHR, *Öcalan v. Turkey* judgment of 14 December 2000; *Bankovic and Others v. Belgium* and 16 other Contracting States decision of 12 December 2001; *Assanidze v. Georgia* judgment of 8 April 2004; *Issa and Others v. Turkey* judgment of 16 November 2004; *Ilascu v. Moldova and the Russian Federation* judgment of 8 July 2004. See also below Section V.

[43] See generally Cameron I., *National Security and the European Convention on Human Rights*, (Iustus, Uppsala/Kluwer, Dordrecht, 2000).

[44] The European Commission on Human Rights expressed the view that national security cannot be defined exhaustively. *Esbester v. UK*, No. 18601/91, 18 EHRR CD 72 (1993) and that in the first place it is for member States to decide whether it is necessary to criminalise particular conduct deemed to be damaging to national security. *M. v. France*, No. 10078/82, 41 D.R. 103, 117 (1985).

[45] See ECtHR, *Refah Partisi (The Welfare Party) and others v. Turkey* judgment of 13 February 2003, where the Court stated that Convention freedoms "cannot deprive the authorities of a State in which an association, through its activities, jeopardises that State's institutions, of the right to protect those institutions … some compromise between the requirements of defending democratic society and individual rights [is] inherent in the Convention system" (at para 96).

[46] ECtHR, *Vogt v. FRG* judgment of 26 September 1995, paras 49-51.

[47] ECtHR, *Sidiropolous v. Greece* judgment of 10 July 1998, para 38.

intelligence accountability have dealt only with the "accordance with law" requirement.[48] In several European States aspects of the legal basis have been found to be inadequate. This has given legislators the opportunity to address the principles that should govern this important area of State activity and to lay down limits to the work of such agencies. Where this opportunity has been taken properly the security and intelligence agencies have obtained increased legitimacy.

129. The requirement of "effective remedies" in Article 13 is a variable requirement. The more serious the alleged violation of a Convention right, and the more important the right is to the individual in question, the more remedies which should be available. However, in the first significant case involving security intelligence the Court dealt with, Klass v. FRG, the Court considered that Article 13 had a subsidiary character to the substantive rights in the Convention. The Court stated that "an effective remedy ... must mean a remedy which is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance".[49] Thus, Article 13 could not be interpreted so as to nullify the efficacy of the measures of secret surveillance already found to be compatible with the protection of privacy set out in Article 8.

130. The main Convention article which has given rise to discussions regarding the control systems for security intelligence is Article 8, and in relation to the specific issues of surveillance and records/screening. The leading case on security surveillance is the Klass case (see para 210 below), now supplemented by *Weber and Saravia v. Germany*.[50] As regards security records/screening, the leading case is *Leander v. Sweden*[51] now supplemented with *Segerstedt-Wiberg v. Sweden*[52] concerning remedies as regards security screening. In both areas there are also a number of Commission decisions.[53]

131. The ECtHR has furthermore delivered important judgments relating to the use of security material and effective remedies as regards deportations on security grounds (Articles 3 and 8, respectively where the deportee risks torture or inhuman treatment or the deportation interferes with family life)[54] and as regards the availability of judicial remedies for security decisions affecting "civil rights" and fair trial (Article 6).[55] In these cases the Court has required the creation of special mechanisms, reconciling the use of intelligence material with the right of fair proceedings, and as such they are relevant to intelligence accountability in the wide sense.[56]

---

[48] See, in particular, ECtHR, *Amann v. Switzerland* judgment of 16 February 2000; *Rotaru v. Romania* judgment of 4 May 2000.

[49] Op. cit. para 69.

[50] ECtHR, *Weber and Saravia v. Germany* judgment of 29 June 2006. See also ECtHR, *Tsavachidis v. Greece* judgment of 28 October 1997, the *Amann* and *Rotaru* cases, op. cit. and the post 2007-cases noted at para. 133.

[51] ECtHR, *Leander v. Sweden* judgment of 26 March 1987.

[52] ECtHR, *Segerstedt-Wiberg v. Sweden* judgment of 6 June 2006.

[53] See in particular *Hilton v. UK*, 12015/86, 57 DR 108 (1988), *Nimmo v. UK*, 12327/86, 58 DR 85 (1989), *Hewitt and Harman v. UK*, No. 12175/86, 67 DR 88 (1989) *Christie v. UK*, No. 21482/93, 78A DR 119 (1994), *Brinks v. Netherlands* No. 9940/04, 5 April 2005.

[54] ECtHR, *Chahal v. UK* judgment of 15 November 1996 and *Al-Nashif and others v. Bulgaria* judgment of 20 June 2002.

[55] ECtHR, *Tinnelly and McElduff v. UK* judgment of 10 July 1998; *Hulki Günes v. Turkey* judgment of 19 June 2003; *Monika Haas v. Germany* judgment of 17 November 2005.

[56] Intelligence material can naturally arise in other contexts, in particular as regards Article 5 (arrest and detention), see Cameron, I., 2000, op. cit., pp. 267-286.

132. As regards remedies, the ECtHR has stressed that, even in the context of national security, the remedy required by Article 13 must be effective in practice as well as in law.[57] The Court has drawn a distinction between the remedies which must be available in the context of measures which are unknown to the alleged victim, notably security surveillance, and measures such as deportation which are known. As regards the latter type of measure, the Court stated in *Al-Nasif v. Bulgaria* that "Even where an allegation of a threat to national security is made, the guarantee of an effective remedy requires as a minimum that the competent independent appeals authority must be informed of the reasons grounding the deportation decision, even if such reasons are not publicly available. The authority must be competent to reject the executive's assertion that there is a threat to national security where it finds it arbitrary or unreasonable. There must be some form of adversarial proceedings, if need be through a special representative after a security clearance. Furthermore, the question whether the impugned measure would interfere with the individual's right to respect for family life and, if so, whether a fair balance is struck between the public interest involved and the individual's rights must be examined."[58]

133. The Court does not define national security.[59] However, its case law gradually clarifies the legitimate scope of the term. It has displayed skepticism as to states' arguments that national security justifies a vaguer and more flexible approach to the requirements of foreseeability and accessibility. In Iordachi and others v. Moldova,[60] "national security" was one of the bases for surveillance. The Court criticized the lack of concretization of this and the other terms used in the applicable Moldovan law.[61] In Association for European Integration and Human Rights and Ekimdzhiev the Court referred to the need to take care "not to stretch the concept of "national security" beyond its natural meaning".[62] In both this and the Iordachi cases, the Court ruled that safeguards which supposedly operated on paper did not function in practice. The Court has developed its case law relating to strategic surveillance: a detailed analysis of this case law can be found in CDL-AD(2015)011. The ECtHR has decided three "rendition" cases, which indicate inter alia that serious failings occurred in the democratic system of control over the security and intelligence services involved.[63] There are other cases where the Court considers that security agencies have not been operating under effective controls in practice.[64] In some cases, the Court has considered that the regulation in subordinate legislation of a particular power was inadequate[65] or that a particular power has to be regulated.[66] It has decided several cases of

[57] ECtHR, *Al-Nasif*, op. cit., para 136.

[58] ECtHR, *Al-Nasif*, op. cit, para 138.

[59] "By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance" Al-Nashif v. Bulgaria, 20 June 2002, para. 121.

[60] No. 25198/02, 10 February 2009.

[61] Para 46.

[62] 28 June 2007, at para. 84. See also Soltysyak v. Russia 10 February 2011, concerning a prohibition on the possibility to travel abroad on the basis that the person had worked with secret defence projects is another example of the Court considering that a state has interpreted national security too extensively

[63] El-Masri v. the former Yugoslav Republic of Macedonia, No. 39630/09, 13 December 2012 (Macedonian responsibility for handing over a person (wrongly) suspected of terrorism to US agents, and the subsequent torture of the person in Afghanistan), Al Nashiri v. Poland No. 28761/11, 24 July 2014, Husayn (Abu Zubaydah) v. Poland, No. 7511/13, 24 July 2014.

[64] In addition to the Iordachi and others v. Moldova, and Association for European Integration and Human Rights and Ekimzhiev cases mentioned earlier, see also Association "21 December 1989" and Others v. Romania, Nos 3381/07 and 18817/08 24 June 2011 and Bucur and Toma v. Romania, No. 40238/02, 8 January 2013 (both concerning security surveillance). See also CDL-AD(2012)015, Opinion on the Federal Law on the Federal Security Service (FSB) of the Russian Federation .

[65] Shimovolos v. Russia No. 30194/09, 21 June 2011 (security data files – not regulated by statute, not in accordance with the law).

expulsion on national security grounds where the issue was the inability, in practice, to know the content of, and challenge, a security assessment.[67] Other cases have concerned the (in)admissibility of secret (torture) evidence.[68] Finally, it has considered that the failure of an intelligence agency to comply with the order of a data protection/freedom of information authority to reveal information can violate articles 6 and 10.[69]

VII. Internal and Governmental Controls as part of overall accountability systems

134. Internal control of security services is the primary guarantee against abuses of power, when the staff working in the agencies are committed to the democratic values of the State and to respecting human rights. External controls are essentially to buttress the internal controls and periodically ensure these are working properly.

135. Internal controls mean in the first place that the senior management of the agency must exercise efficient control in practice over the lower ranks of the agency. This would seem axiomatic, but the necessary "compartmentalization" of intelligence (see above para 86) makes effective control more difficult. Moreover, as already mentioned, some States experience problems of deeply divided security agencies. Senior management may not effectively ensure that authorization routines are followed. Worse, senior management may in different ways attempt to avoid taking responsibility for the actions of junior ranks. In such circumstances, relatively junior ranks can, in practice, end up setting policies, or deciding security priorities, exercise of power is concealed and consequently no one is held responsible for abuses of power. In any type of system this is not acceptable.

136. Procedures must be in place, and be followed, to ensure that requests for authorization for the use of special investigative measures and other measures which involve infringements of personal integrity such as the opening of personal files are approved at a high management level of the agency. There must be clear chains of responsibility, so that senior ranks know exactly what junior ranks are doing.[70] Junior ranks must also know that they will not end up bearing the responsibility for measures which have been ordered higher up in the hierarchy. This means that junior ranks must know what sort of measures are lawful and legitimate, so that dubious orders can be identified and officially queried.[71] This, in turn, requires training and, periodic retraining, of all staff in the importance of democratic and human rights values and in awareness of the dangers posed by security work to these values.[72] It means recruiting staff from relatively different political and social backgrounds.

---

[66] Bykov v. Russia, No. 4378/02. 10 March 2009 (bugging), Uzun v. Germany, No. 35623/05, 2 September 2010 (use of GPS tracking devices). See further Roman Zakharov v. Russia, No. 47143/06, pending before the Grand Chamber.

[67] Gulijev v.Lithuania**,** No. 10425/03, 16 December 2008 (Expulsion on the basis of a "secret" report of the State Security Department which was not disclosed to the applicant), Nolan and K. v. Russia, No. 2512/04, 12 February 2009 (Exclusion of foreign Unification Church activist from country supposedly on national security grounds: violation of Article 9).

[68] El Haski v. Belgium, No. 649/08, 25 September 2012, A and Others v. UK, No. 3455/05, 19 February 2009 (security detentions).

[69] Youth Initiative for Human Rights v. Serbia, No. 48135/06, 25 June 2013.

[70] See e.g. Hungarian Act CXXV of 1995 on the National Security Services, Section 26 "The internal organization and the detailed rules of operation of the national security services, as well as their chain of command shall be determined in a such a way that individual responsibility can always be established."

[71] See e.g. Hungarian Act CXXV of 1995 on the National Security Services, Section 27.

[72] See, by analogy, the judgment of the ECtHR in *Makaratzis v. Greece* of 20 December 2004, on the need for a legislative and administrative framework for the training of law enforcement officers on the use of firearms. See also Committee of Ministers Rec 2005(10) Chap II p.12.

137. The need for competent staff to deal with the complex, transnational problems posed by terrorism also requires a wide form of recruitment and training in social, political, religious contexts.[73] Retaining competent staff requires good working conditions. The staff of a security agency are subject to special psychological stresses as a result of the vital importance of their work and their need to keep matters secret, at times even from close colleagues.

138. Just as strong internal controls are a precondition for effective executive control over the security agency, a strong executive control over the security agency is a precondition for adequate parliamentary accountability, given that access by parliament to intelligence usually depends on the executive. The same is less true for expert review/authorization systems, to the extent that these have their own access to officials and intelligence material. However, as already mentioned, there can be particular difficulties in government exercising control over this particularly closed part of the public administration.

139. One means of exercising control is to provide that the head of the internal security agency is to be appointed by the head of the State or the Government. Other high officials in the system may also be appointed by an executive authority, which normally has the discretion to dismiss the head of the agency and other high officials. This power to hire and fire is intended to keep the agency under control of the executive.[74] This is a power which can obviously be abused and which therefore usually has to be subject to constraints (see below para 196 and Section VIIIE). However, the power to appoint and dismiss the head of the agency will often be insufficient to exercise control over the agency as a whole. As already mentioned, knowledge is a source of power, and security intelligence is, and has to be "compartmentalized" (see above paras 117 and 89). Particularly if the head of the agency is not himself, or herself, an expert in how security intelligence works, and if he or she cannot rely upon a loyal and efficient senior management, a variety of ways exist to keep the head of the agency wholly or partially in the dark about what the agency is doing.

140. The reverse problem can also emerge, namely that the head of an agency has had this position so long, that he or she not only fully controls the agency – which is obviously desirable – but exercises considerable influence over the government – which is not. The formal power to dismiss the head of the agency may not be sufficient, where the government, or administrative officials fear to use it, in case very embarrassing information collected by (or even suspected of having been collected by) the agency is leaked to the press or political opponents. To avoid this risk, some countries therefore provide for a maximum period of tenure for the head of the agency.[75]

141. In order to provide for impartial verification and assurance for the government that secret agencies are acting according to its policies, effectively and with propriety, 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.[76]

---

[73] Arar Commission, Report of the Events Relating to Maher Arar, Analysis and Recommendations, op. Cit. p. 327.

[74] Venice Commission, CDL-INF(98)6, p. 5.

[75] E.g. in Spain the period of tenure of the Director of the former Spanish intelligence agency, the Centro de información de la Defensa (CESID) was five years. See further, Giménez-Salinas, A. The Spanish Intelligence Services, p. 69 in Brodeur, J.P., Gill, P. and Töllborg, D., (eds*), Democracy, Law and Security: Internal Security Services in Contemporary Europe*, (Ashgate, 2002).

[76] UK Parliament, Intelligence and Security Committee *Annual Report for 2001-2*, Cm 5542: Appendix 3.

142. Such mechanisms are particularly prevalent in common law States, and the idea originates from the US intelligence community, which now has around a dozen inspectors-general. All are independent of the agencies concerned. There are, however, significant variations among them: some are established by legislation (for example, the Inspectors-General for the Central Intelligence Agency and the Department of Defense), others are set up by administrative arrangements. 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.

143. While the institution may have a common-law origin, the advantages it can bring of increased executive control means that it has been taken up by other jurisdictions.[77] Inspectors-General commonly operate within the "ring of secrecy": their primary function is not to provide public assurance about accountability, but rather to strengthen accountability to the executive. The Canadian Inspector-General is a clear illustration of this type of office and the Inspector-General is entrusted with unrestricted access to information in the hands of the Service in order to fulfill these functions (Canadian Security Intelligence Service Act 1984, Sections. 33.2 and 33.3). Likewise, in Bosnia and Herzegovina the Inspector-General exercises 'an internal control function' (Law of the Intelligence and Security Agency of Bosnia Herzegovina, Art. 32). 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 to report at least every six months to the Security Intelligence Committee and to keep the main executive actors informed of developments in a regular and timely fashion. The Inspector-General's powers include questioning agency employees and obtaining access to agency premises and data.

144. The function of an Inspector-General may be not only to strengthen executive control but serve as the responsible Minister's conscience.[78] An Inspector-General can also, as noted above, to report to, or in different ways assist, parliamentary or external expert bodies (see below para 241) or to play a role in complaints functions (see below para 254).

145. Some States have senior executive officials which are given a general supervisory authority over administrative agencies, which may even include the security agency. While such officials may, depending on the constitutional context, in practice operate with considerable autonomy from the government, the supervision they are able to exercise over a security agency will often be limited. This is because of the special nature of security intelligence, and the need to build up a relationship of mutual trust between the agency and the supervisor.

146. These last two factors strongly favour both a specialized and continuous supervision, rather than the ad hoc investigations an official with general supervisory authority would be able to deliver.

147. One example of a body exercising specialised and continuous supervision is the Austrian Rechtschutzbeauftragter. This is an independent expert appointed for a period of 5 years by the President of the Republic on the proposal of the government after having heard the presidents of the Parliament, of the Constitutional Court and of the Administrative Court. The position and tasks of the Rechtschutzbeauftragter are regulated by statute, and he/she reports yearly to the minister of the interior who transmits the report to the special Sub-committee of Parliament.

[77] E.g. in the Netherlands, the Supervisory Committee on the Intelligence and Security Services (SCISS) has called for the introduction of an Inspector-General for security, see Annual Report 2005-2006 of the SCISS, p. 8.

[78] Lustgarten, op.cit. p.68.

148. 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.[79] 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 scrutinize 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.
149. One area where the government (and parliament) will want particular reassurance is financial auditing. Both the executive and the parliament have a legitimate interest in ensuring that budgets voted for intelligence are spent lawfully and effectively A precondition for external auditing is obviously that clear internal rules exist on authorisation of expenditure and that these are followed strictly. [80]

150. As already mentioned, strengthening governmental controls over an agency carries with it certain dangers. A variety of mechanisms can be used to limit the potential for political manipulation and abuse of the agency. One method is 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. These provisions help against both improper pressure being applied on the head of the agency and abuse of the office. Hence, it is common to find provisions for security of tenure, subject to removal for wrongdoing.[81] Where staff from security agencies fear improper political manipulation it is vital also that they have available procedures with which to raise these concerns outside the organisation. These include the right for officials to refuse unreasonable governmental instructions (for example, to supply information on domestic political opponents) and whistle-blowing or grievance procedures.

151. There are also commonsense reasons for a formal separation between executive oversight and managerial control of the agencies and their operations. It will be impossible for political leaders to act as a source of external control if they are too closely involved in day-to-day matters and the whole oversight scheme will be weakened. There is the danger also of politicising the intelligence cycle, with the consequence that the analysis stage and the end-product will be less useful.[82]

152. This suggests that there should be a clear delineation of distinct but complementary roles for the executive and agency heads. Canadian legislation embodies the principle in the Canadian Security Intelligence Service Act 1984, referring to the Director of the Service having "the control and management of the Service" that is "under the direction" of the Minister. Similarly, Polish intelligence legislation clearly distinguishes between the respective competences of the Prime Minister and the Heads of the Agencies (Art. 7 Internal Security Agency and Foreign Intelligence Agency Act 2002).

---

[79] Born, H. and Leigh, I., *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, DCAF/Human Rights Centre, Durham, Norwegian Parliamentary Intelligence Oversight Committee, 2005, chapter 22.

[80] See below, Section VIII.E.

[81] See, e.g. Poland, Article 16, Internal Security Agency and Foreign Intelligence Act 2002 and Romania, Law 14/1992. The latter provides for the dismissal of the Director of the Romanian Intelligence Service and of the Foreign Intelligence Service is by vote of a joint plenary session of the two chambers of parliament, on the proposal of the President or at the initiative of at least 1/3 of the senators and deputies (see Secretary-General's report).

[82] See Gill, P., Politicization of Intelligence: Lessons From the Invasion of Iraq, in Born, H., Johnston, L. and Leigh, I. (eds), Who's Watching the Spies, Potomac, Washington, 2005.

153. As regards developments since 2007, experience shows that internal controls (paper trails, structural controls within the agency, factors promoting good professional ethics etc.) continue to be crucial. Without these, both internal and external oversight are dysfunctional. An illustration of this is the Senate Intelligence Committee's extensive report on the CIA which shows the limited role even powerful internal watchdogs – the CIA inspector-general – can play if s/he is not told the entire truth, or even actively lied to.[83]

VIII. Parliamentary accountability

154. A parliamentary body can be given the role of authorising different types of security operations. This is the case for the US, where the congressional committees must approve certain types of covert action. However, more common is that the parliamentary body is not part of the control machinery, but instead exercises different types of supervision or review. The term "oversight" – originating in the US is often used to denote parliamentary accountability, and the two terms will be used interchangeably in the present study.

A. In general

155. There are several reasons why parliamentarians should be involved in the oversight of security agencies. Firstly, the ultimate authority and legitimacy of security agencies is derived from legislative approval of their powers, operations and expenditure. Secondly, there is a risk that the agencies may serve narrow political or sectional interests, rather than the State as a whole and protecting the constitutional order, if democratic scrutiny does not extend to them. A stable, politically bi-partisan approach to security may be ensured therefore by proper control, to the benefit of the State and the agencies themselves. Furthermore, the involvement of parliamentarians can also help ensure that the use of public money in security and intelligence is properly authorised and accounted for; this is especially important where agencies' budgets have increased since 9/11.

156. Despite the strength of the argument for parliamentary oversight, there are some dangers. The agencies may become a political football - inexperienced parliamentarians may air accusations and conspiracy theories in the chamber in order to attract publicity. There is the possibility also of sensitive material disclosed to parliamentarians being leaked to the press. The most effective scrutiny of security is detailed and unglamorous work that may be unattractive to politicians who seek immediate public credit for their contribution. Where the institutions of the State are weak (e.g. there is serious corruption in the parliament), granting the parliament insight into, or even a degree of control over, the operations of the security agency may risk compromising it and the secrecy of its work. Where there is a major lack of political stability in the State, resulting in frequent changes of government or very large changes in parties represented in the parliament, it will be difficult to secure the necessary professionalism from MPs and difficult for MPs to build up the continuity of expertise necessary to exercise a proper degree of control over the arcane world of intelligence. A security agency's job is to keep secrets. It is, or should be, good at this. Where it wishes to conceal information from an amateur, part-time investigator, for whatever motives, good or bad, it is probably able to do so. This factor considerably reduces the value of one of the usual parliamentary means of obtaining information from the executive, or executive agencies, namely parliamentary questions. The same point often holds true for another mechanism of parliamentary control, namely an ad hoc parliamentary commission of inquiry. Such commissions can be powerful investigative tools in many States, with considerable powers of obtaining documentation and examining witnesses. However, the difficulty in penetrating the intelligence world for parliamentarians not continuously in touch with it can considerably reduce the value of ad hoc parliamentary commissions of

[83] Op. cit. For an analysis of when inspectors-general can serve a useful purpose see Sinnar, S., Protecting Rights From Within? Inspectors General and National Security Oversight, 65 Stanford Law Review 1027 (2013).

inquiry.[84] For this reason, the rest of this section concentrates on the standing, continuous, method of control by a parliamentary oversight body, however designated, designed to deal with security and intelligence matters in particular.

157. The constitutional dimension must be borne in mind here. In a presidential system, the elected president also has a source of democratic legitimacy. The constitution may expressly or impliedly reserve control over internal security matters largely, or wholly, to the executive (with the possible exception of a minimal budgetary control granted to the parliament). An antagonistic relationship with the parliament over "ownership" of internal security can arise, especially where the political majority in the parliament differs from that of the president's party. Oversight over internal security can become party politics. For some or all of these reasons, a State may choose to establish an expert oversight body instead of a parliamentary body. Alternatively, in States where there is a second chamber where members are less party political or where there is longer continuity of membership, a State may choose to establish the body in the second chamber.

B. Mandate and functions of the parliamentary oversight body

158. From a comparative international perspective, the most frequent arrangement is for parliament to establish a single oversight body for all the major security and intelligence agencies, rather than having multiple oversight bodies for specific agencies.

159. The advantage of a single oversight body is that it facilitates seamless oversight. Since different parts of the intelligence machinery work closely with each other, an effective oversight body needs to be able to cross agency boundaries. Correspondingly, oversight arrangements designed to track separate agencies can be hampered if they lead in the direction of information supplied by or to an agency outside the legal range of the oversight body's sphere of operation.

160. There are some significant divergences from the single all-agency parliamentary oversight body model, 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 mandate covers only part of the intelligence establishment. The Defence Intelligence Staff, the Joint Intelligence Committee and National Criminal Intelligence Service all fall outside the formal mandate although in practice, and with the cooperation of the government, the Committee has also examined their work.[85]

161. There is considerable variation in the remit of these parliamentary oversight bodies. Some have the power to scrutinize the operations of intelligence agencies: for example, the US Congressional oversight committees and the Control Panel of the German Bundestag both have the right to be briefed about the operations of the agencies.[86] Where a parliamentary oversight body has the ability to examine intelligence operations it is clearly able to report with greater credibility. Even where an oversight committee is given enhanced powers (for example, to compel the production of evidence) it is unavoidable, however, that some operational detail will have to be excluded from its reports to parliament and the public. The potential

[84] American political scientists have called periodic inquiries a "fire alarm" type of control as opposed to the continuous low-key "police patrol". See McCubbins, M. D. and Schwartz, T., Congressional Oversight Overlooked: Police Patrols vs. Fire Alarms, 28 American Journal of Political Science, 165-179 (1984).

[85] Leigh, I. 2005, Accountability of Security and Intelligence in the United Kingdom, in Born, H., Johnston, L. and Leigh, I. (eds), op. cit.

[86] German Bundestag, Secretariat of the Parliamentary Control Commission, *Parliamentary Control of the Intelligence Services in Germany*, Berlin: Bundespresseamt, 2001 and generally; Hirsch, A. Die Kontrolle der Nachrichtendienste : vergleichende Bestandsaufnahme, Praxis und Reform, Berlin : Duncker & Humblot, 1996.

disadvantage of an oversight body working within the ring of secrecy in this way is that there may be a barrier between it and the remainder of parliament.

162. Too close a relationship between the oversight body and the agencies it is responsible for overseeing may be a potential danger also. Consequently, while a legal requirement that the committee be notified in advance of certain actions by the agency apparently strengthens oversight, it could also inhibit the oversight body from later criticism of these operational matters.[87] Where the oversight body is tasked with approving certain types of operation, e.g. surveillance operations, this makes it part of the control system, meaning that it cannot also perform the function of a complaints body; it should not be investigating itself.[88]

163. It can also be noted in this context that a legal requirement of advance notification of a certain type of operation can serve lull the oversight body into a false sense of security. It is difficult exhaustively to define all the types of operation which notification should cover. New types of threat, and new types of response, emerge. By administratively redefining an existing power or authority, an agency may be able to engage without notification in the kind of operations it was originally intended notification should cover. This is another illustration of how important internal controls, are, and staff commitment to democratic values.[89]

164. Conversely, a parliamentary oversight body limited to scrutinising the policy, administration and finance of the agencies (as is the case in the United Kingdom) is able to work more readily in the public arena and can operate under fewer restrictions on what is disclosed.

165. This approach may detract however from parliamentary scrutiny of the security and intelligence agencies' *effectiveness* in executing government policy. To assess that, access to some operational detail is necessary. This applies also to auditing issues of legality (including compliance with the Constitution, which is the case in Romania)[90] or the agencies' respect for human rights (as is the case with the Norwegian Committee[91]). Unless based on clear evidence about the behaviour of the agency concerned, parliamentary oversight will appear hollow.

166. Even where a parliamentary body has access to operational detail, unless it is part of the approval process (see below para 198) this detail is likely to be ex post facto, and will rarely concern forthcoming or ongoing operations. However, the problem consists in knowing when an operation ceases. The ongoing nature of security operations can easily be used as an excuse to avoid the scrutiny of an oversight body. Again, this requires building up a relationship of mutual trust between the agency and the oversight body.

---

[87] This was the experience of the former Norwegian oversight body, see the Dokument No. 15. Rapport til Stortinget fra kommisjonen som nedsatt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere, avgitt till Stortingets presidentskap 28 mars 1996 ("Lund Report"), pp. 434-439.

[88] See also below, para 257.

[89] In the US, for example, the executive is legally obliged to keep the Congressional intelligence committees fully and currently informed of the intelligence activities. Moreover, the US Congressional Oversight Provisions demand that the President keeps the Congressional intelligence committees informed about all covert actions operations, including significant failures, before initiation of the covert action authorised by the Presidential finding (United States Code, Title 50, Section 413). In the Intelligence Authorization Act of 1991 the President promised to continue to inform the Congress in advance in most instances, but he insisted on flexibility in times of crises. See further Johnson, L., Governing in the absence of angels: On the practice of intelligence accountability in the United States, in Born, H., Johnson, L. and Leigh, I., op. cit., pp. 64-65.

[90] Secretary General's report, reply from the government of Romania.

[91] The Act relating to the Monitoring of Intelligence, Surveillance and Security Services. Act No. 7 of 3 February 1995; Sejersted, F., Intelligence and Accountability in a State without Enemies, in Born, H., Johnston, L. and Leigh, I. (eds), op. cit.

167. The powers given to an oversight body will obviously be influenced by the tasks delegated to it. This explains why the approach in some States has been to give a wide remit and then to detail specific matters which may not be investigated.[92] By contrast, other States give comprehensive lists of oversight functions of the parliamentary oversight body (e.g. the US, Section 13, United States Rules of the US Senate Select Committee on Intelligence). The scope for the executive to determine the exact mandate of a parliamentary body may naturally be limited by the constitution, or constitutional traditions regarding parliamentary privilege.[93]

168. 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). Access is also related to the question of the security screening (vetting) of members, considered in the next section.

169. Systems vary also in how they handle reporting of sensitive material. For example, in the US, the onus of being informed not only rests with the oversight body, but with the executive as well. Another useful example is the Norwegian hybrid independent/parliamentary control committee which may request the information it feels it requires, including operational information. However, where the security agency notifies the committee that such information is particularly sensitive, the committee in practice exercises restraint in requesting it. The committee retains the last word in deciding which information it requires, but the government can, ultimately choose not to order the security agency not to release this. This would involve an open conflict with the committee, which all parties want to avoid.[94] As already mentioned, such a system presupposes a high level of mutual trust between the committee and the security agency.

170. How great an independent investigative capability of the oversight body should have depends on its functions and the degree to which it feels it can rely on the material it receives from the government and the security agencies being monitored. Where an oversight body examines more than policy, it should have access to at least a residual investigative capability of its own. This involves having some staff. On occasion, security officials might have to be interviewed systematically, and their replies compared and analysed. Information an oversight body has received, e.g. a threat assessment, might on occasion usefully be compared with other sources, e.g. academic studies and comparative material.

171. Some countries have stipulated explicitly that the oversight body is also entitled to obtain information and documents from experts, e.g. in think tanks or universities. For example, in Luxembourg the Parliamentary Control Committee can decide, with two-thirds majority and after having consulted the Director of the Intelligence Services, to be assisted by an expert.[95] This allows for alternative viewpoints to those of the government and the services to be considered. Another useful source of information is the public reports of the different national parliamentary and expert bodies. Although the constitutional context will vary considerably between States, there may be great similarities in the types of intelligence and security issue which arise, and the problems involved in oversight. As explained below, there may even be

[92] E.g. the United Kingdom, Intelligence Services Act 1994, Section 10. Cf Germany, PKGrG § 1(1).

[93] See e.g. Germany where the Law on the Parliamentary Control of Activities of the Federal Intelligence Services 1978, as amended, (hereinafter PKGrG) § 4 para 2. provides that the number of the PKGr's members, its composition and its working practices shall be laid down in a parliamentary resolution of establishment.

[94] See Sejerstedt, op. cit.

[95] Article 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.

scope for more institutionalized cooperation between national oversight bodies, even on more confidential issues, within the limits of the secrecy legislation which governs their activities.[96]

172. Whatever the degree of access to information they are given, oversight bodies obviously need to make great efforts to protect from unauthorised disclosure information and documents related to sensitive issues (about persons) and/or about national security. 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. Unauthorised disclosure by a member of an oversight body may involve penalties under applicable secrecy legislation.[97] It is also, however, partly a matter of proper behaviour of the members of the oversight body in dealing with classified information with care and attention. Leaks of sensitive material will almost certainly adversely affect oversight.

173. It is possible to provide for different mechanisms for assisting a parliamentary body in obtaining information. As already mentioned, a parliamentary body can have its own staff, which naturally will need expertise in the area. This will usually mean that these have previously served in intelligence-related functions, although to avoid divided loyalties and too close a relationship with the agency being supervised ("agency capture"), it will not usually be appropriate to have staff members who are still serving in the agency, and are simply seconded to the expert body.

174. Staff who are former intelligence officials, as long as these are loyal to the oversight body, can also be important in building up mutual trust between the oversight body and the security agency. Such staff can also serve an important purpose in maintaining continuity of expertise, where the composition of the parliamentary body changes.

175. An alternative to, or an addition to, giving an oversight body its own staff is to permit it to task an executive-appointed Inspector-General to investigate a particular issue and report back to the oversight body. An Inspector General can also be given a function of submitting a general report to parliament as a whole, as is the case in South Africa. An office of this kind in effect bridges the ring of secrecy by providing public assurance that an independent person with access to the relevant material has examined the activities of the security or intelligence agency even if, as is inevitably in the case with a general report, most of the material on which an assessment of the agency's work is made has to remain unpublished. In some States, however, there may be constitutional difficulties in having an executive officer, responsible to the government, also serving on occasion parliament or a parliamentary body.

176. One final issue to be noted in relation to the mandate of the oversight body concerns its report. In most cases, a parliamentary body will report to parliament, and will be able to decide both when it reports, how often it reports and the content of its report. Publicity, or the threat of it, is a means of trying to ensure that the government is responsive to whatever problems the oversight body has identified, and whatever criticism or recommendations it makes for dealing with these. Having said that, the content of a report can obviously be sensitive and different methods exist for reconciling openness with the need for security. The German system can be mentioned in this respect: the report of the Control Panel is secret, but the panel can, by 2/3 majority, waive this requirement.[98] In this way, it retains an important bargaining tool in its relationship with the government, at the same time as minimizing the risk of criticism being made on party political grounds.

---

[96] See also below, para 194.

[97] See, e.g., the already mentioned Norwegian Act relating to the Monitoring of Intelligence, Surveillance and Security Services, 1995, Section 9. See also United States Code Section 413. General Congressional Oversight Provisions, (d).

[98] PKGrG, as amended, § V, 1.

177. Even where a parliamentary committee has the final word on the content of a report, its need for a professional working relationship with the security agency will mean that it can usually be expected to accept the security agency's request not to reveal particular information. A parliamentary body which only has the power to produce an annual report, and not a special report, is unable to draw public and parliamentary attention to activities which require an urgent response. A parliamentary body which cannot control the timing of its report risks, at least on occasion, its report losing all political impact. Finally on reports, where these identify problems, then some follow-up response from the agency and/or the government is obviously expected. The oversight body must be free to respond to the follow-up and give its views on whether identified problems are, or are likely to be, solved.

C. Membership of the Oversight Body

178. The arrangement for appointing members of an oversight body will inevitably be a key factor affecting public confidence in and the success of the arrangements. Autonomy enhances legitimacy in two distinct ways. First is the question of "ownership" of the oversight arrangements - for example, reflected in the power of the parliament to make appointments and cross-party representation. Secondly there is the need for a clear demarcation between the oversight body and the agencies overseen; this is often part of a more general "civilianisation" of transitional societies. The presence of former members of the security agencies on the oversight body (as opposed to simply on the staff of the oversight body) may be a particular difficulty which arises in some transition States and is likely to undermine confidence, especially where the services were implicated in maintaining a repressive former regime. Overlap of this kind is best avoided - if necessary by a legal prohibition.

179. There is a distinction between those States where legislators themselves take on the oversight role through a parliamentary committee (for example, Argentina, Australia, South Africa, United Kingdom and the USA) and those where an expert committee has been set up outside the parliament, the members of which are not parliamentarians, but which reports to parliament (e.g. Belgium, the Netherlands and Portugal). As already mentioned, hybrid bodies can exist (such as in Norway or Sweden), and some States have both parliamentary committees and expert bodies (such as Germany). Expert bodies are considered in Section X.

180. In some systems, parliamentary rules on committee membership generally may mean that there may be little scope for a "tailor-made" parliamentary oversight body. As already mentioned, considerable time is usually needed to build up expertise in security matters. This would be undermined by a rule requiring rotation of committee members every parliamentary term. The ability of the oversight body to command the respect of both the security agency being monitored, and from parliamentary colleagues and the public, will usually be enhanced if its members are relatively experienced and senior. However, seats on committees are often distributed within parties according to seniority, and as there is often little public credit to be derived in this area, there is an evident risk that senior members may choose other committees on which to serve. Another problem relates to constitutional doctrines on parliamentary privilege. The parliament may refuse to allow the vetting of its members. This in turn will mean that the oversight body will face difficulties in its access to information.

181. Variations exist concerning the appointment of members of parliamentary oversight bodies. The head of government may appoint (in the case of the United Kingdom, after consultation with the Leader of the Opposition, see Intelligence Services Act 1994, Section 10). The executive may nominate members but parliament itself appoints (as in Australia; after consultation of other party leaders by the Prime Minister, Intelligence Services Act 2001, Section 14). In other countries responsibility for appointment rests solely with the parliament, as

in Germany and Norway.[99] It can be noted that in Germany, in order to improve legitimacy, the Bundestag votes by majority to accept each individual member of the Parliamentary Control Commission.[100] Finally, although traditions vary within parliamentary systems concerning the chairmanship of parliamentary committees, the legitimacy of a parliamentary oversight body is usually enhanced if, rather than being appointed by the government, the chair is chosen by the committee itself. Legitimacy is also strengthened if the chairman or chairwoman is a member of the opposition (as in Hungary, Section 14, 1, Act No. CXXV of 1995 on the National Security Services), or if the chairmanship rotates between the opposition and the government party (as is the German practice).

D. Oversight and International Co-operation

182. As previously explained, there can be a vacuum of accountability as regards international cooperation in security matters. Legislators may be able to aid accountability by creating a legal framework in which co-operation with foreign agencies is only permissible according to principles established by law and where authorised or supervised by applicable parliamentary, or expert control bodies.

183. As the Secretary General has pointed out in his report, this is an area where there are relatively few known examples of rules, agreements or best practices. The Venice Commission will therefore rather try to identify abstract models allowing an adequate oversight of international co-operation.

184. As regards a foreign agency's exercise of public power (e.g. use of special investigative means, arrest, detention, interrogation) in another State's territory, it is vital that this, if it is to be allowed at all, only occurs in accordance with applicable constitutional rules on transfer of authority.

185. Limited transfers of public power are a feature of a number of modern treaties on police and customs cooperation.[101] However, it is vital that the procedure to make a grant of permission to foreign security agencies to exercise police, or security, powers is set out in the constitution, or at least in statute. Decisions to grant authority in a specific case should normally be made only by the competent authority of the State, which will usually be the government, or a government minister, and properly registered.

186. Accountability structures must be in place to ensure that a foreign security agency is not granted permission to exercise security or police functions in another State by junior or middle-ranking officials of that other State. Administrative, and where applicable, criminal responsibility should apply to unauthorised attempts to transfer police or security powers, or passivity when an official knew, or should have known about a foreign agency's unauthorised exercise of police or security powers in the territory of the State. The Secretary-General's report recommends that parliamentary bodies oversee all such decisions to transfer police or security powers. The Venice Commission considers that, although there may, exceptionally, be grounds for not notifying the parliament in advance of a transfer of authority to exercise police or security powers in a specific case, there must afterwards be full governmental accountability to the parliament for all such decisions. [102]

---

[99] See respectively PKGrG, § 4 para 1, Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS), 1995, Section 1.

[100] PKGrG § 4 para 3.

[101] See, e.g., Article 41 of the Convention applying the Schengen Agreement of 14 June 1985 between the governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, 1990, 30 I.L.M. 84 (1991).

[102] See, e.g., the Law on the Intelligence and Security Agency of Bosnia and Herzegovina, 2004, Articles 70 and 71, Secretary-General's report.

187. As regards the question of transfer of data, this should be regulated in statutory or other rules to avoid a vacuum of responsibility. Both the supply and receipt of data must be regulated by agreements in writing made by the proper authorities.[103] These should be submitted to parliamentary or expert oversight bodies.[104] Conditions should be attached to intelligence transferred. Limits must be placed both on the type of intelligence which can be transferred[105] and requirements must exist to check the reliability and accuracy of the intelligence, before it is transferred and also, for a receiving agency, to check reliability and accuracy when information is received from another State.[106] An example of a supply rule can be found in the German statute governing the BundesVerfassungsschutz, namely "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."[107]

188. Another, more far-reaching method is to require that information should only be disclosed to foreign security and intelligence agencies or to a supranational body 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).[108] As regards receipt of information, then it should be held subject both to the controls applicable in the country of origin and those standards which apply under domestic law.[109]

189. Foreign-source data should in principle not be excluded from the supervision of whatever data monitoring arrangements exist for data of national origin. However, it may be that especially stringent security arrangements may be permissible for access to such data.[110] The complicating factor is that, as already mentioned, assessing the reliability of

---

[103] See, e.g. the Dutch Intelligence and Security Services Act 2002 (De Wet op de inlichtingen- en veiligheidsdiensten) Article 36(1)(d), 40(1) and 42.

[104] See e.g. Canadian CSIS Act, Section 17(2) which requires that the oversight body, the Security Intelligence Review Committee (SIRC) be given copies of all CSIS agreements with foreign governments and international organizations.

[105] See, e.g. Article 9 (conditions and limits on supply of data) of the Agreement on Co-operation Between the Republic of Bulgaria and the European Police Office http://www.europol.europa.eu/legal/agreements/-Agreements/15977.pdf which specifies inter alia that "Personal data revealing racial origin, political opinions or religious or other beliefs, or concerning health and sexual life as referred to in Article 6 of the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data shall only be supplied in absolutely necessary cases and in addition to other information."

[106] See Article 10 of the Europol-Bulgaria Agreement, ibid. (assessment of the source and of the information). See also Arar Commission, Report of the Events Relating to Mahar Arar, Analysis and Recommendations, op. cit, p. 334.

[107] Bundesverfassungsschutzgesetz (BVErfSchG), Germany, 2002, Art. 19 (Unofficial translation).

[108] See e.g. Law on the Intelligence and Security Agency of Bosnia and Herzegovina, 2004, Article 65. A similar purpose could obviously be achieved if common standards could be agreed upon, assuming that these are not the "lowest common denominator".

[109] See Born H. and Leigh, I. *Making Intelligence Accountable: Legal Standards and Best Practice*, chapter 12.

[110] The European Commission on Human Rights accepted in Volpi v. Switzerland (No. 25147/94, 84 DR 106 (1996)) as regards transfer of data that particularly stringent restrictions can apply to allowing access to foreign-source data. However, it meant that foreign-source data could be excluded from members of the public who had been granted access to their own (no longer active) security files, not excluding access to such information to even the State's data protection bodies.

intelligence often involves looking at the "raw" intelligence material, not simply the "refined" product. The same applies to assessing the lawfulness of the methods for obtaining the information (ill-treatment during interrogation etc). A foreign agency may be prepared to transfer the product, e.g. that it considers a particular person to be linked to terrorism, or that an attack on a given target imminent, but not the basis for this product.

190. The situation is likely to arise increasingly that a supervisory authority or oversight body in one State is denied access to important foreign-source data which forms part of the reasons behind the general policies or specific operations of its own security agency and which it accordingly considers that there is a pressing need to examine.

191. Where a supplying agency refuses to accept that the information supplied is subject to the standards and supervision applicable in the receiving State, there are a number of options. The first is that the receiving agency is required to refuse to accept information which the sending agency would refuse to permit the supervisory body to examine, if it chooses to do so. This option will be very unpopular with the receiving agency, especially if it is in practice partially dependent on foreign-source data to do its job of securing the security of its State and individuals in it.

192. The second option is that the supervisory authority or oversight body in the receiving State accepts that it has no access to the raw material or even the refined product transferred, but that it instead accepts a certification issued by whatever equivalent independent supervisory authority or oversight body exists in the sending State that the data is reliable according to the standards applied in the sending State, and that it was lawfully obtained.

193. This option will not exist inter alia where transferring data to, or receiving data from, a State with a suspect human rights record, as there will be no independent supervisory body in the transferring State. In such cases, where the agency nonetheless feels that security considerations require such transfer/receipt of data, it should be a requirement on the agency to take into account the human rights implications of this transfer/receipt before it takes place, and to mitigate whatever risks might arise as a result of such cooperation.[111] This latter option is not optimal, but it is a minimum standard which would reconcile security, and human rights concerns.[112]

194. Finally, it should be stressed that the networking which security agencies engage in is a legitimate, and necessary, response to the problems of network threats, such as some modern forms of terrorism. The correct response on the part of national parliamentary oversight and/or expert oversight bodies which exist is also to engage in networking. Parliamentary and expert bodies may be able to overcome hurdles to accountability by sharing information that they acquire about intelligence co-operation, obviously within the limits of the secrecy rules applicable to them. At the very least, they can exchange information on "best practices" in general terms on trends and problems which have emerged in their work and in making available to one another the published evidence from equivalent investigations and reports. A model for such cooperation can be found in the periodic meetings which are held of police oversight bodies in European States.[113]

---

[111] Arar Commission, Report of the Events Relating to Mahar Arar, Analysis and Recommendations, 2006, p. 348.

[112] It would not, however, solve the problem of transfer of data by supranational bodies, unless and until supranational supervisory bodies are created. Having said this, the supranational bodies which do exist have little or no independent intelligence gathering capacity at the present time, and thus mainly, or exclusively, receive information.

[113] See, for the most recent published conference of Police Monitoring and Inspection Bodies, http://www.igai.pt/publicdocs/Papers_Conference2005.pdf. [note: regarding developments since 2007 there is ad

E. Other Areas where the Parliament can be given a role in Accountability

195. The purpose of embodying checks and balances on executive governance of the agencies is to enlist either a cross-section of political opinion or to involve politically neutral institutions. In both cases, the legitimacy of the agency, and the quality of its decision-making, may be improved. These checks may take two basic forms: external approval or confirmation of certain decisions or a, weaker, duty to inform external actors of sensitive or controversial matters. The mere existence of such duties may serve as a deterrent and act as safeguard for the agency.

196. External involvement or scrutiny of the appointment of the Director of the security agency can be a safeguard of kinds. The process of appointment of an agency head can be used to reinforce and guarantee the status of the position and to ensure the necessary qualities of leadership, integrity and independence. In some countries (for instance, the United Kingdom and Sweden) the safeguards against abuse in official appointments such as this rest on conventions which, if broken, lead to political criticism. Other countries employ formal confirmation or consultation procedures, to allow the parliament to either veto or express their opinion on an appointment. There may be a constitutional requirement either that official appointments must be approved by parliament or, at least allowing them to be blocked by a parliamentary vote (e.g. the practice in the US). Arrangements to achieve a broad political backing for the Director's appointment may include swearing the oath of office before the chairman of the parliamentary committee (as in Belgium, Act Governing the Supervision of the Police and Intelligence Services, 1991, Art. 17).

197. Another area for safeguards concerns political instructions. A legal requirement that certain ministerial instructions be put in writing[114] can act as an aid to accountability by preventing "plausible deniability" and even some questionable instructions from being given in the first place, because to do so would involve a "paper trail".[115] In addition, a requirement that ministerial instructions must be disclosed outside the agency may act a checking device. Examples can be found in Canadian law, which requires them to be given to the Review body, and Australian legislation, requiring them to be given to the Inspector-General of Intelligence and Security as soon as practicable after the direction is given (Canadian Security Intelligence Service Act 1984, s. 6(2), and Australian Inspector-General of Intelligence and Security Act, 1986, Section 32B, respectively). As already noted (see above paras 120-123), a paper trail is especially important as regards international cooperation arrangements.

198. One important consideration in maintaining a bi-partisan approach to security and intelligence is to include prominent opposition politicians within the "ring of secrecy". Such constitutional or statutory requirements can be found in a number of countries.[116] The danger of such briefings is cooption. It becomes more difficult later to criticize a policy – even one of dubious legality – of which one has previously been informed.

---

hoc cooperation between several of the oversight bodies in Europe. See also the initiative regarding the creation of a European Network of National Intelligence Reviewers, http://www.ennir.be/]

[114] See e.g. Act on the National Security Services 1995, Hungary, Section 11, the Dutch Security and Intelligence Services Act 2002, Article 19 and the Canadian Security Intelligence Service Act 1984, Sections 7(1) and (2).

[115] See above para 132. See also the Australian Intelligence Services Act 2001, s. 8(1) which requires the ministers responsible for the Australian Secret Intelligence Service, and the responsible Minister in relation to the Defence Signals Directorate, to issue written instructions to the agency heads dealing with situations in which the agencies produce intelligence on Australians.

[116] For example, in Sweden there is a formalised mechanism in the Instrument of Government Chapter 10, Section 6 for briefing the leaders of the opposition parties of important home and foreign policy matters in the Council on Foreign Affairs (Utrikesnämnden). A similar duty to inform periodically opposition parties of major security issues can be found in Portugal, Internal Security Act, Article 7 (Secretary General's Report).

199. Another role for parliamentary control is audit. The difference between the auditing of security and intelligence services from other public bodies is primarily in the arrangements for reporting. In many countries, the public annual reports of the security and intelligence service (e.g. in the Netherlands) or of the parliamentary oversight body (e.g. in the United Kingdom) include statements about the outcome of the financial audits. Special reporting mechanisms are usually in place, designed to protect the continuity of operations, methods and sources of the services.[117] However, as with the handling of complaints, it requires some ingenuity to devise systems for protecting secrecy while nevertheless ensuring that auditors have the wide access to classified information necessary to certified whether the services have used government funds within the law. Understandably, limited restrictions to protect the identities of certain sources of information and the details of particularly sensitive operations may be imposed on the access granted to an Auditor-General.[118] Even here, an Inspector-General can have a role to play.

F. Developments since 2007

200. There are a number of national reports and other sources indicating that parliamentary oversight has not worked as well as expected, in other words that accountability problems are greater than previously perceived.[119]

201. A number of states have, since the beginning of 2007, introduced improved parliamentary controls. France introduced a parliamentary oversight body (the Délégation parlementaire au renseignement, DPR) in 2007.[120] This is an eight-person body, composed of four members from the Senate and four members from the National Assembly. It has a mandate to follow the overall activity and means of the specialized services. It can call in for hearings the Prime Minister, Ministers and heads of the services concerned, but not more junior officials, and it has no other formal investigative powers. It produces short annual reports. The mandate and powers of the DPR have been criticised as inadequate and its membership as unconducive to serious oversight (the chairs of the Senate and Assembly Law and Defence committees sit ex officio).[121]

---

[117] For example, in Georgia, a group of five members of parliament carries out budget control over the special programs of the secret service (Secretary-General's report). In the United Kingdom only the Chairman of the Public Accounts Committee and the Intelligence and Security Committee are fully briefed about the outcome of the financial audit (including the legality and efficiency of expenditure, occurrence of possible irregularities, and whether the services have operated within or have exceeded the budget).

[118] In Spain, in accordance with article 11 of the law 11/2002 a special Committee in the Parliament is established to control CNI´s budget and be informed generally about its activities and the progress of tasks given to it by the Government. The Director of CNI attends to the Committee on his or the Committee's request. The only official secrets kept from this committee are the CNI's sources and means of gathering information and the information received from foreign intelligence agencies or international organisations. For other models see Born and Leigh, op. cit. chapter 20.

[119] The US Senate Select Committee on Intelligence report on the CIA Detention and Interrogation programme (op. cit), is an illustration of this, as is the ECtHR case law (above section VI) regarding the inadequacy of parliamentary oversight of surveillance in Rumania.

[120] Amending article 6 nonies, Ordonnance no. 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.

[121] See France, Assemblée Nationale, Rapport D'information Déposé en Application de L'article 145 Du Reglement par la Commission des Lois Constitutionnelles, de la Législation et de L'administration Générale de la République, En Conclusion des Travaux d'une Mission d'information (1) Sur L'évaluation du Cadre Juridique Applicable Aux Services de Renseignement, Enregistré à la Présidence de l'Assemblée nationale le 14 mai 2013 which also makes a number of reform proposals. Having senior members of parliament sit in an intelligence committee has certain advantages (above para. 180). The problem is that their other duties (particularly if they are the chairs of other committees), can mean that they have little time to devote to intelligence oversight.

202. Germany made three significant improvements in its parliamentary oversight in 2009, in addition to the symbolically important one of enshrining this scrutiny in the Constitution (Article 45d GG).[122] First, a duty was placed on the government actively to provide accurate and complete information to the Parliamentary Control Panel (Parlamentarisches Kontrollgremium, PKGr). Its staff was increased, and panel members were also permitted to bring in their own (security-cleared) staff to assist them. Finally, a whistleblowing function was introduced: intelligence staff can now approach the Panel directly, without having to go through official channels.

203. The parliamentary supervision in Denmark has been strengthened, particularly over the budget of the Security Police and the Military Intelligence Service. The government must provide the parliamentary committee with an annual report and supplementary reports when requested. The committee may also hold hearings with the heads of the two agencies.[123]

204. Some minor improvements have been made in the UK parliamentary oversight, but these have been criticized as inadequate[124].

IX. Judicial Review and Authorization

205. Judicial control over internal security services can take different forms. First, there is prior authorization in a pre-trial phase, and/or post hoc review, of special investigative measures, such as telephone tapping, bugging and video surveillance.[125] This is the normal practice in European States.[126]

206. Secondly, the judiciary naturally operate as a control in court cases concerning security issues, in particular, criminal trials for security-related offences, but also as regards constitutional, civil or administrative claims brought by someone alleging impropriety on the part of the security agency.[127] A fair trial in civil and criminal cases is a requirement of Article 6 of the ECHR (see below para 222). The extent to which the courts can operate as a control in civil and administrative cases depends upon various factors, inter alia the "accident of litigation", public immunity, national views on justiciability and standing requirements.

---

[122] See also the judgment of the Federal Constitutional Court in 2 BvE 5/06.

[123] Importantly this was not considered sufficient and a new, expert oversight body was also created with powers similar to that of the Norwegian oversight body. See Law 162, 2013 and the travaux préparatoires (Betaenkning om PET og FE, Nr. 1529, 2012).

[124] Leigh, I. Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11, 27 Intelligence and National Security 722-738 (2012).

[125] There is no unified definition of what constitutes a "special investigative technique". Used in a technical sense it means telephone tapping, bugging, video surveillance and other electronic measures for monitoring suspects. This is an area under constant technological development. Used in a more general sense it covers any technique for which national law (on the basis of constitutional provisions and practice) regards as sufficiently serious to require judicial permission. As such it can also cover such matters as the use of infiltration, secret identities, secret searches and Crown witnesses. See Council of Europe, Terrorism: Special investigative techniques, 2005 pp. 13-17. See also the definition given in Committee of Ministers Recommendation 2005(10) Chap I.

[126] Law and practice in this field is collected in Terrorism: Special investigative techniques, ibid.

[127] For recent examples, see the decision of the French Conseil Constitutionnel on requisition of telecommunications data, 275-332, 19 January 2006; the decision of the German Constitutional Court on preventive data screening, 24 May 2006, 1 BvR 518/02, http://www.bundesverfassungsgericht.de/entscheidungen/rs20060404_1bvr0 and the judgment of the Supreme Court of Canada on security detention, Charkaoui v. Canada, 2007 SCC 9.

207. Thirdly, in some States (e.g. France) investigating magistrates, who may be specialists in security issues, can be given a general supervisory control over ongoing security investigations. This supervisory control may be in addition to the (semi-) independent role the State grants to the prosecutor, who, as already mentioned, may, constitutionally speaking, belong to the judicial branch of the State.

208. It can also be noted that, in some States (e.g. United Kingdom), judges, because of their prestige and expertise in criminal procedure, may also be given the role of chairing ad hoc commissions of inquiry into alleged wrong-doing by internal security services. Alternatively, where such bodies exist, serving or retired judges may be given the role of members in, or chairing, standing expert authorization/review bodies (dealt with below, Section X). These last two examples should not, however, be seen as judicial review or authorization, but as judicial involvement in expert or parliamentary standing or ad hoc inquiries.

209. As regards judicial authorization of special investigative measures, State approaches to exactly what measures are regarded as sufficiently serious to require judicial approval tend to vary somewhat, depending on the scope and strength of the constitutional rights recognized in the State in question, in particular, the scope of the right of privacy. The case law of the ECtHR on Article 8 also naturally affects this issue.[128] In some States, such as the UK, judges are not involved in security crime investigations beyond authorizing or reviewing special measures. In other States, specialist judges can exercise a relatively tight control over crime investigations in general. How tight this control is in practice depends first, on the degree of control exercised over police operations by the prosecutor, and second, the degree of control exercised by the judge over the investigation, or certain parts of it. Crucial to the second issue is at what point in time the investigation is seen as becoming “judicial” in nature. However, even in such States, there may be special types of measure (e.g. security surveillance) which are classified as “administrative” or “intelligence” rather than criminal investigative in nature and which fall within another, non-judicial, authorization/review procedure.[129]

210. In its judgment in the case of *Klass v. FRG*, the ECtHR expressed a clear preference for a system of judicial control, stating that "The rule of law implies, inter alia that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure".[130] The ECtHR, however, went on to accept that strategic surveillance and intelligence surveillance (not designed to lead to criminal prosecution) may be subject to the authorization or review of an expert body instead, subject to certain conditions.

211. The ECtHR thus emphasizes judicial control as a mechanism for protecting individual rights. However, much security work may not be regarded as affecting a person’s constitutional rights, or his or her rights under the relevant rules of criminal procedure (e.g. gathering information on individuals from databanks or public sources). Depending on the constitutional system in question, the act of opening a thematic, or organisational, or even an individual file,

---

[128] See Venice Commission, Opinion On Video Surveillance in Public Places by Public Authorities and The Protection Of Human Rights, CDL-AD(2007)014, and the judgments of the ECtHR, in particular *Peck v. the United Kingdom* of 28 January 2003 and *Tsavachidis v. Greece*, op. cit.

[129] See, e.g. as regards France, Terrorism: Special Investigative Techniques, op. cit., p. 157 and as regards Germany, the ECtHR judgment in the case of *Weber and Saravia*, op. cit.

[130] ECtHR, *Klass v. FRG* judgment, para 55. The Court continued as follows: "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge" (para 56). The compatibility of the reformed German legislation was confirmed in *Weber and Saravia v. Germany*, op. cit.

may not be seen as raising an individual rights issue, even if the ECtHR has now clarified that this does involve a limitation under Article 8(1) which must be justified under Article 8(2).[131]

212. The phenomenon of "data mining" in particular should be mentioned here. The investigations made by many European police and security agencies are targeted on individuals in the sense that there must be indications, at least, that a serious criminal offence is being committed, or planned, by an individual to collect data on him.[132] Other States, however, allow police or security agencies to engage in the matching of data banks according to a number of variables without any suspicion of a concrete offence. The data obtained is then subjected to analysis, and the search variables further refined. The information finally obtained can be used to form the basis of subsequent intelligence or criminal investigations directed at individuals or groups. There may be no judicial involvement in this process at all, unless and until a criminal investigation is formally opened, or a criminal prosecution is formally brought. The use of data in this way as well as the development of sophisticated proactive surveillance technology (CCTV, biometrical data etc), programmed with such search variables, has given rise to considerable concern for human rights, particularly as regards racial profiling.[133]

213. Thus, a fair amount of security work is not directed towards pre-trial legal procedures and it is therefore likely to remain unchecked by judicial control over these processes.[134] This applies even in countries which have security police, and which formally speaking only investigate security crime, such as Switzerland, Sweden and Norway. It also applies, albeit to a lesser extent depending on the primacy of a judicial (criminal) investigation over an intelligence gathering investigation, in countries where investigating magistrates exercise relatively tight control over security operations in general.

214. Nonetheless, there is an obvious advantage of requiring prior judicial authorization for special investigative techniques, namely that the security agency has to go "outside of itself" and convince an independent person of the need for a particular measure. It subordinates security concerns to the law, and as such it serves to institutionalize respect for the law. If it works properly, judicial authorization will have a *preventive* effect, deterring unmeritorious

---

[131] ECtHR, *Amman v. Switzerland*, op. cit., paras 65, 69 and 70. See also *Rotaru v. Romania*, op. cit. and *Tsavachidis v. Greece* op. cit.

[132] Having said this, the extent to which this is a meaningful safeguard depends on a number of factors, inter alia the level of the suspicions necessary and how the offences in question are structured. Security offences have a tendency to "begin" early. When combined with the general part of the criminal law (attempt, conspiracy, aiding and abetting) relatively little may be required in the way of concrete suspicion that a specific criminal offence is ongoing.

[133] The European Commission against Racism and Intolerance (ECRI) is preparing a general policy recommendation (No. 11) advocating the definition and prohibition of racial profiling by law, and which would require a reasonable suspicion standard in the exercise of police investigation powers. The recommendation also proposes providing the police with training on the definition of racial profiling and on the use of reasonable suspicion standards. See also the reports on ethnic profiling released in December 2006 by the EU network of independent experts on fundamental rights http://cridho.cpdr.ucl.ac.be/AVIS%20CFR-CDF/Avis2006/CFR-CDF.Opinion4-2006.pdf, and the UN Human Rights Council, Report by Martin Scheinin, Special Rapporteur on the promotion and protection of human rights while countering terrorism, 29 January 2007, at: http://www.ohchr.org/english/bodies/hrcouncil/docs/4session/A.HRC.4.26.pdf. The usefulness of racial profiling has also been questionedsee, *inter alia*, Bakker, E., Jihadi terrorists in Europe, their characteristics and the circumstances in which they joined the jihad: an exploratory study, The Hague, Clingendael Institute, 30 January 2007**.** Another aspect of such "preventive" technological approaches which deserves further study is the extent to which they are promoted by corporations interested in selling their own products, capitalizing on governments' need to meet citizens' (real or exaggerated) fears of insecurity. See Bigo et al, op.cit.

[134] Cf. Arar Commission, A New Mechanism for the RCMP's National Security Activities, 2006, p. 439 "the choice of targets, the methods of information collection and exchange and the means of investigation generally will not be subject to judicial scrutiny, media coverage or public debate". See also Lustgarten, op.cit. who points out that the judicial paradigm of adjudication is far removed from the continuous oversight of the conduct of an organization; its priorities; policies etc. (p. 57).

applications and/or cutting down the duration of a special investigative measure.[135] The Parliamentary Assembly has earlier expressed a clear preference for prior judicial authorization of special investigative measures (depending on the type of measures).[136]

215. The mere involvement of judges in the authorization or review process, however, is not always an effective guarantee for respect for human rights. First, the value of judicial control obviously depends upon the *independence*, in both law and fact, the judges possess from the executive in the State.[137] This in turn depends upon the constitutional law and practices of the State in question, and its legal and political culture.

216. Secondly, the value of judicial control depends upon the *expertise* the judges in question have in assessing risks to national security and in balancing these risks against infringements in human rights. A judge who is experienced in criminal law develops an ability to go to the heart of an issue, and pose the correct, awkward, questions. Moreover he or she also has experience of weighing the probative value of evidence, and an awareness of the fundamental importance of not balancing away the suspect's rights against the public interest, especially when the individual in question is not in a position to defend himself or herself.

217. It must be said however that terrorist offences, while resembling organized crime in some ways, are different in others. As regards identifying terrorist support networks, special political (and religious) knowledge, as well as common sense, are necessary to distinguish people on the outer limits of radical but essentially non-violent dissent from those who actively embrace terrorism.[138] Moreover, security surveillance usually comes in at a very early stage in an investigation and is of an exploratory nature, tending to be for identifying networks rather than gathering specific evidence of specific crimes against specific suspects. In other words, there may not be much in the way of concrete suspicions to go on at the time when surveillance is requested but other means of obtaining information may be regarded as impracticable.

218. Even for a specialised judge, the invocation of "national security" is very potent, conveying as it does a need for urgent and decisive action. National security can obviously be abused as an argument, but there is also an inbuilt tendency to overuse it. The security agency, if it wishes to do its job properly, will naturally tend to err on the side of caution and give priority to the need for information obtained by surveillance over the personal integrity of the group of persons – possibly quite large – subjected to the surveillance.[139] It is likely to be a strong-minded judge with considerable prior experience of dealing with previous applications who is able to question the proportionality of the experts' assessments and stand firm against the temptation to balance away integrity almost every time. Psychologically speaking, a tendency to grant authorizations is likely to be strengthened where the State, for example for reasons of separation of powers, has no procedure for checking up on, let alone criticizing, the number and duration of judicial authorizations granted.

---

[135] This was the conclusion drawn by a study comparing the number of warrants issued under the old (pre-1984) Canadian system of ministerial authorisation with the new system of both ministerial and judicial authorisation. See Brodeur, J. P., "Parliamentary vs. Civilian Oversight", in Töllborg, D. (ed), *National Security and the Rule of Law*, (Gothenburg University, 1997) at p. 88. The author concludes "Whatever the shortcomings of judicial control these data suggest that we are better off with it than we are without it".

[136] Recommendation 1402 (1999)1, Control of internal security services in Council of Europe member States.

[137] See Venice Commission, Judicial Appointments, CDL-JD(2007)001rev; CCEJ Opinion No. 1(2001) on standards concerning the independence of the judiciary and the irremovability of judges; Committee of Ministers Recommendation No. R (94) 1 on the independence, efficiency and role of judges.

[138] See, e.g., the McDonald Commission Report, p. 868. This in turn argues for specialized and specially trained judges. See also Marin, J.C., Lutte contre le terrorisme et état de droit, vingt ans d´expérience française, unpublished conference paper, Ottawa 9 February 2006 and above paras 136-137.

[139] See, e.g. Feldman, D, Human Rights, Terrorism and Risk: The Roles of Politicians and Judges, 2006 Public Law 364.

219. One important restraint in many States on the use made by the ordinary police of special investigative techniques is that these will eventually be notified to the suspect and/or may risk being criticised in a subsequent criminal trial. But in most States, the majority of security cases do not end up in court. And any notification requirements which might exist at national law will likely not apply either because there is an explicit exception for security crimes or because the investigation will be regarded as ongoing.[140] In such situations, an authorizing judge may be tempted to conclude that no one is likely to find out about the surveillance, so no "harm" is done. The experience of a number of countries, such as Norway and Sweden, was that judges, in the past, were too willing to accept security agencies' threat assessments.[141] This has prompted the introduction in these States of expert follow-up mechanisms in addition to judicial authorization procedures, assessing the number of such permissions granted and the time the infringement of integrity went on against the useful intelligence which resulted from the measure (see below paras 247-249).

220. There exist several devices restricting a court's ability to consider all the evidence, or to go to the heart of the issue: the legitimacy of the measure in question. Declaring certain essential documents to be secret, or limiting in different ways the scope of the review can preserve the shell of judicial control while emptying it of substance.[142]

221. Bearing in mind the importance of expertise in this area, very strong arguments exist for a degree of specialisation and specialist training for judges dealing with authorisation procedures, and/or supervision of investigations generally as well as for courts dealing with civil, criminal and administrative security cases. This is indeed the approach taken in a number of States such as France with the concentration of security crime investigations and prosecutions to specialist judges and investigating magistrates at the Tribunal de Grand Instance in Paris, or Spain, with a similar concentration of security crime cases to the Audencia Nacional. Similarly, in Canada it is specially designated Federal Court judges who hear surveillance applications from the Canadian Security Intelligence Service and deal with immigration and freedom of information cases with a security dimension. In the US, judicial warrants are necessary for criminal investigations, and, as regards "agents of a foreign power", the Foreign Intelligence Surveillance Act has given specialist judges the role of approving intelligence-related surveillance for nearly two decades.[143] In the UK, designated judicial Commissioners deal with authorisation/review of surveillance under the Regulation of Investigatory Powers Act 2000.

222. At the same time, there are also risks involved in specialisation. Some may view with suspicion the taking away of security matters from the ordinary courts, to courts with specially chosen and appointed judges and investigative magistrates/prosecutors.[144] Having said this, the European Court and Commission of Human Rights have accepted specialist tribunals, even in security matters as long as adequate guarantees of judicial independence from the executive exist and proceedings are otherwise fair.[145]

---

[140] The EctHR accepted that this was a legitimate reason for non-notification in *Klass v. Germany*, op.cit. para 58.

[141] Norway: Lund Report, pp. 352-355, Sweden: Säkerhetstjänstkommission, SOU 2002:87, pp. 365-383.

[142] Lustgarten, L. and Leigh I., op cit, chapter 12.

[143] For a survey of the work of the FISC see Manget, F., Intelligence and the Rise of Judicial Intervention, in Johnson L.K., (ed.), *Handbook of Intelligence Studies*, (Routledge, 2006), 333.

[144] See principle 22 of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, adopted by an NGO coalition in 1998 (in 20 HRQ, 1998).

[145] The standard test laid down by the Court (ECtHR, *Campbell and Fell v. UK* judgment of 28 June 1984, para 78) is that the requirement of independence entails safeguards relating to "the manner of appointment of judges, the duration of their office, the existence of guarantees against outside pressures and the question whether the body presents an appearance of independence." In Eccles, *McPhillips and McShane v. Ireland* No. 12839/87, 59 DR 212 (1988), the Commission considered that the judges on a special criminal court dealing with terrorist cases were sufficiently independent in practice. In *Ciraklar v. Turkey*, 28 October 1998 and a number of

223. Another risk is "case hardening". The group of security cleared judges and prosecutors can be so small that it is almost "incestuous", and they may come to identify more with the people with whom they are in daily contact – the security officials – rather than their judicial colleagues. There is a danger that these judges become so used to the types of techniques, information and assessments they see every day that they lose their qualities of independence and external insight through a process of acclimatisation. The necessary awareness of the suspect's rights may gradually be lost over the years spent in the isolated world of security intelligence. This implies that some form of appeal or follow-up mechanism should exist for even judicial authorization of special investigation techniques. It also suggests that, unless special reasons exist, the number of years spent as a judge authorising or reviewing security surveillance should not be too long.[146]

224. The need to balance "open justice" with the State's security interests has led to a number of innovations in some States. One idea is the use of special, security-cleared advocates, in deportation and employment, and (increasingly) in criminal cases.[147] This gives protection for State secrets without totally excluding any opportunity of challenge to the evidence on the applicant's behalf. It allows a vetted lawyer to test the strength of the government's case even where the complainant and his lawyer are excluded from parts of the legal process on security grounds. Such procedures have been noted by the ECtHR as a means of satisfying Article 6 (the right to a fair and public trial, in particular the principle of equality of arms), in security cases.[148]

225. There is, however, an obvious problem with having such a mechanism in proceedings such as surveillance where the target is unaware of the proposed measure, and where, in addition, the need for urgent action is alleged. While the special advocate can question the evidence on which a decision to grant surveillance is based, he or she can obviously not contact his or her "client", in order to seek further information. As much security surveillance is based on more or less well supported speculation as to the reality or dangerousness of a particular threat, it is important to be able to counter this with a convincing argument of innocence. The compartmentalisation of security intelligence makes this even more difficult. The risk is that the advocate becomes a hostage of the proceedings, and serves simply as a legitimisation of a - foregone - conclusion.

226. The mechanism of security screened advocates has, for these reasons, received more critical responses in recent years.[149] The ECtHR has also, more recently, drawn a distinction between the degree of legitimate secrecy in special investigative measures the use of which obviously have to be kept secret from the suspect and other administrative measures, such as deportation which can be subject to a greater degree of disclosure.[150] The main value security cleared advocates can have would seem to be in adversarial civil and administrative court proceedings concerning security issues where the measure taken is known to the parties, but for one or other reason, the full file cannot be disclosed to one of the parties. In criminal proceedings, the scope for limiting access to the file is generally more limited. The ECtHR has

---

subsequent cases the Court did not consider that the State Security Courts as then constituted in Turkey satisfied the requirements of Article 6. See also the International Bar Association Task Force on International Terrorism, International Terrorism: Legal Challenges and Responses, 2003, pp. 73-75.

[146] For example, in the US, judges on the FIS court have a maximum period of 7 years in office (50 USC Section 1803(d)).

[147] See UK Treasury Solicitor, *Special Advocates: a Guide to the Role of Special Advocates* (London, 2005).

[148] ECtHR, *Chahal v. UK*, op. cit.; *Al-Nashif and others v. Bulgaria*, op. cit.; *Tinnelly and McElduff v. UK*, op. cit.

[149] UK Constitutional Affairs Select Committee, *Seventh Report for 2004-5, The operation of the Special Immigration Appeals Commission (SIAC) and the use of Special Advocates*, HC 323-I.

[150] *Al-Nashif and others v. Bulgaria* op. cit.

allowed the concealment of security information (e.g. the identify of an informer) only when there are concrete dangers to the life of the person involved, where there is other information on which a conviction is based and where there are strong evidential safeguards to compensate for imbalances which might arise in the equality of arms.[151] In a criminal case, providing a security-cleared advocate is, by itself, most unlikely to satisfy the requirements of Article 6. In criminal case involving limited disclosure the Court has stressed the special responsibility of the trial judge in sifting these claims.[152]

227. These innovations apart, for the reasons discussed control by the ordinary courts does not appear as the best instrument of accountability for or redress against security and intelligence agencies. This leads naturally to a discussion of other processes for accountability (see below Section X) and for handling complaints (see below Section XI).

X. Accountability to Expert bodies

228. Expert bodies can serve as either a supplement or a replacement for parliamentary bodies or judicial accountability. The general issues for expert bodies have thus already been raised under the previous headings. They can also be given complaints functions and this is dealt with in the next section. However, a number of extra points need to be made, relating to mandate/powers and membership of these bodies, the relationship between an expert body and parliament and the connection with judicial accountability.

229. An expert body allows for greater expertise and time in the oversight of security and intelligence services and avoids the risks of political division and grand-standing to which parliamentary committees can be prone. The body may be full or part-time, but even if it is part-time, the supervision exerted is likely to be more continuous than that exercised by a parliamentary body, the members of which have many other political interests and responsibilities. The members' tenure can be made longer than the standard electoral period, something which is particularly important as intelligence has, as already mentioned (see above para 90), a relatively long "learning curve".

230. Like parliamentary oversight, the mandate of an expert body can be institutional, meaning that it can be established to exercise supervision only over a specific internal security body (this is in contrast to functional review discussed below). An example of this is the Canadian Security Intelligence Review Committee (SIRC) which supervises the Canadian Security Intelligence Service (CSIS). SIRC has been an important source of inspiration for various European States in creating their own expert bodies.

231. However, as mentioned before, the problem nowadays with giving an expert body an agency-specific mandate is that different security agencies cooperate with each other in a "security spectrum". In particular, the police and a security agency can act jointly, as an integrated response, or act through one another. In Canada, this gap has been apparent for a while and proposals have recently been made to supplement SIRC's monitoring with a review body able to look at all national security activities under the control and direction of the police.[153] A better approach, found in e.g. the Dutch legislation, is to give functional powers of review.[154]

---

[151] See e.g. *Monika Haas v. Germany*, op. cit.

[152] See in particular *Rowe and Davis v. UK*, No. 28901/95, 16 February 2000 and Cameron, 2000, op. cit. pp. 308-318.

[153] Commission of Inquiry into the Actions of Canadian Officials into Mahar Assar, op. cit, pp. 477-479.

[154] The oversight body, the SCISS, supervises the General Intelligence and Security (AIVD) Service, the Defence Intelligence and Security Service (MIVD), other bodies, such as the police *to the extent that these carry out AIVD and MIVD activities* as well as the coordinator for the intelligence and security services which falls under the authority of the Prime Minister's office (see Intelligence and Security Services Act of 7 February 2002, Articles 1 and 4.

232. It is, however, important that the scope of the review is drawn carefully, to avoid disputes as to whether a particular activity falls within the body's mandate and to avoid overlaps with other accountability mechanisms, in particular judicial controls over police powers and Ministerial accountability to parliament.[155]

233. The scope of the mandate, i.e. the type of the supervision exercised, can also vary. Comparatively, at least six different types of general supervision, partially overlapping, can be identified, ensuring legality, efficacy (that the agency is actually securing its objectives), efficiency, budgeting and accounting, conformity with relevant human rights conventions and finally policy/administrative aspects of the intelligence services.[156]

234. In addition, the mandate of an expert body may also be framed more narrowly to cover only certain activities of the security agency, or agencies, such as their use of a particular form of surveillance e.g. the French *Commission Nationale du Contrôle des Interceptions de Sécurité* (CNCIS) or the content of security databanks, e.g. the Swedish Register Board, (*Registernämnd*) or the Austrian *Rechtsschutzbeauftragter*.

235. Particularly important, as regards general supervisory bodies, is the distinction which also applies to parliamentary oversight between review of overarching policies and review of operational activities. There will probably be not the same problem of vetting the members of an expert body, as compared to a parliamentary body. Thus, generally speaking, it will be easier to give an expert body access to very sensitive operational material.

236. The membership of the expert body will depend partially upon its mandate. Where the focus of the body is ensuring that the security agency abides by the law, it is reasonable to assume that several of the members will be lawyers, or legally trained. Lawyers are trained to have good judgment, weighing different interests against one another. However, they may, depending on the legal culture of the State, be less inclined to question the legitimacy of discretionary judgments, so long as these fall within the acceptable span of decision-making. Where the body has a broader mandate, this will favour appointing experts from different walks of life, historians, criminologists, political scientists etc.

237. If the problem for parliamentary accountability bodies can be summarized in the word "competence", the problem for expert bodies can be summarized in the word "legitimacy". This affects both how the body is established, how members of the body are chosen and to whom or what the expert body reports. As regards establishment of the body, it is greatly desirable for the legitimacy of the expert body, and its good relations with parliament, that it is created by statute. This applies even in States where the constitution, or constitutional traditions, give an elected President primacy in foreign policy and defence matters. Only where the parliament has voluntarily accepted that accountability is better exercised by an independent expert body, rather than a parliamentary body, will the former be in a position to give plausible reassurance to both the parliament and the public that misuse of powers is not occurring. Moreover, in order

[155] For example, the mandate of the Belgian "Committee R" was originally drafted widely, and was narrowed somewhat by statute in 1999. See van Outrive, L., Intelligence Services in Belgium: A story of legitimation and legalisation, at p. 50 in Brodeur, J.P., Gill, P. and Töllborg, D., (eds*), Democracy, Law and Security: Internal Security Services in Contemporary Europe*, (Ashgate, 2002).

[156] Born and Leigh, op. cit. chapter 15. For an example see, Section 2 of the Norwegian Act relating to the Monitoring of Intelligence, Surveillance and Security Services. Act No. 7 of 3 February 1995 which provides that the purpose of the monitoring is: "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, to ensure that the activities do not involve undue damage to civic life, to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law (…)".

to maintain parliament's confidence in the expert body it is necessary to provide for institutional links between the two.

238. As regards membership, an expert body will not consist of politicians having earned a reputation for competence and integrity during a number of years in the public gaze, and having been elected, usually repeatedly, by the people they represent. They will instead usually be figures who are less well known to the public. As the expert body will rarely be in a position to reveal to the public the basis for its conclusions, the public have to trust it. One way of improving the basis for this trust is to reveal, as much as security considerations make possible, the reasons for its conclusions. Another way is to involve the parliament in both choosing the members of the body and by making, or letting, the body report to the parliament. Different ways of involving the parliament in choosing the members exist. For example, the government can appoint the members but after a process of consultation with all the parties represented in parliament, or at least the leaders of these parties. Parliament itself can choose and appoint the members. The government can appoint the members from a list chosen by the parliament. Whatever the methods chosen, it is vital for the legitimacy of the expert body that its members are either generally regarded as apolitical or, where instead members have political affiliations, that there is an appropriate political balance in the body.[157]

239. As regards its powers, an expert body which performs general supervisory functions should be able, like a parliamentary oversight body, to decide its own agenda. Likewise, it should be able to make special reports, as well as producing an annual report. One reason for having an expert rather than a parliamentary body is that the government can task the former to investigate and report a specific matter, whereas it will not be in a position to order a parliamentary body to do so. However, as mentioned, an important part of an expert body's legitimacy is its ability to show it is doing its work, by publishing its report. Where the government decides whether or not the report – or even an edited version of it - shall be published, the body will be perceived as the government's body. Even the government's control over the timing of the report can diminish its legitimacy, as the government can obviously decide to publish the report at a time when it has least political impact. Mechanisms for determining disagreements over the content of the report have already been discussed above (see above, para 177).

240. One solution for the difficulty of reconciling government tasking with the independence, and so legitimacy, of an expert body is to allow *both* government tasking and investigations *proprio motu*. In the case of the former, the government would have a degree of control over the agenda, and full control over the publication of the final report. In the case of the latter, the expert body has the final say. In States where such a dual model has been chosen, such as Belgium, tasking has in practice not occurred, precisely because of the *proprio motu* power of investigation.[158]

241. As already mentioned in the context of parliamentary oversight, it is important that the body is supported by a small number of experienced staff.[159] This is particularly important where the expert body is part-time. Staff provide an element of continuity, and also help build up a relationship of trust with the agency being supervised. As noted, it is also possible to give an Inspector-General the function of assisting an expert body in investigating a particular

[157] See van Outrive, op.cit. for critical remarks concerning the politicisation of the Belgian Committee R.

[158] Tasking can occur under Article 32 of the Act of 18 July 1991 on the supervision of the police and intelligence services. As regards the absence of such tasking in practice see Permanent Committee for Supervision of the Intelligence Services (Committee R) Annual Activity Report 2004, www.comiterib.be at p. 5.

[159] Above paras 136-137. For comments on the Canadian and Norwegian experience in this respect see S. Farson, Parliament and Their Servants: Their role in scrutinizing Canadian Intelligence, 15 Intelligence and National Security 225-256 (2000) and Sejerstedt, op. cit.

security issue. The extent to which this is seen as possible and appropriate will depend upon the constitutional structure of the State, in particular to what extent it adheres to the principle of the separation of powers, and where the main problem of security oversight is envisaged as lying: is it oversight of the government's use of the security agency (political policing), or is it the impenetrability of the agency itself (the State within the State)? Where the Inspector-General is envisaged as being very definitely in the executive branch, for different reasons in different States it may not be regarded as appropriate to make an expert or parliamentary body dependent on the executive branch in such a crucial area as access to information on possible wrongdoing.

242. As regards the relationship an expert body with general supervisory powers has with the parliament, it is important to stress that there must be mutual respect and a rational division of labour between the two types of body. Where there is this, then there can be important advantages in having both a parliamentary oversight body and an expert body. The expert body is operating fully within the "ring of secrecy", and as such, it can get out of touch with political and social developments, and political priorities. Moreover, it will not usually be in a position to defend itself vis-à-vis the press and public or the parliament as a whole. A parliamentary body with a good relationship with an expert body, with better, but not full access to intelligence material, and with better expertise in intelligence matters than parliament as a whole is in a position for two-way communications, reassuring the parliament as a whole and the public that the expert body is in touch with political developments and is doing its job properly.

243. By contrast, where there is no rational division of labour problems can arise. Two different situations may be discerned. The first is where the expert body has been given an explicit reporting duty to a parliamentary committee established specifically to monitor security and intelligence matters, or to existing parliamentary committees with broad competence to look at justice and defence matters. In such a situation it is important to avoid overlapping jurisdiction, leading, in the worst case to conflicts between the two bodies concerning, e.g. which body is entitled to investigate an issue and why. The second type of situation is where there is no such formal relationship to a parliamentary committee and the reporting duty is only to the government. This can have a number of negative implications, at least where there is a parliamentary committee which considers that it has some form of supervisory competence in the field of security (which will almost invariably be the case, as both defence and justice matters are a traditional preserve of parliamentary scrutiny). Not involving parliament in some way can easily lead to resentment and tensions, e.g. parliament may want greater access to intelligence material, and might try to compel the expert body to reveal this.[160]

244. Apart from providing for an explicit reporting duty to a parliamentary committee, and for allowing the expert body to provide a parliamentary committee with some otherwise secret material, if the expert body considers this useful, another mechanism for creating a proper relationship between an expert body and parliament is to provide that parliament can request the expert body to report on a given matter. This is possible in, e.g., the Netherlands, although the power has been used so far only once.[161]

245. As already mentioned, an expert body can be a hybrid body, which consists partly of active politicians, including serving members of parliament, and partly of expert members. An example of this is the Swedish Register Board (tasked with overseeing the databanks of the Swedish security police) which consists of two MPs, chosen from the two largest parties, and three lawyers (one in private practice nominated by the Bar Council, one judge, and a further

[160] See Farson, S., Canada's long road from Model Law to Effective Oversight of Security and Intelligence, in Born, H., Johnson, L. and Leigh, I., op. cit., pp. 99-118 on the experience of SIRC.

[161] Intelligence and Security Services Act 2002 Article 78(2). The Dutch parliament has also asked the Minister twice to report from the SCISS. See Annual Report 2005-2006 of the SCISS**,** p. 5. It is also possible in Norway, though again the power has not been used, Sjerstedt; op.cit., p. 126.

lawyer qualified for senior judicial office serving as chair).[162] In the best case analysis, such a hybrid body can combine legitimacy with expertise and has much to recommend it. Certainly this model is generally regarded as successful in Sweden, both by independent observers and the security police. Another example of a hybrid model is the German G-10 Commission, whose expert members tend to be connected to political parties, even though they have (so far) not been serving MPs. The extent to which these types of hybrid models are appropriate for other States depends upon how far the State in question adheres to a strict separation of powers and where the preponderant problems in security oversight are seen as lying.

246. The Swedish Register Board is an example of an expert body with limited, rather than general supervisory power. Other forms of body with supervision over databanks are data ombudsmen and data protection inspectorates. An example of this is the Austrian institution of the Rechtschutzbeauftragter (see above para 147).

247. Where such data protection ombudsmen and inspectorates continuously supervise the accuracy, reliability, legitimacy and proportionality of the intelligence stored, these operate as controls. Where they decide, ad hoc, on complaints from members of the public who allege that flawed data is stored on them they are a complaints procedure (discussed below). Bearing in mind the crucial importance of data banks to the work of a security agency, and the already mentioned distinction between security intelligence and "hard" data (see above para 89), it is imperative that some such supervisory body exists in every State, and that it has sufficient powers, in law and practice, to perform control functions satisfactorily. An ombudsman may well be independent of the executive, but an ombudsman without specific expertise in security matters, and without a mandate to monitor continuously security databanks specifically will not be an adequate control mechanism in this particular area, however useful the office is for maintaining professionalism in the public administration generally. The same applies to data protection inspectorates. Having said this, some States locate their controls over security data specifically within the general data inspectorate, giving a specific security-screened person, or team of people, the sole function of monitoring continuously this data. Such a system can be an acceptable form of control, providing the person or group given this task is in law and in fact independent from the executive.

248. Another type of specific mandate which can be granted to an expert body relates to surveillance. Here the body operates as a substitute, or a complement, to judicial authorisation procedures. As already mentioned, the exploratory and speculative nature of much security surveillance, and the connection security crime has to politics, is an argument which has been used in some States for having a different system of authorisation or review.

249. As regards security surveillance which is not "strategic" in nature (see above paras 93, 210),[163] there are very good arguments for having both judicial authorisation and a follow-up supervisory control exerted by an expert body. The follow-up control examines past authorisations, matching the initial suspicions with the product obtained. As such it acts as a forward-looking mechanism, recommending improvements in how targeting decisions and intelligence gathering priorities are made in the future, so as to minimize interference with human rights.

---

[162] Note: as regards developments since 2007, the functions of the Swedish Register Board have been taken over by a new body, the Commission on Security and Integrity Protection, which also exercises post hoc supervision over electronic surveillance. It retains its hybrid membership, which has been increased to include a representative from all political parties in the parliament. See http://www.sakint.se/InEnglish.htm.

[163] See, in this respect, CDL-AD(2015)011.

250. While non-judicial systems of control over security surveillance, particularly strategic surveillance, may, depending on constitutional structures, be sufficient, it should be noted that where an expert body instead operates only as a substitute for judicial authorisation and not simply as a complement to it, it is especially important that the body in question is sufficiently capable and independent to exercise a real control. This will depend on three factors. The first of these is the expertise of the expert body in security matters, and the time it actually spends looking at the cases. A part-time body will probably not be able to look in detail at all applications, but will only be able to make spot checks. The second factor is the scope and extent of the review performed – is it of the merits of the request for the use of special investigative measures matched against the final result of these measures, or only whether there seemed to be grounds at the time for authorising the surveillance. The third factor is whether the expert body in making spot checks really critically examines all the supporting evidence for surveillance. This must involve access to the "raw intelligence" (informers' statements, the identity of the informers in question etc.) to assess its reliability and not only the "refined" and "anonymised" material in the actual surveillance application.

XI. Complaints mechanisms

251. Clearly it is necessary for individuals who claim to have been adversely affected by the exceptional powers of security and intelligence agencies, such as surveillance or security clearance, to have some avenue for redress. Quite apart from strengthening accountability, complaints may also help to lead to improved performance by the agencies through highlighting administrative failings. The requirements of human rights treaties, and especially the European Convention on Human Rights, with its protections of fair trial, respect for private life and the requirement of an effective remedy must obviously also be borne in mind.[164]

252. Plainly, though, legitimate targets of a security or intelligence agency should not be able to use a complaints system to find out about the agency's work. A complaints system should balance, on the one hand, independence, robustness and fairness, and, on the other hand, sensitivity to security needs. Designing such a system is difficult but not impossible.

253. Individuals who allege wrongdoing by the State in other fields routinely have a right of action for damages before the courts. The effectiveness of this right depends, however, on the knowledge of the individual of the alleged wrongful act, and proof to the satisfaction of the courts. As already mentioned, for a variety of reasons, the capacity of the ordinary courts to serve as an adequate remedy in security fields is limited. The case law of the European Court of Human Rights (see above, Section VI) makes it very clear that a remedy must not simply be on paper.

254. An alternative is to allow an investigation and report into a complaint against an agency by an independent official, such as an ombudsman. This is the case in e.g. the Netherlands.[165] In other countries (for example, New Zealand and South Africa) complaints against the services are handled by an independent Inspector-General of security and intelligence as part of the office's overall oversight brief.[166] Additionally, specific offices established under freedom of information or data protection legislation may have a role in investigating complaints against the agencies. For example, in Austria the individual usually has the possibility of complaint to the Datenschutzkommission, but if for secrecy reasons the individual has not been informed of the data (mis)use, the complaint may be raised by the Rechtsschutzbeauftragter on his/her own motion.

---

[164] See above para 162 and below para 257. See further Cameron, 2000, op. cit.

[165] Intelligence and Security Services Act 2002, Article 83.

[166] See respectively, New Zealand (Office of Inspector-General of Intelligence and Security, established in 1996) and South Africa (Office of Inspector General of Intelligence, appointed pursuant to Section 12 of the Constitution).

255. In these ombudsman-type systems, the emphasis is on an independent official investigating on behalf of the complainant. These independent offices usually exist to deal with an administrative failure by public bodies, rather than a legal error. Their investigations may give less emphasis to the complainant's own participation in the process and to transparency than would be the case with legal proceedings. Typically an investigation of this type will conclude not with a judgment and formal remedies, but with a report, and (if the complaint is upheld) a recommendation for putting matters right and future action.

256. A less common variation is for a State to use a parliamentary or expert oversight body to deal with complaints and grievances of individuals, as happens in Germany, Norway and Romania. There may be a benefit 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, 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.

257. 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. This approach is also supported by the ECHR. The requirement in ECHR Article 13 of a mechanism for remedies for alleging violations of Convention rights which is independent from the authorization process means that a State's control system, e.g. for data-processing, may pass the test of "accordance with the law" and "necessity in a democratic society" but that the absence of a remedy means that there is nonetheless a violation of the Convention. As already mentioned, the ECtHR has stated that a remedy must be effective in law and fact. It should be noted in particular that the ECtHR has ruled that a data inspection authority which is independent, and which has formal competence in law to award a remedy for the holding of inaccurate, inappropriate etc. security data, but which in fact lacks the expertise to evaluate this data, is not an effective remedy within the meaning of Article 13.[167]

258. The experience of the ECtHR in the case of Leander v. Sweden should also be noted. The Swedish government had argued at the time that a number of control and remedies bodies existed to prevent errors being made in security screening and to remedy any errors that were made. However, later official inquiries showed that none of the controls and remedies worked properly in this area. The people involved in each of the control/remedies systems assumed that each of the *other* systems was working properly. None of the controls/remedies went to the heart of the issue: the reliability and proportionality of the security assessment made of an individual. The existence of several "half" control/remedies provided only a semblance of control, not its reality.[168]

259. In some countries, not only individuals 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 issues with the Parliamentary Control Panel[169] and in South Africa members of the service may complain to the Inspector General.

---

[167] Compare the negative judgment of the Court in *Segerstedt-Wiberg v. Sweden,* op. cit, with *Brinks v. Netherlands*, op. cit.

[168] See Cameron, 2000, op. cit. pp. 225-244, 246-252. As already noted, reforms were later made and the present system is working satisfactorily.

[169] Bundestag, 2001, op. cit. pp. 19-20. See also para. 202 above.

260. Another method of handling complaints is through a specialist tribunal. This 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 (the Intelligence Services Commissioner and the Commissioner for the Interception of Communications). Or complaints may be handled in a tribunal-type procedure but by a specialist oversight body, as with the SIRC in Canada. Where the oversight body is involved in the approval process of security operations it cannot also serve as an independent complaints mechanism (see above paras 162 and 257). Otherwise, a tribunal of this kind 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, 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 advocates have been introduced in some countries. The critical points made before regarding the limitations applying to special advocates (see above paras 224-226) and regarding the value of expert supervision procedures for surveillance (see above para 257) also apply here.

XII. Concluding remarks

261. Intelligence is an inescapable necessity for modern governments and security services are essential in order for any State to be able to protect its values and interests.

262. There are some recurring issues in the design of oversight procedures.[170] Firstly, it is necessary to establish mechanisms to prevent political abuse while providing for effective governance of the agencies. Overall, the objective is that security and intelligence agencies should be insulated from political abuse without being isolated from executive governance.

263. Secondly the rule of law must be respected. Agencies must be subject to legal control. As in other areas of public administration, one key task of the parliament is, by means of statute, to delegate authority to the executive but also to structure and confine discretionary powers in law.

264. The challenge for oversight and accountability is to adapt or devise processes that command democratic respect at the same time as protecting national security. This is a theme that runs through all of approaches to accountability discussed, whether by the executive, to parliament, in the courts, or complaints processes or by independent expert bodies.

265. It is possible to draw distinctions between issues of policy, operations, and review. Examples of policy matters are: what constitutes a security threat; which actions should be criminal; which powers should be available; which agencies should be established and on what terms? The case for public disclosure as an aid to accountability is very strong here and that for secrecy is weak. Examples of operational issues are: should this group/ country be targeted and with what priority; should this form of surveillance be conducted on X? Operational detail affecting the methods, sources and specific activities of the agencies has a much more convincing case for secrecy. Operational matters are primarily for the executive and controls would thus be at the administrative level. Review takes place ex post facto and considers questions such as: was the operational action in accordance with policy, proportionate, legal, economical, and effective? Review, however, is more problematic as parliament, the executive and the judiciary all have legitimate interests in aspects of it.

[170] See also generally as regards the comments made in this section, Leigh, I. The Accountability of Security and Intelligence Agencies, in Johnson L. (ed.) *The Handbook of Intelligence Studies*, (Routledge, 2006), pp. 67-81.

266. These distinctions should not be taken too rigidly. The development of policy must be informed by intelligence and operations which in some cases it may be necessary to keep secret. Another borderline issue concerns the development of surveillance methods or technologies: these may raise controversial policy issues which are difficult to discuss publicly without rendering them ineffective by effectively giving notice to potential targets. There are difficulties too in fully differentiating operations and review. The continuing nature of some intelligence operations makes it difficult to draw a line between authorisation and review; or to engage in review without compromising secrecy.

267. Nevertheless the distinctions between policy, operations and review can assist our understanding of accountability. They make clear that in policy issues there is a strong democratic interest in favour of public discussion and accountability. Secrecy in this field requires compelling arguments to tip the scales.

268. Although the case for operational secrecy is much stronger, that does not mean that there is no room for accountability. The executive should set the parameters for security and intelligence operations, even if, quite properly, the services are insulated from political pressure. At the level of review, it is absolutely necessary to have external mechanisms to bridge the barrier of secrecy and provide assurance for the executive, legislators and the public that operations are being carried out effectively, lawfully and in accordance with policy. This type of assurance must be plausible, which is why some countries allow parliamentary committees or independent expert bodies linked in some way to parliament to review operational detail.

269. Executive control alone is insufficient; other mechanisms of accountability are necessary. No one level of accountability stands alone. They are interlinked, complementary and inter-dependent. A coherent overall system must be found, bearing in mind that several half remedies or half controls can be worse than none, as there is the risk that each control/remedies system could refrain from acting on the assumption that the other is doing the work.

270. Accountability mechanisms must not remain on paper, and must be kept under constant review. Inter-agency co-operation should be the object of particular care; international cooperation arrangements for “paper trails” could be envisaged, and transfers of power should be subjected to clear governmental/ministerial responsibility. Exchanges of best practices between national oversight bodies should be facilitated.

271. This report clearly shows that there exists a variety of innovative models for democratic oversight of security services, which, alone or in combination with each other, allow any State to cater for their specific legal and political contexts as well as security needs.

272. These models show that the secret world and accountability are not mutually incompatible. On the contrary, accountability is necessary both for effectiveness and for legitimacy.