Section III

The Role of the Executive

Chapter 9

The Case for Executive Control

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

The ultimate authority and legitimacy of intelligence agencies rests upon legislative approval of their powers, operations and expenditure. However, for practical reasons and because of the sensitive nature of the subject matter, effective external control of these agencies must rest with the government – the executive. There is no inherent conflict between effective executive control and parliamentary oversight (See Section IV). Quite the contrary: effective parliamentary oversight *depends* on effective control of the agencies by ministers. Parliaments can only reliably call ministers to account for the actions of the intelligence agencies if ministers have real powers of control and adequate information about the actions taken in their name. Where this is lacking, the only democratic alternative is for a parliamentary body or official to attempt to fill the vacuum. This, however, is a poor substitute because legislative bodies can effectively review the use of powers and expenditure *ex post facto*, but they are not inherently well-equipped to direct and manage these matters, whereas governmental structures are.

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

Effective control by the executive does not, however, suggest direct managerial responsibility for security and intelligence operations. Both to prevent abuse and as a prerequisite of effective control, the respective competences of the responsible ministers and the agency heads should be set out in legal provisions. In the interests of effectiveness they should be distinct but complementary. If ministers are too closely involved in day-to-day matters, it will be impossible for them to act as a source of external control and the whole oversight scheme will be weakened. The precise line between the respective functions of ministers and the agency heads is difficult to

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

Box No. 20:

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

Article 7:

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

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

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

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

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

Chapter 10

Ministerial Knowledge and the Control of Intelligence

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

Legislation should contain clear arrangements for political direction and, in the case of internal agencies, political independence, to ensure that matters of policy are determined by politicians accountable to the public. It is preferable that various mechanisms be explicit in legislation and be backed by appropriate legal duties. This is not because it is desirable that daily relations between the agencies and ministers should be handled legalistically. Rather, a legal framework in which the respective powers and responsibilities are clear may of itself help to deter abuses and encourage a responsive and frank working relationship.

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

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

Box No. 21: Rights of the Minister	Responsibilities of the Agency
✓ the ministerial responsibility for formulating policy on security and intelligence matters; ✓ the ministerial right to receive reports from the agencies; ✓ a reservation of the right to approve matters of political sensitivity (such as cooperation with agencies from other countries) or undertakings that affect fundamental rights (approval of the use of special powers, whether or not additional external approval is required, for instance, from a judge).	✓ the duty to implement government policy; ✓ the duty to report to ministers; ✓ the duty to seek approval of specified sensitive matters.

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

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

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

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

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

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

Best Practice

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

Chapter 11

Control over Covert Action

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

Box No. 23:
Covert Action Defined (US)

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

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

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

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

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

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

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

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

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

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

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

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

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

Box No. 25:
Torture

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

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

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

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

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

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

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

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

Section 6 Functions of ASIS

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

Section 6A Committee to be advised of other activities

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

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

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

Best Practice

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

Chapter 12

International Cooperation

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

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

Box No. 27:

Various Practices of Intelligence Cooperation: Bilateral Sharing

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

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

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

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

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

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

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

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

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

- The issue of 'plausible deniability'

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

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

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

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

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

> [B]y using torture, or even by adopting the fruits of torture, a democratic state is weakening its case against terrorists, by adopting their methods, thereby losing the moral high ground an open democratic society enjoys.[22]

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

- Giving information on national citizens to foreign security services

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

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

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

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

Source: *Bundesverfassungsschutzgesetz* (BVErfSchG), Germany, November 2002, Art. 19 (*Unofficial translation*).

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

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

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

Source: Law on the Intelligence and Security Agency, Bosnia and Herzegovina, 2004, Art. 6.

Best Practice

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

Chapter 13

Safeguards against Ministerial Abuse

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

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

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

Safeguards

The legislation governing security and intelligence agencies should contain clear arrangements for political direction and, in the case of internal agencies, political independence, to ensure that matters of policy are determined by politicians accountable to the public. The rights of the executive ought to be counter-balanced to prevent misuse by the executive of the agencies. Various forms of safeguards may be used for this purpose. In Canada, Hungary and Australia there is a requirement that

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

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

Section 11
1 (b) The Minister shall determine in writing the topical tasks of the services for the directors general semi-annually; shall give orders in writing for meeting the information requirements received from the members of the Government.
Source: Act on the National Security Services 1995, Hungary, Section 11.

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

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

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

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

Within a wider frame of checks and balances, the Australian intelligence legislation features another safeguarding provision, namely the duty of the Director-General to brief the Leader of the Opposition.[24] Notice that this is also established informal practice in other national settings aiming, *inter alia*, at the prevention of ministerial abuse. A bipartisan approach to security and intelligence is more likely to be maintained if leading opposition parliamentarians do not feel that they have been wholly excluded from the 'ring of secrecy'. The Australian example is one operating within a Westminster-style democracy, albeit a federation. In a more complex federal presidential state there may be a range of actors who should be briefed on 'a need to know' basis.[25]

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

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

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

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

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

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

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

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

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

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

Best Practice

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

Endnotes Section III – The Role of the Executive

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

which he is accused'. Article 31 of the Fourth Geneva Convention: 'No physical or moral coercion shall be exercised against protected persons, in particular to obtain information from them or from third parties'.

See also Article 12, Declaration on the Protection of All Persons from Being Subjected to Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; Article 69(7) of the Rome Statute of the International Criminal Court; Principle 27, UN Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment.

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