Section II

The Agency

Chapter 4

Defining the Mandate

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

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

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

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

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

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

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

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

Source: ECHR case-law.

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

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

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

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

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

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

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

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

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

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

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

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

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

Maintaining Political Neutrality

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

Box No. 8:

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

'No intelligence agency shall:

1. Perform repressive activities, have compulsive powers, fulfil police functions or conduct criminal investigations unless so required by justice on account of a judicial proceeding or when so authorised by law.
2. Obtain information, collect intelligence or keep data on individuals because of their race, religion, private actions, and political ideology, or due to their membership in partisan, social, union, community, cooperative, assistance, cultural or labour organisations, or because of legal activities performed within any field.
3. Exert influence over the institutional, political, military, police, social, and economic situation of the country, its foreign policies, and the existence of legally formed political parties, or influence public opinion, individuals, the media, or any kind of associations whatsoever'.

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

Best Practice

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

Chapter 5

Appointing the Director

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

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

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

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

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

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

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

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

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

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

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

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

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

Best Practice

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

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

Chapter 6

Authorising the Use of Special Powers

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

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

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

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

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

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

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

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

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

Box No. 13:

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

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

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

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

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

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

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

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

Use of Intelligence Information in Court Proceedings

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

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

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

Oversight of Special Powers

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

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

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

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

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

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

Box No. 14:
Cases of the European Court of Human Rights on the Right to Privacy

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

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

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

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

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

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

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

Best Practice

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

Chapter 7

Information and Files

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

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

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

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

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

Article 47 – Right to inspection of personal data

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

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

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

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

Best Practice

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

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

Chapter 8

Internal Direction and Control of the Agency

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

Reporting on Illegal Action

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

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

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

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

Source: Bosnian Law on the Intelligence and Security Agency.

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

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

Box No. 17:
Disclosure Protection Rules (Canada)

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

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

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

Professional Code of Ethics for Security and Intelligence Services

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

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

Box No. 18:

South African Code of Conduct for Intelligence Employees

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

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

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

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

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

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

Box No. 19:

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

Article 27

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

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

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

Best Practice

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

Endnotes Section II – The Agency

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

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

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