This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
REPORT

Intelligence and Security Legislation for Security Sector Reform

Greg Hannah, Kevin A. O'Brien, Andrew Rathmell

Prepared for the
United Kingdom's Security Sector Development Advisory Team

RAND EUROPE

The research described in this report was prepared for the United Kingdom's Security Sector Development Advisory Team.

Published 2005 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
Newtonweg 1, 2333 CP Leiden, The Netherlands
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
Uhlandstraße 14, 10623 Berlin, Germany
RAND URL: http://www.rand.org/
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

This report was prepared for the UK's Security Sector Development Advisory Team. Its aim is to act as a basis for discussion and to provide an opportunity to learn from the successes and failures of intelligence and security legislation in various countries. The report outlines the choices that need to be made when designing or implementing legislative oversight on intelligence and security services. The report will be of interest to policy makers in countries seeking to reform their security sectors and to practitioners in the international aid community seeking to support security sector reform.

The information in this report is drawn from a number of published and unpublished studies, updated and informed by the knowledge of RAND staff in this domain. No original fieldwork was undertaken for this study.

This document does not necessarily reflect the views of the SSDAT or the British Government

For more information about RAND Europe or this document, please contact the authors at:

RAND Europe (UK)
Grafton House
64 Maids Causeway
Cambridge CB5 8DD
United Kingdom
T: 44 (0) 1223-353329
F: 44 (0) 1223-358845
E: reinfo@rand.org

Contents

Executive Summary

This study was undertaken on behalf of the United Kingdom's Security Sector Development Advisory Team. Its aim is to act as a basis for discussion and to provide an opportunity to learn from the successes and failures of intelligence and security legislation in various countries. Drawing on the body of academic work in this field and the knowledge of RAND staff, this report: provides a definition of intelligence; describes in detail how intelligence is produced; examines the role of intelligence in security sector reform; highlights the importance of control and accountability in intelligence structures; examines how six countries have developed and implemented intelligence legislation and associated reforms; and, finally, draws out a number of key lessons to be considered in any future security sector reform activity encompassing intelligence structures.

Intelligence in security sector reform

As the security sector reform (SSR) agenda has developed over the last decade, intelligence has been the most oft-overlooked element. Increasingly, however, intelligence is being included as a key element of SSR. Intelligence can both support SSR and be the target of reform activities. The most crucial task facing countries embarking on SSR processes is to build a nationally owned and led vision of security. This can be achieved through a national security review to elaborate an overarching policy on national security. Such a review allows a government to distinguish between legitimate and illegitimate security activity, and helps choose between competing claims for resources.

Intelligence services can make a significant contribution to this process through the provision of accurate intelligence on the range of risks and threats faced by the state. In addition to assisting the process of SSR, intelligence agencies and services themselves frequently require reform. There are numerous examples where the intelligence services of the state have been involved in serious human rights abuses and have colluded in maintaining a corrupt or tyrannical regime. Thus, there may be a requirement to evolve the intelligence agencies and structures of a transitional state through the SSR process, potentially through the development and implementation of reforming legislation.

Defining intelligence

Intelligence is a special kind of knowledge, a specialised subset of information that has been put through a systematic analytical process in order to support a state's decision and policy makers. It exists because some states or actors seek to hide information from other states or actors, who in turn seek to discover hidden information by secret or covert means.

Within a security sector reform context, intelligence has also been defined as the 'production of unbiased information about threats to the national vision'. Intelligence can be three things: a

process of gathering and analysing information; an **organisation** which undertakes the process; and a refined **product** that is delivered to policy makers.

Intelligence as a process

Intelligence is a process by which data is refined into a usable form for decision-makers. It is also a structure of organisations that collect and process information. It is the relationship between processes and structures that determines the successful outcome of the intelligence activity.

Intelligence as a structure

There are several considerations that influence the structures of intelligence services. Some of these considerations include:

- The roles and mandates adopted by one or more services (i.e. are there different agencies for both the domestic and foreign role?) – as well as understanding overlaps between intelligence agencies and other players (such as law enforcement) in the security community
- The shape of any central analysis and/or assessments mechanism to process collected intelligence
- The need to ensure central control and co-ordination of, and accountability for, the intelligence community
- The need to ensure public oversight of the intelligence community

The different but frequently overlapping categories of intelligence – for example foreign, domestic, criminal and military – have spawned separate intelligence services in different countries. In some (mostly authoritarian) states, one agency often undertakes both internal and external roles simultaneously (for example, the KGB in the former Soviet Union). The typical separation of domestic, foreign and specialist intelligence functions into separate agencies requires co-ordination of intelligence collection and analysis; this is especially the case when the cross-border aspect of threats such as terrorism leads to the collection of information on the same targets by a number of agencies.

Intelligence as a product

Intelligence services are responsible for the collection, processing and dissemination of information, in order to ensure the security of the society and the freedom of its citizens. Modern intelligence agencies generally provide three key services:

- intelligence on foreign or external threats
- intelligence on threats to internal security:
- intelligence-led advice on policy- and decision-making

Purpose of Security and Intelligence Legislation

Security and intelligence activities are increasingly subject to legislative frameworks which provide the mandate, co-ordination and control, and oversight and accountability guidelines for intelligence communities. Such legislation will only be effective if it takes account of the apparently competing requirements of secrecy and democratic oversight. Placing intelligence agencies on a legislative basis provides them with a clear set of operating parameters and a legal mandate for their work – it is only if security and intelligence agencies are established by law and derive their powers from legislation that they can enjoy legitimacy. Also less tangibly, a legal framework can help to reinforce democratic values and give them a symbolic status, which may encourage powerful actors to respect them.

However it cannot be assumed that legislation will result in a change in intelligence agencies' behaviour. Accountability mechanisms must be developed to ensure that intelligence services implement and adhere to the legal framework imposed upon them. Achieving lasting change within intelligence services that have an established history of autonomy or rogue activity requires long-term political will and effective oversight mechanisms, both internal and external. Placing security agencies within a legal structure also has important constitutional consequences, as intelligence oversight is shifted, at least partly, to the legislature and/or the judiciary.

Role of oversight and accountability

There is a distinction to be drawn between the concepts of 'control' and 'accountability'. Control is the set of constraints under which an intelligence agency operates, whereas accountability is an information process whereby an agency is under a legal obligation to answer truly and completely the questions put to it by an authority to which it is accountable (for example, a parliamentary intelligence oversight committee). The components of effective oversight and accountability include:

- **Executive accountability** - due to the inherent secrecy of their activities, effective control of intelligence agencies can only be exercised by the executive in the form of ministers. Ministers need to have sufficient powers to exercise control over intelligence services – including the right to demand information from those agencies.
- **Parliamentary oversight** - oversight by the legislature of intelligence services enhances their legitimacy and democratic accountability, while ensuring that these agencies are serving the state as a whole rather than a narrow political or other interest. The involvement of parliamentarians can also help to ensure that public funds are properly accounted for.
- **Legal compliance** – The principal mechanism for ensuring legal compliance is judicial review. Judges are often perceived to be independent of government and, traditionally, the role of the courts is to protect individual rights.

Case-Studies & Methodology

To better understand specific issues regarding intelligence processes, structures, and roles, it is useful to look at particular case-studies to demonstrate how individual countries have addressed the issues. The case-studies chosen cover a wide range of nations—from developed to developing nations, from different governance systems, and from different heritages. The six nations chosen for analysis were:

- United Kingdom
- Canada
- South Africa
- Argentina
- Germany
- The Czech Republic

These case studies were chosen, in agreement with the client, in order to achieve a balance between developed and developing world, and between those that have experienced evolutionary versus revolutionary reforms in their intelligence structures. These also offer a wide range of useful learning points for those utilising this report.

Lessons identified

From the above case-studies and the body of academic work in this field, it can be concluded that a number of key issues must be addressed to make intelligence and security legislation meaningful. These fall into four key areas from which lessons can be drawn:

- **Intelligence Mandates** - the agency or community that is being legislated for must be given a clearly-defined mandate for its activities; legislation also can be used to establish distinct agency boundaries between domestic, foreign and military intelligence activity, as well as the types of activities undertaken.
- **Central Co-ordination, Oversight and Accountability** - through central co-ordination, states can check that individual agencies do not overlap, become involved in rivalries, and ensure that complimentary collection and analysis paths are followed. Such centralised oversight also serves to assure the public that all capabilities and agencies are being watched over by one body, ensuring against duplication and that gaps are being filled. A further key requirement of intelligence legislation is to provide clear lines of accountability, while subordinating intelligence services to the control of democratically-elected leaders. The inherent secrecy that surrounds the activities of intelligence services makes it vital that both the executive and other oversight actors scrutinise the actions of these agencies.
- **Judicial Oversight** - in several of the cases above, the judicial system plays a role in regulating the activities of intelligence services in the domestic sphere. This primarily relates to instances when services wish to encroach upon the rights of individual citizens by means of intrusive surveillance or covert searches. Judicial oversight is required to set

limits to achieve the proper balance between the protection of individual rights and the collection of necessary information.

- **Parliamentary Oversight and Accountability** - Legislative involvement in the oversight of intelligence services enhances legitimacy and democratic accountability, while ensuring that security and intelligence agencies are serving the state as a whole rather than narrow political or other interests. There are many models of parliamentary oversight, with some being more robust than others.

In addition to these generic areas, it is also important to recognise differences between developed and developing countries when considering the implementation environment for security section reform. In the countries examined, there were a variety of factors influencing the environment in which intelligence legislation was developed and implemented. These factors exerted influence both from within the agencies and the executive as well as externally from parliament, the public, the media, foreign states and international bodies. Some or all of these pressures are likely to be felt in other developed and developing states which undertake intelligence reform.

1. What role Intelligence in modern society?

Intelligence is Knowledge. It can be decision-oriented or action-oriented; it is the pursuit of information required for decision or action – ideally allowing its users to optimise their actions. Intelligence has been defined as 'information that meets the stated or understood needs of policy makers and has been collected, refined and narrowed to meet these needs'.[1]

Intelligence as a requirement for the state

Intelligence is not just information; it is a specialised subset of information that has been put through a systematic analytical process in order to support a state's decision and policy makers. Intelligence is also differentiated from other types of information due to the secrecy that is often involved in its collection or concealment. Intelligence exists because some states or actors seek to hide information from other states or actors, who in turn seek to discover hidden information by secret or covert means.[2]

What makes 'intelligence' different from 'information'? Three key elements: *collection*, *analysis* and *dissemination*. *Collection* is the procurement of information believed to be pertinent to decision-makers (sometimes referred to as 'raw' intelligence data); *analysis* (sometimes referred to as *evaluation and production*) is the process of sifting, sorting and judging the credibility of that collected information, drawing pertinent inferences from its analysis, and interpreting such inferences in keeping with the requirements of decision-makers; and *dissemination* is the act of communicating the intelligence findings in the form most suitable to the decision-maker.[3]

Intelligence has been defined as a special kind of knowledge that 'a state must possess regarding other states in order to assure itself that its cause will not suffer nor its undertakings fail because its statesmen and soldiers plan and act in ignorance'.[4] Within a security sector reform (SSR) context intelligence has also been defined as the 'production of unbiased information about threats to the national vision'.[5] This is especially important in situations – such as many of those encountered in SSR – where government resources are limited and requirements many: accurate intelligence allows for limited resources to be applied efficiently towards a goal.

Intelligence has three dimensions:

- Intelligence as a **process** by which information is gathered, processed and analysed to aid in decision making
- Intelligence as an **organisation** – the functional structures that exist to undertake the intelligence process
- Intelligence as a refined **product** (resulting from collection and analysis) delivered to customers to support those decisions – whether immediate or long-term

The different categories of intelligence include:

[1] Lowenthal (2002): 2.
[2] Lowenthal (2002): 1.
[3] Ransom (1958): 13-14.
[4] Kent (1966): 3.
[5] Wilson (2004): 5.

- **National Intelligence**: high-level integrated intelligence covering broad national strategy and transcending the exclusive competence or needs of a single department

- **Strategic Intelligence**: information regarding the capabilities, vulnerabilities, and intentions of foreign nations required by planners in developing the basis for an adequate national security policy in time of peace; also provides the basis for projected overall military operations in time of war

- **Tactical Intelligence:** collection under devolved control, normally geared to produce intelligence for use at the command level to which it is devolved; of short-term rather than long-term use

- **Foreign Intelligence:** intelligence on foreign targets, including external threats

- **Security Intelligence**: Intelligence on internal threats

- **Counterintelligence:** that phase of intelligence activity devoted to countering the effectiveness of hostile foreign intelligence operations (Ransom, 1958); or the targeting of opponents' human intelligence agencies and attempts to penetrate them by human means; intelligence on any foreign intelligence agency, obtained by any means

- **Counterespionage**: the detection of espionage

- **Assessment**: definitive all-source intelligence products written for executive users, often with policy implications

Finally, while not an actual category of intelligence, **covert action** should also be considered as part of intelligence activities, as it is generally undertaken (in this context) for intelligence purposes (i.e. either driven by or attempting to generate intelligence). Covert action can be defined as those "activities conducted abroad in support of national foreign policy objectives which are designed to further official government programmes and policies abroad and which are planned and executed so that the role of the government is not apparent or acknowledged publicly".[6]

Products of intelligence services

Intelligence services are responsible for the collection, processing and dissemination of information, in order to ensure the security of the society and the freedom of its citizens.[7] Modern intelligence agencies provide three key services:

- **intelligence on foreign or external threats**: two of the main drivers behind a foreign intelligence capability today are, first, to learn and understand as much as possible about other states' capabilities (whether friend or foe), and, second, to prevent a foreign power achieving strategic surprise (such as the Japanese attack on Pearl Harbour in December 1941). To do this requires access to both secret and open source information, primarily focused on national security, military and defence, political, economic and foreign policy issues; it will also take into account social, environmental and cultural intelligence. The

[6] These definitions are drawn collectively from Ransom (1958), Johnson (1989), and Herman (1996).
[7] Born (May 2002): 3.

UK's Secret Intelligence Service (SIS) and the USA's Central Intelligence Agency (CIA) are primary examples of intelligence agencies centred on this type of activity.

- **intelligence on threats to internal security**: 'security intelligence' focuses on those threats that operate internally rather than externally. Security intelligence has some distinctive features, specifically its affinity with police forces in detecting particular activities which drives such agencies in different ways to foreign intelligence agencies.[8] However, these distinctions are becoming blurred as domestic and foreign intelligence activities increasingly overlap in the 21st Century - particularly the case in the realm of counter-terrorism which can encompass threats to domestic targets (including critical national infrastructure), overseas embassies, armed forces or commercial interests in foreign countries. Such security intelligence can also provide support to the 'softer' side of security concerns, such as those national contingencies – like lawful protest and other malicious but non-violent activities – where the government has a need to know.

- **intelligence-led advice on policy and decision-making:** intelligence is also used – beyond its immediate applications as noted in the above two bullets – to support the wider policy-formulation and decision-making processes of government. This can occur through the provision of either tactical intelligence data to government or strategic intelligence assessments which provide a long(er)-term view of a particular issue. Ultimately, it allows governments to reduce certainty and manage risk through bounding the possible set of futures that the government may be faced with, while giving that government the ability to see opportunities where and when they arise.

[8] Herman (1996): 47.

2. Intelligence as a process and a structure

Intelligence is a process by which data is refined into a usable form for decision-makers. It is also a structure of organisations that collect and process information. It is the relationship between processes and structures that determines the successful outcome of the intelligence activity.

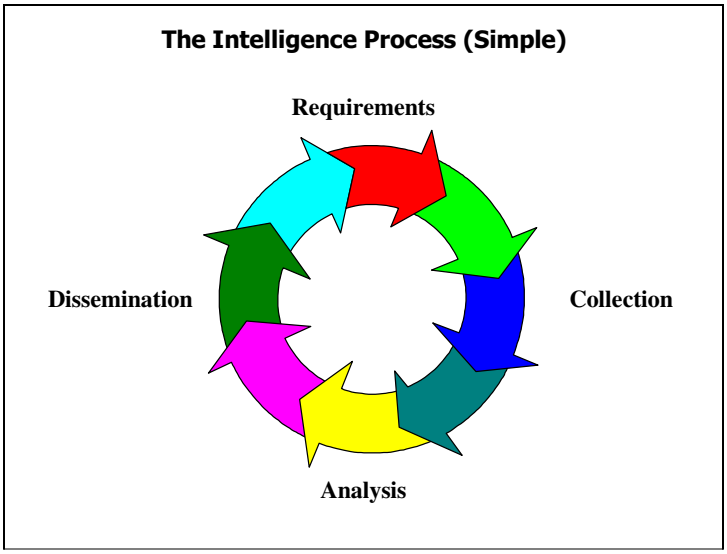
Intelligence as process

The intelligence process has four main phases:

- collection
- processing
- analysis
- dissemination

The classic intelligence cycle outlines a uni-dimensional, uni-directional process (see Figure 1).

Figure 1: The Intelligence Process – Simple



Collection is the means of gathering raw information that forms the basis for refined intelligence. This can be undertaken by a variety of methods, ranging from using covert human agents or informers (referred to as Human Intelligence or HUMINT) to the interception of electronic communications (known as Signals Intelligence or SIGINT) and satellite images (Imagery Intelligence or IMINT). No one source is likely to provide a full understanding of an issue, therefore agencies will attempt to use as many sources as possible to arrive at the most accurate picture of events. This is referred to as All-Source Intelligence.[9] A fundamental question here is 'what to collect', or 'what can be collected?' The limited collection resources (both HUMINT and SIGINT) of agencies must be prioritised to a number of issues or targets. This inevitably means that some areas will be left with little or no coverage. There is also a danger – particularly with technical collection means (e.g. SIGINT) – that the system will gather much more information than the receiving agency or organisation has the capacity to absorb and process,

[9] Lowenthal (2002): 54.

potentially missing small but vital pieces of intelligence, often referred to as the 'collection to analysis imbalance'.

Turning the potentially large quantities of information gathered by collection methods into a format suitable for closer inspection is known as **Processing**. An example would be the decryption of intercepted coded signals intelligence. It is here that the issue of collection versus processing capacity comes to the fore. The US intelligence community, with its large SIGINT collection means, routinely collects more information than it can usefully process – for example, towards the end of the Cold War, the US National Security Agency was reportedly processing only 20 per cent of the information it collected[10].

Analysis is arguably the most important part of the intelligence process. It is the means by which the information gathered and processed from a variety of sources is pulled together and developed into a usable product to help decision-makers address the issues of the day. In some systems, different agencies will be focused on one primary means of collection (e.g. in the UK, the SIS is a HUMINT-focused organisation, whilst GCHQ works exclusively on SIGINT), relying on other organisations in the structure to undertake the analysis of their processed material. In others, such as the US, different agencies will undertake the entire collection, processing, analysis and dissemination process within their own structures; this is known as competitive analysis, with each agency undertaking its own analysis of an issue, on the basis that this approach will make the overall analysis stronger and is therefore more likely to provide decision makers with the most accurate intelligence.

The distribution of completed intelligence analysis is referred to as **Dissemination**. This is the means by which policy-makers receive the collected, processed and analysed intelligence. The key issue here for the agencies is how to present the information in a manner which meets the requirements of decision-makers – both in content and presentation – while ensuring that it highlights sufficiently the limitations of the intelligence to answer the questions of the day.

Intelligence as structure

There are several considerations that influence the structures of intelligence services. Some of these considerations include:

- The roles and mandates adopted by one or more services (i.e. are there different agencies for both the domestic and foreign role?) – as well as understanding overlaps between intelligence agencies and other players (such as law enforcement) in the security community
- The shape of any central analysis and/or assessments mechanism to process collected intelligence
- The need to ensure central control and co-ordination of and accountability for the intelligence community
- The need to ensure public oversight of the intelligence community

The establishment of differentiated intelligence services

There are four different but frequently overlapping categories of intelligence – foreign, domestic, criminal and military – which, in turn, have spawned separate intelligence services in different

[10] Johnson (1996): 21.

countries. In some (mostly authoritarian) states, one agency often undertakes both internal and external roles simultaneously (for example, the KGB in the former Soviet Union).

The mission of domestic or **security intelligence** services (such as the Canadian Security Intelligence Service or Britain's Security Service) is to obtain, correlate and evaluate intelligence relevant to internal security. Internal security aims to protect the state, territory, society and people against malicious acts – including terrorism, espionage, sabotage, subversion, extremism, organised crime, and drugs production/trafficking. Sometimes, law enforcement bodies are involved in 'security policing'; the UK's Special Branch structure is a good example of a law enforcement-based security intelligence service.

The task of **foreign intelligence** services (such as the US Central Intelligence Agency or the South African Secret Service) is to obtain, correlate and evaluate intelligence relevant to external security and for warning purposes. Protection of external security requires knowledge of the threats, dangers, and risks, as well as of the opportunities and likelihood of events and outcomes. Therefore, information is needed about the intentions, capabilities and activities of foreign powers, organisations, groups or persons, and their agents that represent actual or potential threats to the state and its interests.

Intelligence and law enforcement have very different purposes; the task of intelligence is to collect as much information as possible on a broad spectrum of actual or potential threats to the state or society; law enforcement seeks to obtain convictions related to specific criminal offences. Despite this difference, **criminal intelligence** agencies (which collect information on organised crime activities with an aim to prosecution – such as the UK's National Criminal Intelligence Service) do require skills similar to those of classic intelligence work.

In addition to foreign intelligence on foreign powers' intentions, defence ministries and armed forces have historically required intelligence on potential adversaries military capabilities. This has given rise to the existence of, in many states, a specialised **defence or military intelligence** arm or service (such as the Intelligence Division of the South African National Defence Force).

The central co-ordination of intelligence

The typical separation of domestic, foreign and specialist intelligence functions into separate agencies requires coordination of intelligence collection and analysis; this is especially the case when the cross-border aspect of threats such as terrorism leads to the collection of information on the same targets by a number of agencies. Examples of this type of co-ordinating role are the Director of National Intelligence (previously the Director of Central Intelligence) and the National Security Council in the United States; the Security and Intelligence Co-ordinator and the Joint Intelligence Committee in the UK[11]; and the National Intelligence Co-ordinating Council (NICOC) in South Africa.

The central assessment of intelligence

Most of the different models examined apply – to a greater or lesser degree – a central assessment of intelligence. The strictness to which this is adhered varies to a large degree. For example, the UK's Joint Intelligence Committee's (JIC) provides one model – replicated by Canada, Australia and others – whereby all different sources of intelligence are integrated into a developed product,

[11] The JIC's role is to 'give direction to, and keep under review, the organisation and working of British intelligence activity as a whole at home and overseas in order to ensure efficiency, economy and prompt adaptation to changing requirements': Herman (1996): 28.

especially but not exclusively covering strategic intelligence interests, for the policy-makers to consider. In this system, most agencies provide a combination of raw and refined intelligence data to the central assessments mechanism, which is then processed and turned into a product. Under the US model – involving the Office of the Director of Central Intelligence and the National Security Council, alongside the individual agencies[12] – a more disparate product is developed, oftentimes involving a degree of competition between the different collection agencies to produce the best intelligence assessment (generally referred to in the US as an 'intelligence estimate').

Some countries have opted to adopt a hybrid approach – South Africa is one of these. This combines a central assessments mechanisms through the National Intelligence Co-ordinating Committee's National Intelligence Estimates Board and a more disparate approach through the assessments capabilities of both the National Intelligence Agency and the SANDF Intelligence Division, as well as intelligence elements attached to the Office of the State President.

Another recent development in terms of centralised analysis and assessments is the establishment in a number of the countries of a centralised counter-terrorism assessments capability. New agencies include the UK's Joint Terrorism Analysis Centre (JTAC), the US's National Counter-Terrorism Center (NCTC), the Canadian Integrated Threat Assessment Centre (ITAC), and Australia's National Threat Assessment Centre (NTAC).

[12] This is currently changing as the roles of both the new Director of National Intelligence and the National Counter-Terrorism Center are further defined.

3. What role Intelligence in SSR?

As the security sector reform (SSR) agenda has developed over the last decade, intelligence has been the most oft-overlooked element. Increasingly, however, intelligence is being included as a key element of SSR. Intelligence can both support SSR and be the target of reform activities.

Intelligence to support SSR

States that have undergone significant changes in their forms of governance or ruling ideology are likely to also undergo changes in their external relationships with other states and actors. This may involve a shift in alliances or forging new relationships with a previously hostile neighbour. There is a danger that the perception of old risks to the transitional state may be maintained due to both historical prejudice or experience – policy-makers or security actors may be unable to jettison the historical baggage associated with previous conflicts. It is equally possible that new risks that have emerged as a result of transition are not recognised or prioritised because they do not fit with the established preconceptions of the leadership. Previously hostile states may find it difficult to overcome such enmity and struggle to provide convincing evidence of benign intent.

Intelligence services can play a key role in overcoming this issue, given their access to secret sources that should provide them with the widest possible view, compared to many of the other players in such a situation.[13] In situations where conflict has not yet ended but the parties wish to conduct initial negotiations towards a potential settlement, the secrecy involved in intelligence circles means that intelligence services can be used to make overtures to former enemies who are not yet trusted by the wider population. This was the case in South Africa where the Apartheid government used its intelligence apparatus to conduct secret exploratory talks with the African National Congress.

Intelligence as an advisory function in SSR

The most crucial task facing countries embarking on SSR processes is to build a nationally-owned and -led vision of security. This is the foundation that countries require to develop appropriate security systems and security policy frameworks, including the required institutional mechanisms to implement them.[14] This can be achieved through a national security review to elaborate an overarching policy on national security, that is set in the context of overall national development goals while clarifying the distinctions between internal and external security.

Such a review performs two functions: a) it allows a government to distinguish between legitimate and illegitimate security activity, and b) it helps a government to choose between competing claims for resources both within the security sector, and between the security sector and other societal sectors such as health or education.[15] Intelligence services can make a significant contribution to this process through the provision of accurate intelligence on the range of risks and threats faced by the state. It is worth noting that this is not always easy to achieve – there are examples (such as Czechoslovakia) where intelligence services are unable to adjust to the new strategic situation and continue to focus on old threats and enemies who may now be allies.

[13] Wilson (2005): 6.
[14] OECD (2004): 19.
[15] Wilson (2005): 4.

Intelligence as an object of SSR

In addition to assisting the process of SSR, intelligence agencies and services themselves frequently require reform. There are numerous examples where the intelligence services of the state have been involved in serious human rights abuses and have colluded in maintaining a corrupt or tyrannical regime. Thus, there may be a requirement to evolve the intelligence agencies and structures of a transitional state through the SSR process. Indicators of where services may require reform include:

- the balance between the necessary secrecy of the intelligence services and transparency regarding their mandates and their powers
- the existence of oversight structures to minimise maladministration
- the extent of control over and public accountability for the financing of intelligence services
- the controls in place to govern the use of intrusive methods of intelligence collections
- the professionalism and ethics of intelligence officers

4. What purpose Security and Intelligence legislation?

Around the world, security and intelligence activities are increasingly being subjected to legislative frameworks. These frameworks provide the mandate, co-ordination and control, and oversight and accountability guidelines for intelligence communities.

Legislating a sensitive area: mandate, oversight and accountability

The world of intelligence is a sensitive one – not only in terms of the nature of the sources which contribute information to the intelligence process, but also in terms of the desire by many intelligence services to operate outside of oversight and accountability. For both of these reasons, legislation will only be effective if takes account of these two contrasting – indeed competing – dynamics. On the one hand, intelligence requires a 'cloak of secrecy' in which to operate effectively. On the other hand, intelligence methods and products require strong oversight to ensure both that the state is not engaging in activities that violate human rights or basic democratic principles, and that the intelligence process is robust and effective enough to ensure demonstrable support for the products and recommendations given to decision-makers resulting from the intelligence. Legislating for both of these functions – oversight of activities, accountability for methods and processes – is a permanent challenge.

Providing Security & Intelligence services with an operating mandate and framework

Historically, a key reason for placing intelligence agencies on a legislative basis was to provide them with a clear set of operating parameters and a legal mandate for their work. The rule of law is a fundamental and indispensable element of democracy – it is only if security and intelligence agencies are established by law and derive their powers from legislation that they can enjoy legitimacy. The exceptional powers of such services must be grounded in a legal framework and within a system of legal controls. Such legislation also allows elected representatives to address the principles that govern this area of state activity and set down limits to the work of intelligence agencies. [16]

There is arguably a greater need to legislate for domestic security intelligence agencies (due to potential for abuses against a state's own citizens as has been witnessed in many transitional states with repressive histories), though some states – including the UK – have legislated for their foreign intelligence arms also. The rule of law requires that security and intelligence services should act within their powers as set down in domestic legislation, especially where it is intended to qualify or restrict the constitutional rights of citizens, in the security interests of the state. [17]

Less tangibly, a legal framework can help to reinforce democratic values and give them a symbolic status, which may encourage powerful actors to respect them. This is particularly true where new institutions are created – the legal framework can be a means of inculcating a new democratic

[16] Born and Leigh (2005): 17.

[17] For example, the European Convention on Human Rights (ECHR) allows restrictions to the rights of public trial, respect for private life, freedom of religion and expression and of association 'in accordance with law' and where 'necessary in a democratic society' in the interests of national security (Articles 6, 8, 9, 10 and 11 ECHR): Leigh I 'Democratic Control of Intelligence and Security Services: A Legal Framework' (2003): 116; consequently, only lawful action can be justified by way of interference with human rights under the European Convention: Born and Leigh (2005): 19. The European Court of Human Rights also applies a 'quality of law test' whereby the legal regime governing the activities of the intelligence services is to be clear, foreseeable and accessible.

order and consolidating reforms. It also provides a relatively clear standard against which compliance may be measured. Indeed, the use of legal standards enables those who transgress to be disciplined or dismissed in a way that cannot be portrayed as arbitrary.[18] In addition, laying down a legal structure within which institutions may operate has at least the potential to make it easier for victims of abuses of power to seek some form of redress (i.e. a system of complaints handling and investigation).

Providing oversight and accountability for Security & Intelligence operations and agencies

There is a danger in assuming that legislation will, solely by its passing, cause a change in intelligence agencies' behaviour. It is important also to develop accountability mechanisms to ensure that intelligence services actually implement and adhere to the legal framework imposed upon them.[19] Achieving lasting change within intelligence services that have an established history of autonomy or rogue activity requires long-term political will and effective oversight mechanisms, both internal and external. Placing security agencies within a legal structure has important constitutional consequences. The execution of intelligence oversight no longer remains exclusively within the executive, but is shifted at least partly to the legislature and/or judiciary. It may also involve the public more – for example, through the media as a public forum, as information is no longer held entirely by the executive.[20]

[18] Lustgarten (2003): 323.

[19] Gill P '*Democratic and Parliamentary Accountability of Intelligence Services after September 11th*', Working Paper No.103, Geneva Centre for the Democratic Control of the Armed Forces: 3.

[20] Lustgarten (2003): 232-234.

5. The role of oversight and accountability

There is a distinction to be drawn between the concepts of 'control' and 'accountability'. Control is the set of constraints under which an intelligence agency operates. The legislative mandate and parameters provided by an intelligence law such as the Canadian Security Intelligence Act (1984) is an example of such control. Accountability is an information process whereby an agency is under a legal obligation to answer truly and completely the questions put to it by an authority to which it is accountable (for example, a parliamentary intelligence oversight committee).

The components of effective oversight and accountability

Executive accountability

It is a basic tenet of democratic systems that defence and intelligence actors are placed under the control of elected politicians. Due to the inherent secrecy of their activities, effective control of intelligence agencies can only be exercised by the executive in the form of ministers. Ministers need to have sufficient powers to exercise control over intelligence services – including the right to demand information from those agencies. Indeed, such ministerial control and accountability is essential to enabling effective parliamentary oversight (see below).

The need to ensure the flow of information necessary to seeing that the services are following government policy has led several states to create the post of Inspector-General. Typically, Inspectors-General carry out audits of intelligence service activities, then report to the executive on the compliance of the services with both policy and the legal framework in which they operate. In some countries (e.g. Canada) the Inspector-General carries out work on behalf of the parliamentary oversight committee.

Parliamentary oversight

In a democratic state, no area of government activity should be out of bounds to the legislature. Oversight by the legislature of intelligence services enhances their legitimacy and democratic accountability, while ensuring that these agencies are serving the state as a whole rather than a narrow political or other interest. The involvement of parliamentarians can also help to ensure that public funds are properly accounted for.[21]

An effective parliamentary oversight committee has the following features:

- its functioning and powers are based on rules of procedure
- it has control over its own schedules
- it has the power to demand that ministers and officials testify at meetings
- it normally meets behind closed doors (for security purposes)
- the committee reports annually to parliament (without disclosing classified information)
- it is entitled to request any information, providing it does not disclose information on current operations or the names of sources
- it may disclose any information after it has determined that the public interest would be served by such a disclosure

[21] Born and Leigh (2005): 77.

- the committee has its own meeting rooms, staff, budget and documentation system (capable of handling classified material)[22]

Whilst parliamentarians can make a significant contribution to the oversight and, consequently the effectiveness, of intelligence services, there are a number of difficulties in this area. Perhaps most obvious is the issue of secrecy. Much of the knowledge and documentation relating to the structure, policies, administration and above all operations of intelligence services are necessarily classified. This generates a number of problems: for example, there is a possibility that a committee or one of its members may deliberately or inadvertently disclose information that compromises an ongoing operation or source - some governments have used this as a justification for denying intelligence oversight committees access to documentation or officials. There are also practical issues, such as the need to provide secure office and storage space, or whether parliamentarians (and their staff) are required to be security vetted.

There is also the risk that intelligence services could be dragged into political controversy by politicians seeking partisan advantage. If sensationalised, such debates may lead the public to form an unnecessarily negative perception of intelligence services and lead to a lack of trust between the agencies and parliamentarians. Conversely, parliamentarians may be reluctant to become involved in intelligence oversight work precisely because it is largely conducted behind closed doors, denying them opportunities to demonstrate their achievements to the electorate. Finally, there is sometimes a tendency to not want to know what intelligence agencies get up to in the course of their duties. A member of the US Senate Armed Services Committee once remarked '[t]here are things that my government does that I would rather not know about'. Such reluctance may arise from a personal ethical objection to such activities or, for those in the governing party, a desire not to criticise the government.

Legal compliance

The principal mechanism for ensuring legal compliance – in addition to the other mechanisms of oversight and accountability discussed above – is judicial review. Such judicial scrutiny has two clear strengths: first, judges are perceived to be independent of government, while, second, the traditional role of the courts is to protect individual rights. Therefore they are well-suited to oversight tasks in areas such as the surveillance of individuals. One challenge this raises is that sensitive information must be shared outside the services. Furthermore, too intrusive a role could carry judges into the realm of the executive, which risks politicisation of the process. In addition, much of security work (such as surveillance) will only be regulated in this manner if the individual affected is aware and brings a complaint against the service. In some states, legal barriers prevent judicial reviews.[23]

[22] Born (May 2002): 13.
[23] Leigh (2003): 123.

6. Case-Studies of Legislating Security and Intelligence

To better understand specific issues regarding intelligence processes, structures, and roles it is useful to look at particular case studies to demonstrate how individual countries have addressed the issues. The case studies chosen cover a wide range of nations—from developed to developing nations, from different governance systems, and from different heritages. The six nations chosen for analysis are:

- United Kingdom
- Canada
- South Africa
- Germany
- The Czech Republic
- Argentina

United Kingdom

Challenges

As a result of a number of human-rights cases brought before the European Court of Human Rights in the late-1980s and early-1990s,[24] the lack of a specific statutory basis for Britain's Security Service (MI5) was highlighted.[25] The existing administrative charter – the Maxwell-Fyfe Directive of 1952[26] – was deemed an insufficient authority since it did not have the force of law and its contents were not legally binding or enforceable. As a result of the ruling, the UK passed the Security Service Act 1989 which placed the Security Service on a statutory basis. This was followed by the Intelligence Services Act 1994, which placed the UK's other two main intelligence agencies – the Secret Intelligence Service and the Government Communications Headquarters – on a legislative footing.

Structure of the UK intelligence community

The **Secret Intelligence Service** (SIS, sometimes referred to as MI6), with its origins in the Secret Service Bureau at the turn of the 20th Century, was established as a separate foreign intelligence entity in 1922 and is the UK's primary covert foreign HUMINT collection service. The principal role of SIS is the production of secret intelligence on issues concerning the UK's interests in the fields of security, defence, foreign and economic policies, in accordance with requirements established by the Joint Intelligence Committee and approved by Ministers. SIS uses human and technical sources to meet these requirements, as well as engaging in liaison with a wide range of foreign intelligence and security services.[27]

[24] Such as the case of *Herman and Hewitt v UK (1992).*

[25] The complaints were specifically with regard to surveillance and file keeping contrary to Article 8 of the ECHR on the right to privacy. Additionally, the Maxwell-Fyfe Directive was couched in language, which failed to indicate with sufficient certainty the scope and the manner of the exercise of discretion, by the authorities in the carrying out of secret surveillance activities.

[26] This Directive – the basic administrative Charter governing the Security Service's work – was named after the Home Secretary of the time. It emphasised the role of the Service in the 'Defence of the Realm' and its duty to behave non-politically; it made the Service responsible to the Home Secretary and gave its Director-General a right of access to the Prime Minister. The Security Service Act 1989 subsequently made no change to these constitutional arrangements, leaving the Service accountable only to Ministers and not to Parliament.

[27] *National Intelligence Machinery*, 2nd ed (London: The Stationery Office, 2001).

The **Security Service** (or MI5) originated in 1909 as the internal arm of the Secret Service Bureau. As the UK's domestic security intelligence agency, the Service's purpose is to protect against substantial, covert threats, including primarily terrorism, espionage and the proliferation of weapons of mass destruction. Most recently, following the passing of the Security Service Act 1996, its role has been expanded to provide support to law enforcement agencies in fighting serious crime.[28] A 2005 declaration will now see its authority for all national security intelligence in Britain extended to include Northern Ireland by 2007.[29]

Government Communications Headquarters (GCHQ) is the UK's SIGINT collection and information assurance agency, based in Cheltenham – although interception operations are run from sites in both the UK and overseas. GCHQ also works closely with a number of foreign intelligence and security services. The choice of what to intercept and report to Government Departments and Military Commands is, as for SIS, based on requirements established by the Joint Intelligence Committee and approved by Ministers.[30]

The **Defence Intelligence Staff** (DIS) is not an agency in its own right; rather it forms part of the Ministry of Defence's central staffs. As its name suggests, it is primarily concerned with providing intelligence to the Ministry of Defence and Armed Forces on the capabilities of foreign armed forces. The DIS's task is to analyse information, from both overt and covert sources, and provide intelligence assessments, advice and strategic warning to the Joint Intelligence Committee, the MOD, Military Commands and deployed forces.[31]

The **Joint Intelligence Committee** (JIC), created in 1939, is part of the Cabinet Office, under the authority of the Secretary of the Cabinet. It is responsible for providing Ministers and senior officials with regular intelligence assessment on a range of issues of immediate and long-term importance to national interests, primarily in the fields of security, defence and foreign affairs. The JIC also brings together the Agencies and their main customer Departments and officials from the Cabinet Office, to establish and prioritise the UK's intelligence requirements that are then subject to Ministerial approval. The JIC periodically scrutinises the performance of the Agencies in meeting these requirements.[32]

Legislation

The first non-statutory mandate for MI5 was written in 1945 but was never published; this was superseded in 1952 by a Home Office Directive (the Maxwell-Fyfe Directive) which described the Security Service's tasks as the 'Defence of the Realm' from espionage, sabotage and subversion. This was left largely unchanged until the **Security Service Act 1989** which defined its role as: '*the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means*'.[33]

---

[28] *National Intelligence Machinery*, 2nd ed.

[29] Northern Ireland Office, "Statement on national security intelligence work" (24 February 2005): www.nio.gov.uk/media-detail.htm?newsID=10949.

[30] *National Intelligence Machinery*, 2nd ed.

[31] *National Intelligence Machinery*, 2nd ed.

[32] *National Intelligence Machinery*, 2nd ed.

[33] *Security Service Act* s. 1(2). Gill points out that the requirement for this legislation was as a result of (subsequently justified) fears that the complete lack of a statutory mandate or provision for handling complaints from the public meant the UK would lose cases before the European Court brought by two former civil liberties activists over MI5's surveillance of them: Gill (2003): 270.

The UK subsequently placed SIS and GCHQ on a statutory basis with the **Intelligence Services Act 1994**. Within this Act, the role of SIS is defined as: '*a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; b) to perform other tasks relating to the actions or intentions of such persons*'.[34] GCHQ's mandate is outlined as being to '*monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted materials*'.[35] A significant omission from this Act was the lack of any detail regarding the international collaborative aspects of GCHQ's work, notably within the Quadripartite intelligence sharing alliance (including the US National Security Agency, the Canadian Communications Security Establishment, and the Australian Defence Signals Directorate). The other key provision of the 1994 Act was the creation of the Intelligence and Security Committee (ISC) with a view to satisfying parliamentary demands for some form of legislative accountability (see below)

It is worth noting that the Joint Intelligence Committee and the Defence Intelligence Staff both lie outside the statutory boundary created by the above legislation.

Executive control and oversight

The legislation outlined above deals with ministerial responsibility for the three agencies (the DIS is not covered by statute), with overall responsibility resting with the Prime Minister. Indeed, the 1989 and 1994 Acts made provisions unique in UK legislation in that they grant the heads of the agencies direct access to the Prime Minister, reflecting that the agencies are not conventional government departments.[36] Although the agencies' heads have day-to-day responsibility, they remain responsible to individual ministers: the Security Service is responsible to the Home Secretary, whilst the Chief of the SIS and the Director of GCHQ are responsible to the Foreign Secretary. Whilst the majority of the services' operational activities are dealt with by their respective heads, the Regulation of Investigatory Powers Act (RIPA) 2000 requires explicit ministerial approval (in the form of a warrant) for the interception of communications in the UK.

Judicial oversight

In addition to placing the Security Service on a legal basis, the 1989 Act also made provisions for the creation of a Commissioner and Tribunal. The Tribunal, composed of three lawyers, was to receive complaints from members of the public, involving the Commissioner if the complaint involved an 'interference with property' which would require a Ministerial warrant. The Commissioner would then examine the granting of a warrant and decide if the Minister's decision was 'reasonable'. The provisions in the 1989 Act were expanded upon in the Intelligence Services Act 1994 and in RIPA 2000. All three services are now covered by judicial commissioners; an Intelligence Commissioner who is responsible for reviewing and reporting upon the issue and authorisation of ministerial warrants for operations by the Agencies; and the Interception Commissioner who reviews the issue and authorisation of warrants to intercept mail and telecommunications. The output from this process is the Commissioners' annual reports to the Prime Minister which are reviewed for sensitive information and submitted to Parliament.[37] There is also the Investigatory Powers Tribunal, established to investigate public complaints

[34] *Intelligence Services Act* 1994 s. 1(1).
[35] *Intelligence Services Act* 1994 s. 3(1)(a).
[36] Leigh (2003): 7.
[37] Gill (2003): 283.

against the agencies or interceptions. Since its creation in 1989, the Tribunal had - by 2003 - received 200 complaints, none of which were upheld.

Parliamentary oversight

The Intelligence and Security Committee (ISC), created under the Intelligence Services Act 1994, is unusual in UK parliamentary terms. It was created by statute (whereas all other Parliamentary Select Committees are not); its nine members are drawn from both the House of Lords and the House of Commons, and are appointed by the Prime Minister (whereas the membership of other Committees is approved by Parliament); and it submits its reports to the Prime Minister, who then submits them to Parliament.[38]

The ISC is not, therefore a Parliamentary Select Committee – although in many practical aspects it operates like one. Its remit is to examine the expenditure, administration and policy of the three services, but not operations. There are some limits to the ISC's powers; it can only request information and does not have the power to demand specific documentation, even those relating to policy, administration or expenditure of the agencies; it has no statutory right to interview agency staff lower that the director of a service. Agency heads may also refuse to disclose information on the grounds it is sensitive – although this is discretionary. In keeping with parliamentary norms, although members of the ISC are not security vetted, they are subject to the Official Secrets Act and, as such, operate within the 'ring of secrecy'.

Conclusions

The UK placed its domestic and, unusually, its foreign and SIGINT intelligence agencies on a statutory footing as a response to an external impediment on their operation (i.e. the European Court of Human Rights). That this was the key concern is evidenced by the fact that the legislation is generally vague regarding the limits of the agencies' activities, apart from in relation to the issues of warrants for surveillance and interception. It has established a fragmented system of accountability whereby not all aspects of the intelligence machinery are subject to effective external oversight, and the oversight functions (such as complaints handling, review of warrants and efficiency of the services) are separated between different bodies.

Canada

Challenges

Prior to 1984, Canadian law made no distinction between politically-motivated and ordinary crime. Consequently, the federal Royal Canadian Mounted Police (RCMP) was responsible for defending Canada's national security from an internal perspective (in conjunction with regional police forces). Between 1910 and 1983, the RCMP's Security Service led on national security and gradually evolved into a separate and increasingly powerful entity.

As it evolved, the RCMP Security Service became increasingly subject to accusations that it was abusing its growing powers; thus, intelligence activities became an issue of public concern. Between 1966 and 1981, there were six major commissions of inquiry into the RCMP Security Service's activities:

[38] Leigh (2003): 12. The Prime Minister has the right – under the legislation – to edit these reports for sensitive information which will not be provided to Parliament. The Committee may also, and does, provide *ad hoc* reports to the Prime Minister from time to time.

- the Wells Commission (1966)[39] which centred on the firing of a Vancouver postal worker as a suspected Soviet spy, the cause of the first public outcry.
- the Spence Commission (1966)[40] which centred on the implication that two former cabinets ministers were maintaining a relationship with a woman believed to have connections to Soviet espionage.
- the Mackenzie Commission (1969):[41] this Commission made the first formal recommendation for the creation of a formal accountability mechanism for the RCMP Security Service. It also recommended that the Security Service should be detached from the RCMP. Neither recommendation was implemented at the time.
- the Keable Commission (1981)[42] was established by the new *Parti Québécois* provincial government in 1976 to examine the activities of the RCMP in countering the Quebec independence movement.
- the McDonald Commission (1981)[43] which was established following revelations surrounding the activities of the RCMP Security Service in Quebec (alleged extra-legal surveillance of Quebec separatists involved in democratic and law-abiding activities).

The McDonald Commission recommended a complex new institutional architecture to ensure an unprecedented level of accountability over the RCMP Security Service, through both internal controls and external review. One of its key recommendations was the separation and civilianisation of the Security Service – repeating the findings of the Mackenzie Commission; it was also highly critical of the lack of a legislative mandate for the organization. The Canadian government's response to the findings of the McDonald Commission was to introduce the Canadian Security Intelligence Service Act 1984 (CSIS Act).

Structures and legislation

The CSIS Act provided for the creation of the Canadian Security Intelligence Service (CSIS). Its mandate was to collect, analyse and retain information and intelligence 'respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada',[44] as well as to provide threat assessments to the Government of Canada and, by approval, to the provinces or to foreign governments or international organisations.

Different to many other countries, Canada defines its national security – within the CSIS Act – not so much by its qualities as by the threat to it; these include:

- espionage or sabotage directed against or detrimental to Canada's interests
- foreign influenced activities within or related to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person
- activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state

---

[39] *Commission of Inquiry into complaints made by George Victor Spencer*, The Hon. Mr Justice Dalton Wells, Commission July 1966 – the inquiry centred on the firing of a Vancouver postal worker as a suspected Soviet spy which caused a public outcry.

[40] *Commission of Inquiry into matters relating to one Gerda Munsinger*, The Hon. Mr Justice Wishart Spence, Commissioner, September 1966.

[41] *Report of the Royal Commission on Security* (1969).

[42] *Rapport de la Commission d'enquete sur les operations policieres en territoire Quebecois*, Government of Quebec, Ministry of Justice, 1981.

[43] *Commission of Inquiry Concerning Certain Activities of the RCMP* (Ottawa: Supply & Services, Canada, 1980).

[44] *CSIS Act* 1984 s12-13.

- activities directed toward undermining by unlawful covert acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence, of the constitutionally established system of government in Canada.

The Act, therefore, provides the CSIS with a relatively clear set of defined activities it may legitimately target.

Internal control and accountability

One of the key criticisms of the McDonald Commission's key concerns was the lack of **clear ministerial responsibility** for the activities of the Security Service. Therefore, the Act placed the Director of CSIS under the authority of the Solicitor-General. The Act also states that the Minister must personally approve all CSIS judicial warrants; all CSIS arrangements with other federal agencies, departments, local authorities and foreign governments; and the nature of assistance provided by CSIS in the collection of foreign intelligence. The Minister is ultimately accountable to Parliament.

There are two important internal CSIS committees which contribute to the operational control of CSIS. The first is the Target Approval and Review Committee (TARC), comprised of senior CSIS officers and representatives from the Ministries of Justice and the Office of the Solicitor-General. TARC authorises the targeting of specific individuals for specified periods of time and approves the use of various investigative techniques which do not require judicial warrants. The second is the Warrant Review Committee (WRC), which reviews CSIS warrant applications and is chaired by the Director of CSIS. It has been suggested that this is not an effective control mechanism, as the number of warrants requested each year has been estimated to be in excess of 200. As such, it is unlikely the Director of CSIS has sufficient time to scrutinise these applications rigorously.[45]

The Inspector-General of CSIS

Section 30 of the CSIS Act established the post of the Inspector-General of CSIS (IG). It requires the IG to monitor the compliance of the Service with operational policies, and to review both the operational activities and the submission of 'certificates' to ministers. Subsection 33(1) obliges the Director of CSIS to submit a report to the Minister at least annually (and upon specific demand) on the activities of CSIS; a copy of these reports is given to the IG who must inform the Minister in written certificates of the extent of his satisfaction with reports, with particular regard to: a) whether anything done by CSIS was not authorised by the CSIS Act, b) if the Service contravened any directions issued by the Minister, and c) if any action involved any unreasonable or unnecessary exercise of powers of CSIS.

In order to carry out its role, the IG has access to all relevant (i.e. classified) CSIS information and may interview its staff, but does not have access to Cabinet documents. Whilst the IG conducts internal reviews for the Minister only and no IG document has ever been released into the public domain, it does facilitate some indirect public accountability through the Security Intelligence Review Committee (SIRC – see below), which receives a copy of the IG's certificates and can direct the IG to undertake a review, which would then be publicly disclosed through the Committee.

[45] Brodeur (2003): 236.

Judicial and parliamentary oversight

Sections 21 to 28 of the CSIS Act lay out the mechanism whereby the Service applies for **judicial warrants** authorising technical surveillance actions. However, there are significant loopholes in the CSIS Act in that a single warrant can authorise the use of several devices against multiple targets (despite elaborate pre-screening processes such as TARC and WRC). Recommendations by the SIRC to close these loopholes have been rejected by the government.

The **Security Intelligence Review Committee** (SIRC) was created by the CSIS Act to oversee CSIS following the recommendations of the McDonald Report. The Committee consists of a Chair plus between two and four other persons who are all Privy Councillors not serving in Parliament. The Prime Minister appoints its members after consultation with government and all opposition parties.[46] The SIRC also has a small staff (16), and both SIRC members and staff are held to a strict code of confidentiality regarding information disclosed to it. The Committee acts in two ways: it reviews the performance of the Service to ensure all activities are carried out in accordance with the CSIS Act and according to the rule of law; and it receives complaints against the Service from members of the public. SIRC can react to an external complaint or alternatively demand an inquiry on its own initiative (as well as directing the IG or the Service to conduct investigations).

The Committee's powers of investigation are significant; it has access to any information under the control of CSIS or the IG, and it can require from any CSIS personnel verbal explanations necessary for the performance of its role. However, as with the IG, SIRC is barred from access to Cabinet documents. SIRC submits an annual report to the Solicitor General who must lay it before Parliament in 15 days; the Committee has complete control over the annual report's content and publication; however, for special reports the Solicitor General decides what part of report is made public.

Whilst the CSIS Act created a relatively demanding set of control and accountability mechanisms for CSIS, it did not consider the position of Canada's signals intelligence agency, the **Communications Security Establishment** (CSE). Created in 1941 and taking its current name in 1975, the CSE's existence was not publicly acknowledged until 1983 (during the parliamentary debate on the bill that became the CSIS Act). The five-year review called for in the *CSIS Act* was completed by a Special Committee of the House of Commons under Chairman Blaine Thacker. The Committee's report, *In Flux But Not In Crisis*, completed in September of 1990, declared that CSIS and the Act were essentially on course, but provided recommendations for improvements nonetheless. It stated that the CSE 'clearly has the capacity to invade the privacy of Canadian's in a variety of ways. It was established by Order in Council, not by statute, and to all intents and purposes is unaccountable', and recommended that the CSE be established by mandate and that SIRC be appointed as the oversight body for CSE's activities. The CSE was subsequently give a loose statutory mandate in part of the National Defence Act 1985, which established the role of the CSE Commissioner to provide a point of review for its activities.

In October 2001, the Canadian Government passed enabling legislation for the CSE, as part of a package of anti-terrorist measures. The Anti-Terrorism Act 2001 appoints a Commissioner for the CSE who will oversee its activities to ensure they comply with the law, and inform the

[46] One unforeseen consequence of the *CSIS Act* stipulation that SIRC members must be Privy Councillors and cannot be MPs or Senators during tenure came to light following the 1993 election where the majority of opposition MPs were new and therefore not Privy Councillors. As a result many of the new opposition parties were not represented on SIRC.

Minister of Defence and Attorney General of any breaches of law; the Commissioner will also investigate complaints. However, there remains little public accountability and the legislation is problematic in that it fragments the accountability structure of the intelligence services rather than establishing one body with comprehensive oversight of all agencies.

In 2004, all entities concerned with national security in the Canadian Government – including CSIS, the Office of the Inspector-General, SIRC, the RCMP, and the Solicitor General of Canada – who has responsibility for all national security and counter-terrorism activities – became part of the new Department of Public Safety and Emergency Preparedness Canada (PSEPC) established by the Canadian Government to centralise Canada's approach to national security and contingencies. Finally, the Government also proposed – in the same year – the establishment of a "National Security Committee of Parliamentarians"; at present, this committee and its potential mandate remains under discussion – however, members of the existing Sub-Committee on National Security in Canada's Parliament have expressed the desire to include elements of oversight and accountability for Canada's security and intelligence community in their eventual mandate.[47]

South Africa

Challenges

South Africa presents one of the best case-studies of a country in transition from an authoritarian regime to a universal democratic state; as such, it presents a wider range of issues, challenges and concerns than countries such as the UK or Canada which – although fully democratic states – required enhancements to existing legislative and juridical frameworks to ensure oversight and accountability for their security and intelligence services.

The security forces of South Africa were key actors in the repression that characterised the apartheid system. During the period 1978 to 1990, South Africa was in effect a security state. While nominal political authority and power rested with the elected Cabinet Ministers, the State Security Council (SSC) was the true centre of power; executive/cabinet responsibility for intelligence and its three main agencies – the South African Police Security Branch, the Directorate of Military Intelligence (DMI) and the Bureau of State Security (BOSS, later the National Intelligence Service or NIS) – was governed by the SSC through several pieces of legislation (most significantly the 1972 Security Intelligence and State Security Council Act), with DMI dominating all.

Despite this, the intelligence services of both the apartheid state and the African National Congress (ANC) played a significant role in the termination of the conflict. President F W de Klerk used the NIS to oversee the negotiation process with the ANC, resulting in the new political order that led to the Transitional Executive Council (TEC) and – following the April 1994 elections – the Government of National Unity (GNU). Within the TEC, a Sub-Council on Intelligence formulated new polices and legislation to reform the intelligence and security services. It noted that 'prior to the election of a democratic government, security policy was formulated by a minority government. Its ability to detail what was in the national interest was therefore flawed. Moreover, since the minority government was faced with a struggle for

---

[47] Department of Public Safety and Emergency Preparedness Canada, *A National Security Committee of Parliamentarians: A Consultation Paper to Help Inform the Creation of a Committee of Parliamentarians to Review National Security* (2004): www.psepc-sppcc.gc.ca/publications/national_security/nat_sec_cmte_e.asp.

liberation, this issue dominated the question of security and, consequently, the activities of the statuary instruments that served it…the role of the state's security apparatus was over-accentuated with virtually no institutional checks and balances', and that the new government believed that 'reshaping and transforming intelligence in South Africa is not only a matter of organisational restructuring. It should start with clarifying the philosophy and redefining the mission of intelligence in order to establish a new culture of intelligence'.[48]

Structures and legislation

In developing the new structure and ethos for its intelligence services, the new government set about examining a number of comparative examples from Western intelligence communities (Canada, Australia, the UK and the US), with particular emphasis on oversight and accountability structures. As a result, the Canadian and Australian models were seen as the most favourable examples – particularly regarding oversight and accountability. A new structure was subsequently developed for the South African intelligence function.

The agencies

The 1994 White Paper defined the role of the new **National Intelligence Agency** (NIA) as being to 'conduct security intelligence within the borders of the Republic of South Africa in order to protect the constitution' with an overall focus being 'to ensure the security and stability of the State and the safety and well-being of its citizens'.[49] It was established in January 1995 under section 3(1) of the Intelligence Services Act (Act 38 of 1994). The new NIA absorbed members of the NIS, ANC Intelligence and any other members of any intelligence service either attached to a political organisation or operating in the independent homelands or self-governing territories.

At the same time, the foreign intelligence-gathering department of the NIS was established separately as the **South African Secret Service** (SASS) also under section 3(1) of the Intelligence Services Act, with its mandate further defined in section 2(2) of the National Strategic Intelligence Act (Act 39 of 1994). SASS has a complimentary role to the NIA, to 'conduct intelligence in relation to external threats, opportunities, and other issues that may effect the Republic of South Africa, with the aim of promoting the national security and the interests of the country and its citizens'.[50] It was hoped that dividing the operational mandates of the old National Intelligence Service between its foreign and domestic roles would 'promote greater focusing, effectiveness, professionalism and expertise in the specialised fields of domestic and foreign intelligence'.[51]

Within the new South African National Defence Force (SANDF), formed in April 1994 following the national election, the **Intelligence Division** was greatly downsized and brought under civilian oversight and control. It included former members of DMI, ANC Military Intelligence, and personnel from the intelligence components of the defence forces of the independent homelands or self-governing territories. Its operational mandate is to 'gather, correlate, evaluate and use foreign military intelligence, and supply foreign military intelligence to [the National Intelligence Co-ordinating Committee]...gather correlate, evaluate and use domestic military intelligence excluding covert collection….and institute counter-intelligence measures within the [SANDF].

---

[48] Republic of South Africa, *White Paper on Intelligence* (October 1994): 2-3.
[49] Ibid, 12.
[50] Ibid, 12.
[51] Ibid, 12-13.

In 2002, a new signals intelligence organisation (**Comsec**) was established under the Electronic Communications Security (Pty) Act (Act 68 of 2002) which provided 'for the establishment of a company that will provide electronic communications security products and services to organs of the state'.

Oversight and accountability actors

These new agencies and organisations are overseen by two key committees: the **Cabinet Committee on Security and Intelligence** (CCSI) which directs security policy, and the **National Intelligence Co-ordinating Committee** (NICOC) which oversees the co-ordination of the Services and investigates any actions which contravened their mandates. In addition, the civilian services are directly responsible to the Office of the State President; in the case of SANDF intelligence, responsibility flows through the SANDF Chief of Staff (Intelligence) and the Defence Secretary in consultation with the Minister of Defence to the President.

Within Parliament, the **Joint Standing Committee on Intelligence** (JSCI) was established in September 1995 to exercise legislative oversight of the intelligence services. The JSCI is similar in function to the Canadian Security Intelligence Review Committee. Originally composed of 18 members appointed by the President, proportionally representative to the seating of various the parties in Parliament, subsequent legislation led to a change in the numbers and composition of the committee to be more proportionally representative of Parliament and required members to be security cleared by the NIA.[52] The Committee's remit covers not only NIA and SASS, but also SANDF Intelligence Division; the Committee reports directly to the President and through him to Parliament. It has a broad mandate, and has access to any and all information it may require in its investigations and duties (although the Services may withhold any information which may identify sources or those involved in intelligence or counter-intelligence activities).[53] The Committee's mandate was further widened by the Intelligence Services Control Amendment Act 2002 to include 'the administration, financial management and expenditure of the Services'.[54]

In addition to the JSCI, the Intelligence Services Control Act 1999 also further clarified the position of **Inspectors-General** for the Services (NIA, SASS, and SANDF Intelligence) to whom the Director-General of each service is accountable. The Inspectors-General are to review the activities of the intelligence services and to monitor their compliance with policy guidelines and other established mandates and principles. They have full access to documents, budgets, reports and all other classified information (including that on sources).

Problems were encountered, however, with the Inspector-General of the services. Within the first eight years of the new structures, the post had only been occupied twice briefly, with each incumbent resigning shortly after taking office. These difficulties led to a change in the legislation affecting the Inspectors-General. The Intelligence Services Control Amendment Act 1999 stated that there would now be 'one or more Inspector-General of Intelligence' rather than the previous dictate of 'for each Service an Inspector-General'. It also stipulated that the IG could be approved by 'at least two-thirds' of the members of parliament rather than the previous 'majority of at least 75 per cent'[55] – relating clearly to the failures to appoint an IG successfully. The IG's mandate

[52] Section 2 of the *Intelligence Services Control Act* 1999.
[53] This was primarily to prevent the identification of those who spied for either side prior to the 1994 elections. *Intelligence Services Control Act* 1994 s4(1)/(3) and s4(2)(a).
[54] *Intelligence Services Control Amendment Act* 2002 s2.
[55] *Intelligence Services Control Amendment Act* 1999 s5b.

was also expanded to 'receive and investigate complaints from members of the public and members of the Services on alleged maladministration, abuse of power, transgressions of the laws and policies…corruption and the improper enrichment of any person through an act or omission of any member'.[56] In order to achieve this, the IG was granted 'access to any intelligence, information or premises under the control of the service in respect of which he or she has been appointed...No access to intelligence, information or premises...may be withheld from an Inspector-General on any ground'.[57] That this revised legislation failed to address the difficulties with the IGs is evidenced by the subsequent Intelligence Services Control Amendment Act 2002 which stated that there should be only one IG of Intelligence. The IG's mandate was again expanded and the complaints mechanism from the public was strengthened. In addition, the Head of each Service was now required to report to the IG regarding 'any unlawful intelligence activity or significant intelligence failure of that Service and any corrective action that has been taken or is intended to be taken'.

Politicisation of the Intelligence Services

A series of scandals[58] involving the South African intelligence services in the mid-to-late-1990s demonstrated that, whilst the legislative framework seemed impressive on paper, it was far from thoroughly effective on the ground. Despite the 1994 Intelligence Services Act, which obliges each service's Director-General to ensure 'no action is carried out that could give rise to any reasonable suspicion that the agency or service is concerned in furthering, protecting or undermining the interests of any section of the population or any political party or organisation', it became increasingly worrying that the intelligence community was being politicised by:

- the placement of ANC loyalists in key positions within the intelligence services, as well as those within the services wishing to meet the anticipated expectations of the political leadership.
- the failure to ensure the integration of former rival intelligence personnel into the NIA and the emergence of factionalism along old opposing lines within the services.
- the development of parallel intelligence structures of political purposes due to a lack of trust in the national intelligence functions.

Conclusions

Those who sought to reform South Africa's intelligence services set themselves a very high standard in terms of quality, transparency, accountability control and oversight. Despite creating a commendable system in terms of legislation, the implementation has been poor. The intelligence services are barely independent from the executive, whilst the oversight mechanisms remain at best fragile.

Germany

Challenges

Following the Second World War and the division of Germany, the Allied occupying powers permitted the creation of West German security forces, but these were decentralised and demilitarised. However, as the tensions of the Cold War grew, it was recognised that a centralised defence and security apparatus would be required. While the Soviet-controlled Zone established

[56] *Intelligence Services Control Amendment Act* 1999 s7.
[57] *Intelligence Services Control Amendment Act* 1999 s8-9.
[58] Including accusations of services 'bugging' each other; spying on opposition parties; collusion with criminals *et cetera*.

its own intelligence services, in the West the US Central Intelligence Agency began to create a West German intelligence body in the form of Organisation Gehlen (OG) – led by Major General Reinhard Gehlen, former head of intelligence of the Eastern Front section of the German General Staff. OG began its existence operating primarily as a HUMINT-gathering organisation, operating in Soviet-occupied Eastern Europe. OG's legacy was highly controversial as it later emerged it had employed hundreds of former SS and Wehrmacht personnel, many specially released from Allied prisoner of war camps. Although it mounted a number of operations in the Soviet Zone, and comprised several thousand personnel, by the mid-1950s it had become clear that OG had been heavily infiltrated by Soviet intelligence, with dozens of operations and hundreds of agents compromised. Consequently, OG was transformed into the Bundesnachrichtendienst (BND – the Federal Intelligence Service) on 1 April 1956, with Gehlen heading it until 1968. In tandem, with the creation of the Federal Republic of West Germany, came the establishment of agencies to perform domestic counter-intelligence and their counterparts in the armed forces.

Throughout the Cold War, the federal German intelligence services suffered from a low level of public legitimacy and were frequently in the media spotlight. Germany's Basic Law (Constitution) guaranteeing freedom of the press allowed the media much greater scope to investigate and publish information about the intelligence services, than would be found – for example – in the UK with the restrictions imposed by its Official Secrets Act. In the post-Cold War environment, this poor public perception, combined with concerns over effectiveness or even the need for intelligence services to exist, forced the agencies to move rapidly to realign with the new situation. The system of oversight and accountability has evolved alongside the German intelligence community since 1950.

Structure of the post-war German intelligence community

Dating from the early years of the Federal Republic, the German intelligence community comprised three main services[59]:

- The **Federal Intelligence Service** (Bundesnachrichtendienst - BND): established in April 1956 (from the Organisation Gehlen), the BND is responsible for the collection and analysis of information from a variety of covert sources from outside of Germany's borders; it is also Germany's primary SIGINT body. The BND is responsible to the Federal Minister in the Office of the Federal Chancellor. It was not placed on a statutory footing until the passing of the **Federal Intelligence Service Law 1990**.
- The **Office for the Protection of the Constitution** (Bundesamt fur Verfassungsschutz – BfV): created in 1950 to conduct domestic counter-intelligence in defence of the German Basic Law (Constitution),[60] the BfV also undertakes monitoring of a wide range of groups (terrorist, political extremist and racist) active in Germany and believed to have the potential to pose a violent threat to the democratic order of the state. The agency is responsible to the Federal Ministry of Internal Affairs.
- The **Military Counter-intelligence Branch** (Militaerischer Abschirmdienst – MAD): established at the same time as the Bundeswehr (German Federal Armed Forces) in the mid-1950s, MAD is responsible for military counter-espionage and internal security within the armed forces; it is barred from conducting actions relating to civilians. MAD is responsible to the Federal Ministry of Defence.

[59] Shapiro, "Parliament, Media and the Control of Intelligence Services in Germany" (2003): 295

[60] German Basic Law Article 87 (1) provides the constitutional basis for the creation of the BfV; its position at both federal and state (Lander) levels was articulated in the *Federal Office for the Protection of the Constitution Act* 1950.

Executive control

Legally-binding security policy decisions are taken at the executive level by the Chancellor in consultation with his cabinet and the Federal Security Council (*Bundessicherheitsrat*), as well as within the Ministerial responsibilities by the supreme federal authorities, and at the legislative level by the Bundestag and Bundesrat. Whilst ministerial responsibility for each service rests with the relevant Federal Minister, there is also an Intelligence Co-ordinator of Cabinet rank responsible for overseeing the co-ordination and co-operation of the three Services. This Minister is in turn supported by Department VI of the Office of the Federal Chancellor which co-ordinates the activities of the German intelligence services in relation to parliamentary oversight and control, as well as the internal administrative control of the BND. The Co-ordinator has a statutory right of access to any information from the intelligence services relating to operations, budgets structures and staffing; he also has a right of direct access to the heads of the Services. Ad-hoc interagency committees are also used extensively as the preferred tool for such consultations within the Cabinet and the Chancellery; in addition, coalition politics play significant roles in many decision-making processes.

In addition to the Federal-level activities are those taking place at the State (*Länder*) level. Recent initiatives have seen Bavaria has strengthened the *Landesamt für Verfassungsschutz* (State Intelligence Service for the Protection of the Constitution) and established the *Innovationszentrum der Bayrischen Polizei* (Innovation Centre of the Bavarian Police, Centre for Academics and Police). Such State-level activities have their own concerns and challenges.

Parliamentary oversight

Created by the **Law over the Parliamentary Control of Intelligence Activities 1978**, the **Parliamentary Control Commission** (PKG) is the main organ of parliamentary oversight in Germany examining political and operational issues. The PKG consists of nine members of the Bundestag (the lower chamber) who, following election by their fellow assembly members, sit for the duration of each new parliament. The Chair of the PKG rotates on a six-monthly basis between members of the opposition and the governing coalition. Under its enabling legislation, the PKG is entitled to be informed by the executive of the general activities of the Services and on specific operations of political significance (i.e. those that, if discovered, may damage Germany's interests). The PKG receives the information it requires for its work through the Office of the Federal Chancellor and has secure facilities for storage and access to classified information. The Commission has the right to ask for specific information from the intelligence services and to interview individual officers (with the exceptions where this information may compromise sources or has been provided by foreign intelligence services). The proceedings of the PKG are held in closed session, and members are under a legal obligation not to reveal any information gleaned via their participation – this obligation remains once they are no longer members. However, the PKG does hold a significant power in that it can, by a two-thirds majority, vote to waive this secrecy in specific cases.

Article 10 of the 'Basic Law' guarantees it citizens the freedom from interference in their communications.[61] This measure alone was demonstrated to be inadequate when, in 1963, became apparent that the BfV had assisted Allied intelligence agencies in the widespread

[61] Article 10 on "Privacy of correspondence, posts and telecommunications" states "(1) The privacy of correspondence, posts and telecommunications shall be inviolable; (2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature".

interception of German citizens' telephone and postal communications.[62] These revelations prompted the introduction of the **State of Emergency Law 1968** (also refereed to as the G-10 Law) which passed responsibility for domestic communications interception to the BND. The control of these powers was then passed to the Office of the Federal Chancellor in 1971, which tasks the BND to undertake technical interceptions with the oversight of the Parliamentary 'G-10 Committee' and 'G-10 Commission'.

The **G-10 Committee** is made up of nine members of the Bundestag, meeting every six months to examine the guidelines governing interception activities. It does not oversee or regulate the use of technical interceptions in individual cases, rather it makes policy decisions as to what collection methods are appropriate to different types of operations, while regulating which communications media the BND can monitor. The **G-10 Commission** comprises four legal experts (normally lawyers or retired civil servants) who, while not members of the Bundestag, are nominated by the political party leaderships and formally appointed by the G10 Committee. The Commission meets once a month and examines the legality of ongoing interception operations; if the Commission believes that an operation infringes any law or the evidence is too weak to justify a warrant, it has the right to suspend an operation. In the case of wider monitoring of communications (rather than individual targets of interception), the Commission supervises the detailed list of key-words used to filter collected interception material. In effect, the Commission fulfils the role of a judicial oversight body, which is otherwise lacking in this area of intelligence activity.

The final Bundestag oversight body is the '**Committee of Confidants**', which examines the budgets of the intelligence agencies, and approves them to the Bundestag. It is made up of nine parliamentarians, all members of the Bundestag budgetary committee. Elected by the assembly, they hold the highest level of security clearance. The intelligence services are required to submit to the Committee detailed financial statements and budgetary projections, including both expenditure and income (from normal and clandestine sources). This Committee also examines the financial audits carried out by the Federal Audit Office.

The Bundestag has also created *ad hoc* **Parliamentary Investigative Committees** to examine publicly-disclosed intelligence failures and controversies. Such committees (not limited to intelligence matters) have the ability to summon witnesses and request documentation. Such committees investigated the 1963 revelations of BfV interception of domestic communications and following the 1974 arrest of an East German spy in the office of Chancellor Willy Brandt. These *ad hoc* committees have not been well regarded by the German intelligence community, as they have tended towards sensationalism and the Services have been reluctant to provide witnesses or information to them. They are perceived as platforms for opposition politicians to gain public exposure but have on occasion discovered evidence of malpractice and abuses.

Conclusion

In recent years, Germany has moved to establish more robust approaches to security and intelligence. For example, a new Anti-terrorism Law (*Terrorismusbekämpfungsgesetz*) amending numerous security statutes was passed in January 2002; among other measures, the law has now been modified to ban (private) associations – of a religious or other nature – when their objectives or activities are directed towards the perpetration of criminal acts, if they are unconstitutional, or if they contradict the ideals of international understanding. At the same time, the German

[62] Schmidt-Eenboom E, "The Bundesnachrichtendienst, the Bundeswehr and Sigint in the Cold War and After", *Intelligence and National Security*, Volume 16, Number 1 (Spring 2001):163.

government has consistently strengthened security agencies such as the Federal Office of Criminal Investigation (BKA), not only by increasing the investment for expanding human resources but also by financing modern investigation technologies. In all of this, Germany must ensure that the comprehensive democratic principles and freedoms established by its Basic Law are not undermined in the interests of a security state.

The Czech Republic[63]

Challenges

Czechoslovakia generally – and the Czech Republic specifically – presents yet a different case to many of the others, given its history as a key player of the Soviet Bloc and its previous inter-locking relationships with the Soviet KGB and the intelligence services of other Soviet Bloc states. Having seen the non-violent overthrow – the Velvet Revolution of 1989 – of the Communist state, Czechoslovakia was keenly interested in establishing the same norms as Western countries in anticipation of becoming a future partner of the West.

In the first years of security intelligence reform in Czechoslovakia, the challenge was twofold – purification and prestige:

- purging intelligence institutions of the old regimes personnel
- a new bureau of domestic intelligence had to earn and receive the respect of the public, partly in order to attract talented recruits

The attempt to achieve this in Czechoslovakia immediately following the Velvet Revolution foundered badly. Attempts to place the old service, the StB, under the control of a non-communist Minister failed, partly due to the opposition's timidity in negotiations with the old regime. The result was that effective control fell to StB General Lorenc, who ordered the destruction of a third of its files relating to its 52,000 ongoing operations. When a non-communist Minister was installed in late-December 1989, his most pressing task was to dismantle the StB to prevent it posing a danger to the new regime; however, this was tempered by the need to retain the skills of existing StB personnel until new recruits had been trained, as well as to maintain the new government's commitment to adhere to the rule of law. A systematic vetting process was undertaken of all StB officers, allowing those uncompromised by involvement in political oppression to remain in-post. By 15 February 1990, the StB had ceased to exist – its personnel were then screened by a series of citizens committees and screening committees; However, these committees were poorly resourced and had incomplete access to documentation, so much so that by August 1990, the committees were only able to assess 14 per cent of the vetted StB members, police officer and soldiers as being unfit for continued employment.

New structures

There was broad consensus among the new political leadership that the new intelligence structures had to be based on statute and operate under parliamentary oversight.[64] However,

---

[63] This case study draws extensively on Kieran Williams, "Czechoslovakia 1990-2" and "The Czech Republic since 1993" in Williams, Kieran and Deletant, Dennis (eds). *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia And Romania* (Basingstoke: Palgrave, 2001).

public pressure for a root and branch restructuring of the security sector caused the government to create new institutions without a legislative basis. In the event, two key (among other) agencies were created to replace the old StB's functions.

The first was the **Bureau for the Protection of the Constitution and Democracy** which employed some 6,000 personnel and was structured along the same lines as the old StB; indeed, with a large proportion of its staff being former StB officers, the perpetuation of the old ways of thinking manifested itself in the creation of two sections initially devoted to targeting West Germany and other Western states (contrary to the new government's stated foreign policy goals). The lack of a clearly defined mandate and debates about the extent of its powers led to the dissolving of the agency in late-1990 and its replacement by the Federal Security Information Service, comprising only some 1000 staff – of which roughly only 10 per cent were retained.

The second body, the **Bureau for Foreign Contacts and Information**, was largely unreformed; it retained both 85 per cent of its Communist predecessor's staff and its incongruous position within the First Directorate of the Interior Ministry. It too maintained its forerunner's focus on targeting the West.[65]

New legislation

Despite the early recognition of the need to legislate for the intelligence services, the government had failed to prepare or propose a new bill. The frustration arising from this lack of progress caused a group of four parliamentarians to draft a Bill creating a new Federal Security Information Service (FBIS), which would be separated from the Interior Ministry. Despite the good intentions behind its origins, the Bill was flawed and suffered from a large number of amendments.

The legislation envisaged the FBIS as an agency for the acquisition, centralisation and analysis of information pertaining to the protection of the constitutional order and the state's economic interests, for countering –espionage, and for exposing terrorism. However, this mandate was weakened by the failure to define either state or economic security – itself a result of the lack of an articulated security doctrine for the state. The new service's relationship with the police was undefined and the provision that its personnel would be subject to military law blurred its status as a civilian intelligence agency. Ultimately, the FBIS was to have significant powers at its disposal, as the legislation permitted a broad array of surveillance techniques to be utilised upon approval of a warrant from the Prosecutor General.

The issue of control over the FBIS was controversial – many members of the assembly felt that it was too soon in the nascent democracy's existence to allow the interior ministry full control over the service; thus, the Bill attempted to create a separation of powers between the executive and parliament. The result was a muddle whereby no single official, elected or otherwise, had overall responsibility for the FBIS. This situation was not improved by the collapse of the Czechoslovak federation, which occurred as the law was debated. While consensus existed on the need for effective parliamentary oversight, the means by which this was to be achieved was less clear. The

---

[64] Cerny O, "Czechoslovak (Czech) Intelligence after the Cold War". Paper presented at the Workshop on 'Democratic and Parliamentary Oversight of Intelligence Services' Geneva 3-5 October 2002 (Geneva Centre for the Democratic Control of the Armed Forces): =4.

[65] In 1992, the head of the service presented the Czechoslovak leadership with a list of 20 risks to state security, of which 11 related to Germany. Following a strong German diplomatic protest, the director resigned, but was immediately made the head of Czech military counter-intelligence.

Bill called for the creation of a 'special oversight organ' (ZKO), consisting of eight members, half elected by each of the parliament's two chambers. The ZKO was to have a broad mandate to monitor FBIS activity and adherence to the law, receive regular reports from the Service's director, and have access to basic documentation. Revisions made to the Bill in the Assembly removed the envisaged role of the ZKO as a complaints handling body.

Following the passage of the enabling legislation, the FBIS came into existence on 1 July 1991. The new service had some initial successes but also some significant difficulties. Chief among these were the confused lines of accountability and control. The service decried their lack of direction and a failure on the part of decision-makers to react to their products. There was no effective Cabinet-level committee for directing intelligence activity. This situation continued for several months before the creation of a security policy committee which failed to include the Ministries of the Interior and Defence, but had significant representation from the intelligence agencies themselves.

The FBIS and its accompanying structures were quickly overtaken by events with the collapse of the Czechoslovak federation and the creation, on 1 January 1993, of the new Czech Republic.

The new Czech Republic

The new state created four new intelligence services:

- the Security Information Service (BIS) for civilian counter-intelligence
- the Bureau for Foreign Contacts and Information for civilian intelligence
- Military Defensive Intelligence, the defence ministry's counter-intelligence arm
- the Intelligence Service of the General Staff, the army's intelligence branch

The first few years of the new country – and of the government of its first Prime Minister Vaclav Klaus – were difficult for the intelligence community. At the first meeting of the new Council for Co-ordination of the Intelligence Services, Klaus reportedly told the assembled intelligence hierarchy 'If I could I would dissolve you all but I probably would not get away with it'.[66] Given this ambivalence, the development of new legislation proved to be a difficult process. As with the FBIS law in the old Czechoslovakia, the first attempt to legislate for an intelligence service (the BIS) was haphazard; the Bill was again developed by parliamentarians, hastily drafted and based on old FBIS working papers. Unsurprisingly, the resulting Bill bore a significant resemblance to the old FBIS legislation and was passed on 22 October 1992, with an agreement it would be superseded by a better bill by the end of 1993.

Oversight and control

A key failing of the new law was that there was still no clear ministerial responsibility for the BIS. The continuing indifference of the government to intelligence issues was again demonstrated by its failure to prepare the new Bill due to be introduced at the end of 1993 – with the result that the existing legislation was extended until 31 July 1994. This delay also was partly as a result of disagreements within government over the number and structure of the agencies, with the Prime Minister Klaus favouring a unified civilian intelligence/counter-intelligence agency and a single military equivalent. Others (including the foreign and interior ministers) argued for the need to maintain an externally-focused organisation under a separate mandate. The latter view prevailed, with only the two military services being merged into a single entity. The government

[66] Cerny, *op cit,* 9.

subsequently prepared a framework Bill setting out the mandates and oversight mechanisms of the one military and two civilian agencies.

The new Bill went further than before in outlining the BIS's mandate, which included targeting 'intentions and activities aimed against the democratic foundations, sovereignty and territorial integrity of the state', as well as gathering information on foreign intelligence services, threats to state security, and terrorism. In terms of control, the government gave itself sole authority to appoint and remove the BIS director, and had exclusive control over assigning tasks to the service (though the President could request tasks through the government). Further to this, the Bill stated that the government exercised oversight of the intelligence services activities, while parliament would perform only a supervisory role with regards to the rights and freedoms of citizens. Parliament would not examine expenditure, government assignment of tasks or the legality of operations, and would receive information via the government rather than the agencies themselves. Finally, BIS personnel would no longer be entitled to complain to the assembly if they were ordered to conduct illegal actions. This Bill – named the Act on the Intelligence Services of the Czech Republic (Act 153/94 S) – was finally passed by the assembly as a new 'umbrella law' in July 1994, with the proviso the government would produce a further bill to clarify parliamentary oversight – which the government failed to do.

The parliamentary ZKO committee was severely constrained by this new legislation, without access to any information regarding ongoing operations. Following the government's failure to honour its commitment, in January 1996, the Chairmen of the Defence and Security Committee and the committee for oversight of police use of technical surveillance proposed a new intelligence oversight bill. The basis of their bill was to divide responsibility between two new bodies: a five-member supervisory commission made up of parliamentarians to scrutinise the budgets and closed cases of the various agencies; and a three-member oversight body, made up of leading citizens elected by the Government, President and Senate, to oversee all the agencies and examine ongoing operations.[67] Members of the latter body were to be employed full time for at least five years, independent of the electoral cycle, and to undergo security clearances. The Bill was rejected outright by the government, which insisted that it alone had the right to oversee budgets and internal matters of the services. The proposed legislation was defeated on its first reading.

There have been two further attempts to introduce reforming legislation for the intelligence services, both originating in 1999, the combined effect of which would have been to create stronger and more direct executive control, and to establish a five-member oversight committee, supervising the civilian and military agencies. Thus far these proposals have not be passed and the existing 1994 law remains extant, subject to a number of minor amendments.

Conclusions

The Czech Republic faced a number of serious hurdles in developing and implementing effective legislation, oversight and control of the country's various intelligence services. The greatest among these was the break-up of Czechoslovakia and the impact that this had on future developments. In addition, there are indications that, at times, the government demonstrated a lack of interest in the intelligence portfolio. When it did become interested, it moved to internalise oversight away from public and parliamentary scrutiny. Part of the problem, though, was the lack of power and respect demonstrated for these parliamentary committees. These

[67] Williams, 'The Czech Republic since 1993' (2001): 98.

problems highlight some of the challenges that emerging democracies face – particularly if their final form remains fluid for some years – in creating an effective intelligence sector with robust oversight and control mechanisms.

Argentina[68]

Challenges

Prior to the restoration of parliamentary democracy in 1983, the Argentine intelligence services had been largely subordinated to the armed forces. They were heavily implicated in the human rights abuses of the 'dirty war' conducted by the military dictatorships in the 1970s. Broad political and public concern centred on the need to ensure the subordination of the various civilian and military agencies to effective civilian control and external oversight, as well as eliminating the involvement of military agencies in the domestic security sphere.

Legislation and structures

Between 1983 and 2001, a series of legislative Acts were passed with direct or indirect relation to the intelligence sector. Article 4 of the **National Defence Law No. 23554 1988** (NDL 1988) set out the distinction between national defence and internal security, and prohibited military intelligence agencies from conducting actions related to domestic political affairs.

The **Internal Security Law No. 24059 1992** (ISL 1992) laid the framework for the legal basis for the Argentinean domestic security sector, establishing a system for the planning, co-ordination, control and support of the national police effort to guarantee internal security. Relating directly to intelligence, this Act created a Directorate of Internal Intelligence, through which the Interior Minister exercises the functional direction and co-ordination of the activities of the intelligence components of the Argentine Federal Police, the National Gendarmerie and the Coast Guard.

The most significant aspect of ISL 1992 was its provision for the creation of a Joint Oversight Committee on Intelligence and Internal Security, with a remit to supervise and control all internal security and intelligence activities. This committee had significant powers: it had access to all information it deemed necessary; it could require witnesses to appear and prevent witnesses from leaving the country (both with judicial enforcement if necessary); and it could propose to the executive measures to overcome any deficiencies it discovered in the course of its work. The committee could cover the whole spectrum of internal and intelligence activity.

The 1988 National Defence Law provided for the drafting of several additional bills, including one devoted to the intelligence sector; article 47 of the Law stated that 'until the pertinent law is passed and put into force, the intelligence agencies shall hold the mission, structure and functions determined by the National Executive'. However, as a result of a lack of political consensus on these issues, placing the intelligence services of Argentina on a statutory footing was a long time in coming. During the intervening years, a flurry of private bills proposed by members of parliament indicated a continuing strong legislative interest in the issue of intelligence reform,

---

[68] This case study draws extensively on Eduardo Estevez, "Executive and Legislative Oversight of the Intelligence System in Argentina: A New Century Challenge", Conference Paper for workshop on *Making Intelligence Services Accountable*, Oslo: Geneva Centre for the Democratic Control of Armed Forces (19-20 September 2003): www.dcaf.ch/news/Intel%20Acct_Oslo%200903/Est%C3%A9vez.pdf.

but with widely varying views on the scope of congressional control and other issues. Such disagreements caused the failure of an intelligence bill in 1995. These differences were eventually overcome and a new piece of intelligence legislation was passed in November 2001.

The **National Intelligence Law no. 25520 2001** (NIL 2001) created the legal framework for the 'National Intelligence System' (NIS) which it defined as the group of functional relations of the intelligence agencies of the National State, under the direction of the Secretariat of Intelligence, for the purpose of giving assistance to decision-making in the field of foreign and domestic security of the Nation. It codified the then-extant intelligence agencies and bodies which had evolved from the pre-1983 structure. The key elements of Argentina's NIS are:

- the **Secretariat of Intelligence**: the primary intelligence agency, responsible for collecting and producing foreign and domestic intelligence, as well as counter-intelligence; the Secretariat produces all-source National Intelligence material and is also responsible for the general direction of the NIS. The Secretary of Intelligence holds Cabinet rank and is appointed by the President through consultation with the Congressional intelligence oversight committee.
- the **National Directorate of Criminal Intelligence**: a co-ordination body concerned with domestic security intelligence activities.
- the **National Directorate for Strategic Military Intelligence**: responsible for the production of military intelligence.

These top level agencies are supplemented by a number of operational elements, including the Joint Staff of the Armed Forces Intelligence branch; Army Intelligence, the Naval Intelligence Service, the Air Force Information Service and the intelligence elements of the National Gendarmerie, Coast Guard, Federal Police and the Federal Penitentiary Service.

Executive control and oversight

The NIL 2001 gives the President powers to 'determine the strategic outlines and general objectives of the national intelligence policy', as well as to convene 'an inter-ministerial council to advise on the strategic guidelines and general objectives of the national intelligence policy'. In terms of Cabinet responsibility, the Secretariat of Intelligence reports to the President; the National Directorate for Criminal Intelligence sits within the Ministry for Justice, Security and Human Rights; and the National Directorate for Strategic Military Intelligence forms part of the Ministry of Defence. The three armed services' intelligence branches report to their respective service Chief of Staff. The NIL 2001 made no provision for the creation of an Inspector General for the intelligence services.

Legal constraints and oversight

The NIL 2001 stipulates that telephone calls, mail, telegraph, facsimile or any other form of communications media, as well as any kind of private files and documentation to which the public does not have access, is considered inviolable; however, the Act allows for the interception of such communications upon application for and receipt of a judicially approved warrant. The Secretary for Intelligence must request this in writing, and a specialist unit within the Secretariat - the Directorate for Judicial Observations - carries out such approved operations.

In addition, the NIL 2001 provides a set of legal safeguards relating to information gathered in the course of intelligence activities and its disclosure. No such information can be disclosed to

any individual or entity unless expressly authorised or required by the courts. Furthermore, the agencies are subject to the provisions of the Personal Data Protection Law No. 25326 2000.

In order to address the concerns around the involvement of the intelligence services in political activity and subsequent human rights abuses prior to 1983, the NIL 2001 imposed clear standards for the political neutrality of the services. Article 4 stated that '*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, co-operative, 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 owned political parties, or influence public opinion, individuals, the media or any kind of associations whatsoever'.*[69]

Legislative oversight

The existing means of parliamentary oversight of the intelligence sector was also overhauled in the 2001 legislation. As the Joint Committee created in 1993 proved to be ineffectual in the exercise of its role, the new legislation created the Joint Committee for the Oversight of Intelligence Activities and Agencies of the National Congress. Made up of 14 Assembly members - half elected by the Chamber of Deputes and half by the Senate[70] - this Committee's remit includes the legality of intelligence activities; the policy that guides the intelligence system; the effectiveness, management and administration of the agencies; its budgets; and complaints from members of the public. The Committee is obliged to report to the Assembly and to the public at large. The Committee receives a classified 'Annual Report on Intelligence Activities' from the Secretariat of Intelligence. In addition, the agencies are required to provide all documentation the Committee requests relating to internal regulations, policy and structures, and the executive is required to provide any reports or explanations the Committee may deem necessary. Finally, the Committee is formally entitled to scrutinise the classified intelligence budget.

Conclusion

The National Intelligence Law 2001 appears to have created a strong legal framework for the Argentine intelligence sector. Whilst it marks a significant break from the past, it is too soon to be able to assess the effectiveness of this new system in practice.

[69] Article 4 of *National Intelligence Law No. 25520*.

[70] Members are not required to undergo security-vetting procedures.

7. Lessons Learned

From the above case-studies and the body of academic work in this field, it can be concluded that a number of key issues must be addressed to make intelligence and security legislation meaningful. These fall into four key areas from which lessons can be drawn:

- Intelligence Mandates
- Central Co-ordination, Oversight and Accountability
- Judicial Oversight
- Parliamentary Oversight and Accountability

In addition to these generic areas, it is also important to recognise differences between developed and developing countries when considering the implementation environment for security section reform.

Mandate

The agency or community that is being legislated for must be given a clearly-defined mandate for its activities. One aspect is the requirement to differentiate between the intelligence services and domestic law enforcement– an area which is becoming increasingly blurred by the threat from transnational actors engaged in terrorism, narcotics and organised crime. In a number of states, whilst the intelligence services are not the lead agencies in combating organised crime, they are given additional powers to assist law enforcement agencies. An example would be the UK's **Security Service Act 1996** which, in amending the Security Service Act 1989, extended the Security Service's remit to include serious and organised crime.[71]

In addition, most states that have introduced legislation have established distinct agency boundaries between domestic, foreign and military intelligence activity, as well as the types of activities undertaken. South Africa provides a clear example where the legislation clearly differentiated between the territorial demarcations of the various foreign, domestic, criminal and military intelligence arms. Argentina opted for a different approach by maintaining a single civilian agency for both domestic and foreign intelligence collection (the same is true of other states such as The Netherlands, Spain and Turkey). Conversely, the UK's Security Service Act 1989 contains detail on the process by which surveillance is to be authorised (i.e. by Ministerial warrant) and the process by which complaints may be lodged against the Service's activities (the Tribunal) but does little else to define the limits or scope of the Service's powers.

Central co-ordination, oversight and accountability

Clear processes for co-ordination and oversight are strong features of many intelligence communities today. By ensuring central co-ordination, the government is able to ensure that individual agencies do not overlap, become involved in rivalries, and ensure that complementary collection and analysis paths are followed. On the other hand, such centralised oversight also serves to ensure the public that all capabilities and agencies are being watched over by one body, ensuring against duplication and that gaps are being filled.

[71] *Security Service Act* 1996, 1(1)(4).

A key requirement of intelligence legislation is to provide clear lines of accountability, while subordinating intelligence services to the control of democratically-elected leaders (i.e. Ministers). The inherent secrecy that surrounds the activities of intelligence services makes it vital that both the executive and other oversight actors scrutinise the actions of these agencies. Examples of where these lines of oversight are clearly established in legislation include:

- The Canadian Security Intelligence Service Act 1984, with the Director-General placed under the authority of the Solicitor General, who in turn is responsible to Parliament. The Act states that 'This accountability is strengthened by the existence of an Inspector-General with powers to monitor agency compliance with legislation and directions issued by the Minister'.
- South Africa's legislative approach which created a National Intelligence Co-ordinating Committee backed up by Inspector-Generals to whom each Service Director was accountable (although this has been less than successful in practice).

In the UK, the heads of the three main Services are accountable to a Minister; they also have the right of direct access to the Prime Minister. The Czech Republic's legislative record on intelligence was less clear in developing lines of accountability: the 1991 enabling legislation for the Federal Security Information Service attempted to create a complex separation of powers (due to a fear of centralising too much power in the Interior Ministry), but resulted in confusion, with no single elected official with overall responsibility for the Service. This in turn impacted on the Service's ability to function, as it had little direction or feedback from the executive. This example indicates a need to clarify executive responsibilities, so as to avoid the vacuum created by ministerial or governmental indifference to intelligence services, as in the case of the Czech Republic. Indeed, without effective executive control (i.e. access to necessary information and awareness of service's activities), there can be no effective parliamentary oversight (as in many systems the Minister is responsible to the legislature).

Other countries similarly use executive oversight and accountability mechanisms to ensure proper co-ordination, control and guidance. For example, the United States has two bodies – the President's Foreign Intelligence Advisory Board (PFIAB), which advises the President on the quality and adequacy of intelligence collection, analysis and estimates, of counterintelligence, and of other intelligence activities – and its attached Intelligence Oversight Board (IOB) – which monitors and alerts the President and the Attorney-General to any intelligence activity which it believes may be unlawful or contrary to Executive order or Presidential directive.

It is clear therefore that strong executive control is a requirement for the effective oversight and functioning of intelligence services and therefore a key element to be addressed in any intelligence legislation.

Judicial oversight

In several of the cases examined above, the judicial system plays a role in regulating the activities of intelligence services in the domestic sphere. This primarily relates to instances when services wish to encroach upon the rights of individual citizens by means of intrusive surveillance or covert searches. Judicial oversight is required to set limits to achieve the proper balance between the protection of individual rights and the collection of necessary information. Different approaches have been adopted in the countries examined. In Canada and Argentina, judges are

asked to authorise surveillance warrants submitted by the intelligence services. In Canada a loophole exists in that a single warrant may be used to authorise several collection methods against a number of individuals. Guarding against such loopholes – and the potential for abuse that they present – is something that those developing intelligence oversight systems should keep clearly in mind.

Parliamentary oversight and accountability

The other key accountability mechanism is the legislature. Legislative involvement in the oversight of intelligence services enhances legitimacy and democratic accountability, while ensuring that security and intelligence agencies are serving the state as a whole rather than narrow political or other interests. There are many models of parliamentary oversight, with some being more robust than others.

In the Czech Republic, an initial impetus to ensure effective parliamentary oversight was curtailed by the 1994 legislation which restricted the relevant oversight committee to examining only issues regarding the rights and freedoms of individuals, while preventing it from examining budgets, the legality of operations or executive tasking of the agency. It also determined that the committee would receive information only from the government rather than the agencies, as well as that agency personnel would not have the right to report illegal actions to the committee. These restrictions have seriously curtailed the operation of effective parliamentary oversight and offer a clear lesson for what aspects should be included when developing effective parliamentary oversight mechanisms.

The UK model – as embodied in the Intelligence & Security Committee (ISC) – offers a compromise between the legislature's desire to oversee a secretive area of executive activity and the requirement to maintain the secrecy of the intelligence services. Whilst the ISC is not a traditional select committee and is appointed by the Prime Minister, it is made up of senior parliamentarians; and it has effective (if not statutory) access to the services and a range of information. The ISC is also limited by the fact it reports to the Prime Minister, not directly to Parliament. Whilst its mandate is somewhat limited (it cannot access ongoing operations, for example), the ISC has been operating beyond the parameters of its statute – for example, by looking at the intelligence assessments prior to the 2002 Bali bomb attack,[72] or the actions of UK intelligence personnel in handling detainees overseas.[73] The ISC does not, however, have the remit to examine complaints from the public; that function is undertaken by the judicial Commissioners. The result is that, combined with the lack of thorough oversight of defence intelligence and of the Joint Intelligence Committee, the UK's legislative oversight function is less than comprehensive and somewhat fragmented.

In contrast, the Security Intelligence Review Committee (SIRC) in Canada is not made up of parliamentarians and is appointed by the Prime Minister. It has a wide range of powers, including the ability to instigate investigations, access any information held by the Service, and interview any personnel. It also has the ability to direct the Inspector-General to conduct investigations and has full control over the content and publication of its annual report. The SIRC has been regarded as a good practice model for creating new parliamentary oversight bodies (as in the

[72] Intelligence & Security Committee, *Inquiry into Intelligence, Assessments and Advice prior to the Terrorist Attack on Bali 12 October 2002* (10 December 2002): www.cabinetoffice.gov.uk/publications/reports/intelligence/CM5724.pdf.
[73] Intelligence & Security Committee, *Handling of Detainees by UK Intelligence Personnel in Afghanistan, Guantanamo Bay and Iraq* (1 March 2005): www.cabinetoffice.gov.uk/publications/reports/intelligence/treatdetainees.pdf.

South African example). However, the SIRC does not have the remit to oversee the CSE – Canada's SIGINT agency – and thus the Canadian system of parliamentary oversight is also fragmented.

Germany has a complex system of parliamentary oversight, consisting of four separate committees, each examining aspects of the intelligence community's activities. In total, some 27 members of the Federal parliament are involved in oversight work. While there may be an element of overlap or fragmentation, the committees and commissions do wield some significant powers – for example, the Bundestag Control Commission's ability to make findings public if they feel it is necessary. In contrast to the UK system, the German executive is required by law to inform the Commission of intelligence activities. Notable also is the power of the G-10 Commission to terminate technical interception operations if it believes the law has been contravened or if a warrant has been issued on insufficient evidence. Whilst complicated, the multilateral system of parliamentary oversight in Germany has been refined over several decades and appears to offer potential lessons for the establishment of similar systems in other countries.

Differences between developed and developing world environments

In the countries examined, there were a variety of factors influencing the environment in which intelligence legislation was developed and implemented. These factors exerted influence both from within the agencies and the executive as well as externally from parliament, the public, the media, foreign states and international bodies. Some or all of these pressures are likely to be felt in other developed and developing states which undertake intelligence reform.

From within the executive, there are a number of potential influences. Perhaps the most obvious is the potential for the executive to abuse the exceptional powers of the intelligence services under its control. This can include the use of intelligence services to spy on political opponents or, as in the cases of South Africa and Argentina, to use the services to physically repress dissident elements of the population. As has been seen from the cases above, the reform of politicised intelligence services engaged in this kind of activity is a difficult and long-term task, which cannot be completed through legislation alone. On the opposite end of the spectrum is the Czech example, where the problem was not initially the executive's abuse of the intelligence services, rather their neglect. The new political leadership (made up mostly of former dissidents and political activists) deeply mistrusted the intelligence services which had spied on them for decades. This failure to engage effectively with the intelligence community left the agencies directionless and, in some instances, allowed them to return to their old methods and outlooks, thereby further complicating the process of effective reform.

In both the South African and Czechoslovak examples, the retention of former intelligence officials from the old regime caused difficulties. The decision to consolidate elements of opposing intelligence services into the new intelligence structures in South Africa was done for very understandable and pragmatic reasons. However, the consequences of this policy have since manifested themselves in the re-emergence of old factional lines within the principal intelligence agency and the creation of parallel intelligence organs to circumvent the official, but distrusted agencies. In Czechoslovakia, an initial decision to screen and remove those intelligence agents tainted by repressive activities faltered due to lack of resources and access to information. This failure to 'clean house' thoroughly was compounded by the initial muddle over the recreation of intelligence services, which saw large sections of the new agency being staffed by old intelligence personnel who began to replicate the old ways of working and targets.

The issue of how to deal with the retention or replacement of personnel from discredited or repressive intelligence services is a thorny one. By retention, one risks the continuation of old style practices under a new banner. By replacement the danger is that the services will have very few experienced personnel in their employ, with the subsequent risks this poses to their efficacy in guarding against threats to the new state.

Externally, a key consideration is the perception of the media and therefore the public. The public view that the intelligence services are acting beyond the rule of law can be a powerful agent for reform. In the Canadian example, the CSIS Act was the culmination of a series of scandals concerning intelligence activities that aroused public concern. Canada provided a further example of the importance of public opinion when, following the publication of a book written by a former Communication Security Establishment officer, outcry spurred the government to create a CSE Commissioner to oversee the agency's activities.

Another factor influencing legislation and implementation is that of international law and organisations. As we have seen, a primary driver for UK intelligence legislation came from within the agencies and the executive as a result of the need to address the European Court of Human Right's concerns regarding the legality of surveillance activities. Within a reform context, similar influence may be exerted by donor organisations (such as the International Monetary Fund or Work Bank), on the proviso that continued funding is dependent on effective reform.

Conclusion

In summary, it is clear that intelligence requires a number of key elements to both support its activities and ensure that it is operating within acceptable norms. These include:

- Clear mandates
- Central co-ordination, oversight and accountability
- Independent judicial oversight
- Independent parliamentary oversight and accountability
- Centralised analysis and assessments for all-source products
- An appreciation of the different governance structures that intelligence is designed to support

Key Sources

Brodeur, Jean-Paul. "The Globalisation of Security and Intelligence Agencies: A Report on the Canadian Intelligence Community". Brodeur, Jean-Paul, Gill, Peter, and Tollborg, Dennis (eds). *Democracy, Law and Security – Internal Security Services in Contemporary Europe*. Aldershot: Ashgate Publishing Limited, 2003.

Born, Hans. *Learning from Best Practices of Parliamentary Oversight of the Security Sector*, Working Paper Series No. 1, Geneva: Geneva Centre for the Democratic Control of Armed Forces (April 2002): www.dcaf.ch/publications/Working_Papers/01(E).pdf.

Born, Hans. *Democratic and Parliamentary Oversight of the Intelligence Services: Best Practices and Procedures*, Working Paper Series No. 20, Geneva: Geneva Centre for the Democratic Control of Armed Forces (May 2002): www.dcaf.ch/publications/Working_Papers/20.pdf.

Born, Hans and Leigh, Ian. *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Publishing House of the Parliament of Norway: Oslo, 2005).

Cerny, Oldrich. *Czechoslovak (Czech) Intelligence after the Cold War*, Conference Paper for workshop on 'Democratic and Parliamentary Oversight of Intelligence Services', Geneva: Geneva Centre for the Democratic Control of Armed Forces (October 2002).

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. *Accountability of Security Intelligence in Canada: a Background Paper to the Commission's Consultation Paper* (10 December 2004): www.ararcommission.ca/eng/index.htm.

Eenboom-Schmidt, Erich. "The Bundesnachrichtendienst, the Bundeswehr and Sigint in the Cold War and After", *Intelligence and National Security*, vol. 16: no. 1 (2001).

Estevez, Eduardo. *Executive and Legislative Oversight of the Intelligence System in Argentina: A New Century Challenge*, Conference Paper for workshop on 'Making Intelligence Services Accountable', Oslo: Geneva Centre for the Democratic Control of Armed Forces (19-20 September 2003): www.dcaf.ch/news/Intel%20Acct_Oslo%200903/Est%C3%A9vez.pdf.

Gill, Peter. "Security and Intelligence Services in the United Kingdom". Brodeur, Jean-Paul, Gill, Peter, and Tollborg, Dennis (eds). *Democracy, Law and Security – Internal Security Services in Contemporary Europe*. Aldershot: Ashgate Publishing Limited, 2003.

Herman, Michael. *Intelligence Services in the Information Age*. London: Frank Cass Publishers, 2001.

Herman, Michael. *Intelligence Power in Peace and War*. Cambridge: University Press, 1996.

Johnson, Loch. *America's Secret Power: the CIA in a Democratic Society*. New York: Oxford University Press, 1989.

Kent, Sherman. *Strategic Intelligence for American World Policy*. Princeton, New Jersey: Princeton University Press, 1966.

Leigh, Ian. "Democratic control of Intelligence and Security Services: A Legal Framework". Bryden, Alan and Fluri, Phillip (eds). *Security Sector Reform: Institutions, Society and Good Governance*, Baden-Baden: Nomos Verlagsgesellschaft, 2003.

Leigh, Ian. *Oversight of Security and Intelligence in the United Kingdom.*, Conference Paper for workshop on 'Making Intelligence Services Accountable', Oslo: Geneva Centre for the Democratic Control of Armed Forces (19-20 September 2003): www.dcaf.ch/news/Intel%20Acct_Oslo%200903/Leigh.pdf.

Lowenthal, Mark. *Intelligence: from Secrets to Policy*. Washington DC: CQ Press, 2000.

Lustgarten, Laurence. "National Security and Political Policing: Some Thoughts on Values, Ends and Law". Brodeur, Jean-Paul, Gill, Peter, and Tollborg, Dennis (eds). *Democracy, Law and Security – Internal Security Services in Contemporary Europe*. Aldershot: Ashgate Publishing Limited, 2003.

O'Brien, Kevin. *Controlling the Hydra: An Historical Analysis of South African Intelligence Oversight*, Conference Paper for workshop on 'Making Intelligence Services Accountable', Oslo: Geneva Centre for the Democratic Control of Armed Forces (19-20 September 2003): www.dcaf.ch/news/Intel%20Acct_Oslo%200903/OBrien.pdf.

OECD Development Assistance Committee '*Security Sector Reform and Governance – Policy and Good Practice'* (2004): www.oecd.org/dataoecd/8/39/31785288.pdf.

Ransom, Harry. *Central Intelligence and National Security*. London: Oxford University Press, 1958.

Rempel, Roy. "Canada's Parliamentary Oversight of Security and Intelligence", *International Journal of Intelligence and Counterintelligence*, Vol 4: No. 17 (2004).

Shapiro, Shlomo. "Parliament, Media and the Control of the Intelligence Services in Germany". Brodeur, Jean-Paul, Gill, Peter, and Tollborg, Dennis (eds). *Democracy, Law And Security – Internal Security Services In Contemporary Europe*. Aldershot: Ashgate Publishing Limited, 2003.

Williams, Kieran. "Czechoslovakia 1990-2". Williams, Kieran and Deletant, Dennis (eds). *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia And Romania*. Basingstoke: Palgrave, 2001.

Williams, Kieran. "The Czech Republic since 1993". Williams, Kieran and Deletant, Dennis (eds). *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia And Romania*. Basingstoke: Palgrave, 2001.

Wilson, P. 'The Contribution of Intelligence Services to Security Sector Reform'. Conflict, Security and Development 5:1 April 2005