



GENEVA CENTRE FOR THE DEMOCRATIC CONTROL OF
ARMED FORCES (DCAF)

OCCASIONAL PAPER NO. 3

**INTELLIGENCE PRACTICE AND DEMOCRATIC
OVERSIGHT – A PRACTITIONER'S VIEW**

DCAF Intelligence Working Group

Geneva, July 2003

**GENEVA CENTRE FOR THE DEMOCRATIC CONTROL OF
ARMED FORCES (DCAF)**

OCCASIONAL PAPER NO. 3

**INTELLIGENCE PRACTICE AND DEMOCRATIC
OVERSIGHT – A PRACTITIONER'S VIEW**

DCAF Intelligence Working Group

Geneva, July 2003

DCAF Occasional Papers

DCAF Occasional Papers constitute studies designed to promote reflection and discussion on civil-military relations and issues of democratic control over defence and security sectors. These studies are commissioned by the Geneva Centre for the Democratic Control of Armed Forces.

The views and opinions expressed are those of the author(s) and do not necessarily reflect those of the Geneva Centre for the Democratic Control of Armed Forces.

CONTENTS

1. Introduction.....	1
2. The Functioning of Intelligence Services.....	5
2.1. The Purpose of Intelligence.....	5
2.2. Coping with New Risks, Dangers, and Threats.....	7
2.3. International Cooperation.....	9
2.4. The Categories of Intelligence.....	12
2.5. The Functions of Intelligence.....	13
2.5.1. Collection.....	13
2.5.2. Analysis.....	15
2.5.3. Counterintelligence.....	16
2.5.4. Covert action.....	17
2.6. The Intelligence Cycle.....	18
2.7. Secrecy.....	20
2.8. The Missions of Intelligence Services.....	23
2.8.1. The Mission of Internal Intelligence Services.....	23
2.8.2. The Mission of External Intelligence Services.....	24
2.9. The Organization of Intelligence Services.....	28
3. The Legal Framework.....	32
4. Democratic Control of Intelligence Services.....	36
4.1. Executive Control and Accountability.....	38
4.2. Legislative Oversight.....	46
4.3. Judicial Control and Supervision.....	53
4.4. Informal and Indirect Supervision by the Public.....	56
5. Transformation and Reform of Intelligence Services.....	59
5.1. Challenges That States in Transition Face When Reforming Their Intelligence Services.....	59
5.2. Replacing the Old System with New and Democratically Controlled Intelligence Services.....	62
5.2.1. Clear Guidance and Coordination of Intelligence Services.....	64
5.2.2. Control, Supervision, and Oversight of Intelligence Services.....	65
5.2.3. Professionalization of Intelligence Services.....	66
5.2.4. Strengthening the Relationship between Legislation & Reform.....	67
5.2.5. Practical Measures to Enforce the Program of Change & Reform.....	67
5.3. The Threats to Security and the Impact of September 11, 2001.....	68
6. Summary of Conclusions.....	73
Bibliography.....	75

INTELLIGENCE PRACTICE AND DEMOCRATIC OVERSIGHT – A PRACTITIONER'S VIEW

DCAF Intelligence Working Group

1. Introduction

Democracy is founded on every citizen's right to take part in the management of public affairs. This requires the existence of representative institutions at all levels and, as a cornerstone, a parliament in which all components of society are represented and which has the requisite powers and means to express the will of the people by legislating and overseeing government action¹.

A democratic state must ensure the enjoyment of civil, cultural, economic, political and social rights by its citizens. Hence, democracy goes hand in hand with an effective, honest and transparent government that is freely chosen and accountable for its management of public affairs. By democratic constitutional design, the executive branch is required to share its powers with the legislative and judicial branches. While this can lead to frustrations and inefficiencies, its virtue lies in the accountability that sharing provides.²

Public accountability applies to all those who hold public authority, whether elected or appointed, and to all bodies of public authority. Accountability has the *political purpose* of checking the power of the executive and therefore minimizing any abuse of power. The *operational purpose* of accountability is to help to ensure that governments operate effectively and efficiently.³ Securing and maintaining public consent for the organization and activities of the state and the government is fundamental precept of democratic theory. For this reason, no institution, function or act of the state, and no organization or activity of the government can be exempted from parliamentary oversight. All the components of a state's '*security sector*' are

¹ Hopkinson, Nicholas. 2001. *Parliamentary Democracy: Is There a Perfect Model?* Bodmin, Cornwall: MPG Books Ltd., pp. 1-8; and, Held, David. 1999. *Models of Democracy*, 2nd ed. Oxford: Polity Press, p. 108.

² A standard definition of democracy today is: Modern political democracy is a system of governance in which rulers are held accountable for their actions in the public realm by citizens, acting indirectly through the competition and cooperation of their elected representatives. See: Huntington, Samuel. 1991. *The Third Wave Democratization in the Late Twentieth Century*. Norman: University of Oklahoma Press.

³ Heywood, Andrew. 1997. *Politics*. Houndmills: Palgrave, p. 375.

included therein, and these may broadly be defined as encompassing those institutions that are legitimately authorized to use, or order the use of force, or the threat of force, for the protection of the state and the people, and for safeguarding the national interests, the society and the liberty of the citizens. The organizations concerned comprise the armed forces, paramilitary forces, the border guards and customs services, security services, intelligence services, police forces, judicial and penal systems, and the civil authorities mandated to control and oversee these institutions.⁴

Among these organizations, intelligence (or secret) services have always stood out as a conspicuous exception to the rule, in that they enjoyed greater immunity from accountability and close oversight than others. Compared with other organizations of the security sector, intelligence services do present unique difficulties for control and also for providing accountability. The basic conundrum for intelligence lines in its requirement for secrecy to be effective. Intelligence services cannot disclose their activities to the public without disclosing them to their targets at the same time. Their budgets are secret; their operations are secret, and both their products and their achievements are secret. As a result, intelligence services are not subject to the same rigors of public or parliamentary debate or to the same scrutiny by the media as other parts of the government. A degree of secrecy on intelligence matters has always existed within governments and this has always presented a conflict with democratic ideals, which remains unresolved. Thus, intelligence services are still the least controlled entity, as well as being the most difficult to control.

As instruments of the state, intelligence services can be used for the better or for the worse. The history of the bygone century is replete with lessons of both: on the one hand illustrating the misuse of intelligence services by despots such as Lenin, Stalin, Hitler, and Mussolini to impose their brand of totalitarian regimes, to enforce control over their populations, to prepare and support expansion through conquests, the subjugation of other states and enslavement of peoples. One of the most depressing lessons of the Cold War is that intelligence and security services possessing unprecedented powers to monitor and suppress dissent in all its forms, have become central to the structure of authoritarian states. The KGB was many times larger than any western intelligence or security service largely because of its war on all fronts against 'ideological subversion'. As is now known, informers of the GDR's

⁴ For further elaboration on the definition of the 'security sector' see: Hendrickson and Karkoszka. 2002. The challenges of security sector reform. In: *SIPRI Yearbook 2002, Armaments, Disarmaments and*

Staatssicherheits-dienst were seven times more numerous than in Nazi-Germany. However different the Nazi, communist, apartheid, clerico-fascist, and national-militarist ideologies of Hitlerite Germany, the Soviet Empire, South African white supremacists, Iranian fundamentalist Ayatollahs, and Iraqi Baathists or Latin American Juntas, they shared the application of the most unrestrained methods against domestic opposition to the regime, and to this day, such services remain indispensable support networks for some of the world's most unpleasant regimes.

On the other hand, lessons abound demonstrating the crucial role that intelligence played in helping democratic powers to defeat Nazi-Germany; in containing the spread of communist ideology by force; in preventing the Cold War from turning hot and nuclear; and – through the monitoring of arms control measures with IMINT⁵, ELINT⁶, and TELINT⁷ – in precluding the arms race which has been embarked upon by superpowers, from getting out of hand. Nowadays, in the global war against terrorism, the lessons are again obvious: that intelligence has proven to be the most effective weapon against terrorism and that there is no substitute for intelligence services.⁸

If one good thing can come out of these lessons, it may well be an awakening to the necessity of establishing democratic oversight of intelligence services, which is essential in protecting democracy. In a democratic state, intelligence services should strive to be effective, politically neutral or non-partisan, adhere to a professional ethic and operate within their legal mandates, in accordance with the constitutional-legal norms and democratic practices of the state.⁹

The prerequisite for making democratic oversight work is an intimate knowledge of the purpose, role, functions, and missions of the intelligence services. Such knowledge and understanding is also needed for making intelligence smarter and for any reform of intelligence services commensurate with democratic norms and standards.

International Security. Oxford: Oxford University Press, p. 179.

⁵ *Imagery Intelligence*, mainly by satellites, UAV, or aircraft.

⁶ *Electronics Intelligence*, together with Communications Intelligence (COMINT), constitutes the main parts of Signals Intelligence (SIGINT).

⁷ *Telemetry Intelligence*: a special variety of Signals Intelligence (SIGINT).

⁸ United States Congress Committee on Foreign Relations. 2000. *Countering the changing threat of international terrorism*. Washington D.C.: US GPO.

⁹ Gill, Peter. 2003. Democratic and Parliamentary Accountability of Intelligence Services after September 11th. Geneva, January 2003. Geneva Centre for the Democratic Control of the Armed Forces. *Working Paper No. 103*.

Thus, this paper examines the work, the place, and the functioning of intelligence services in open and free societies. The papers considers the various elements that are necessary for creating a coordinated, civilian intelligence structure that is reflective of the needs of a democratic society and the threats to the state, and lists the main criteria for democratic control, supervision, accountability, and oversight of their activities. Correspondingly, the legal framework, the role, functions and procedures of executive and judicial control and supervision, and of legislative oversight are presented. In addition, some of the main problems facing states in transition whilst establishing democratic control and with the reform of their intelligence services are discussed.

But what is intelligence? There is no shortage of definitions.¹⁰ In general usage, intelligence denotes three things: (1) a *particular* knowledge; (2) the type of organization producing this knowledge; and, (3) the activity pursued by this organization.¹¹ In a narrower sense, intelligence is a subset of the broader category of information which, in the hierarchy underlying modern knowledge management theory, is a step in the chain of value creation, beginning with data, which leads to information, then to knowledge, and culminates in wisdom. Since knowledge resides in the user and not in the collection of information, only human beings can take the central role in knowledge creation. Information, available in ever greater abundance and thus ever cheaper, has become the only factor of production¹² which gains value by its use.

Moreover, if more people work on the same data and information, the greater the value in knowledge they can gain from it. Thus, while information is anything that can be known, regardless of the way in which it is discovered, intelligence refers to that knowledge that meets the stated or understood needs of policymakers and to the entire process by which data and information are identified, obtained, and analyzed to respond to these needs. Most intelligence output has a significant element of ‘processing’, and precisely this is reflected in the military distinction between “unprocessed data of every description” – defined as information – and “the product

¹⁰ For the many definitions see: http://intellit.muskingum.edu/whatis_folder/whatisintelintro.html

¹¹ Kent, Sherman. 1965. *Strategic Intelligence for US World Policy*. Hamden: Archon Books, p. xxiii.

¹² Land, labour, and capital – the traditional factors of production – do not disappear, but they become secondary to knowledge. Companies born in virtual forms on the Net, such as ‘*etoys*’ and ‘*amazon.com*’ have gained many times the value of their brick-and-mortar counterparts, despite limited investments in traditional factors of production.

resulting from the processing of information” – defined as intelligence.¹³ Hence, all intelligence is information; but not all information is intelligence.¹⁴

Compared to the assemblage of information from diplomatic and all other sources, intelligence works more by ‘*push*’ than ‘*pull*’ and its processing gives ‘*added value*’ to its collected evidence. A corollary is that it tends to deal with difficult questions in which there may also be elements of concealment or deception. The degrees of processing vary. Many covertly acquired documents and intercepted messages need careful exegesis. Others may be relatively transparent, though even these may necessitate translation. Moreover, since it is a ‘*tailored output*’, meeting specific user needs, intelligence has to persuade its customers through ‘*analytic tradecraft*’ of a trail of evidence, assumptions and conclusions. Furthermore, ‘*opportunity analysis*’ is advocated, identifying opportunities or vulnerabilities one can exploit to advance a policy, to plan an intervention, or to conduct a joint or combined operation. Thus, it is the accent on analysis, presentation, and persuasion which distinguishes intelligence from information that is more of the reporting and news type. In addition, the emphasis on processing is reinforced by the forecasting role since intelligence’s greatest value is as a guide to the future.¹⁵

Thus, intelligence is like archaeology: a matter of interpreting evidence as well as finding it¹⁶. Cleverness in a wide sense distinguishes intelligence from information and data – though even the best intelligence does not guarantee wisdom. Nevertheless, the idea of intelligence as objective judgment and forecasting deserves recognition and a prominent place, not only in any concept of liberal international order, but even more so in the multilateral scope of international cooperation.

2. The Functioning of Intelligence Services

2.1. The Purpose of Intelligence

The purpose of intelligence is to inform government: ‘*telling truth unto power*’. Intelligence serves and is subservient to policymaking. It exists: (1) to avoid strategic

¹³ *British Joint Operational Intelligence*. 2000. Joint Warfare Publication 2-00; Annex 1A, p. 1.

¹⁴ Lowenthal, Mark M. 2003. *Intelligence: From Secrets to Policy*. 2nd ed. Washington D.C.: CQPress, p. 2.

¹⁵ Herman, Michael. 2001. *Intelligence Services in the Information Age*. London & Portland, OR: Frank Cass Publishers, pp. 7-9.

¹⁶ *Ibid.* p. 10.

surprises; (2) to provide long-term expertise; (3) to support the policy process; and (4) to maintain the secrecy of information, needs, sources, and methods¹⁷. Intelligence is partly a government's specialist on certain methods of collection and exploitation of data and information, but at the same time to a certain extent the expert on certain subjects, with its role balancing uneasily between the two. In formal terms, the scope of coverage appears unlimited since there are few guides to the subjects that intelligence should not tackle. Yet, there are limitations to the subjects on which it holds authority. These are areas where intelligence has a comparative advantage over other sources of knowledge, and these tend to consist in the fungible but recognizable ideas of '*national security*'. There, its biggest area of concern is actual or potential risks of violent change, threats of this, and instability, as well as situations in which these figure, along with all means and methods of conflict, their use or intended use, the capabilities they provide, their scope for development and the threats that they constitute.

Thus, when properly used as the '*first line of defence*', intelligence services contribute to a democracy's ability to safeguard the security and well-being of the nation and its people, to '*good governance*', and efficient and effective functioning of the state. In the hands of responsible democratic leaders, intelligence is the major contributor to the state's absolute obligation to its people to make sure that threats to security are detected in time for them to be counteracted, and for harm, death and destruction to be prevented.¹⁸

The world of the 21st century is likely to be fraught with new perils, coupled with more uncertainty and unpredictability than at any other time in history. Leadership has become more complicated with the multiplication of actors, sources of crises, and means of conflict, increasing economic interdependence, accelerating technological developments and the growing interconnectivity of information and communications, and thus new dynamics and vulnerabilities at play. Governments must understand these in order to respond to them. It is often the case that the options available will depend upon how early problems are identified. Choosing the right option, in turn, will depend upon knowing what the consequences are apt to be. Once a course of action is chosen, it is vital to know what the effects of the decision may be, so that any necessary adjustments can be made. In any case, making the right choice will hinge

¹⁷ Ibid. pp. 2-5.

¹⁸ Lustgarten, Laurence and Leigh, Ian. 1994. *In from the Cold: National Security and Parliamentary Democracy*, Oxford: Clarendon Press.

upon the quality of the information available. Hence, informed decision- and policymaking require adequate intelligence, assessments and warning.

Only if top executive decision- and policymakers, and their planners and councillors are sufficiently informed about the state of the world, the likely developments, the existing and potential threats, dangers, risks, and opportunities, can they be expected to make sound judgments in the areas of internal and external security, national defence and foreign relations.

Intimate knowledge of the strategic situation, the possible and probable developments, the risks, dangers, threats and opportunities, are a prerequisite for (1) the definition of national interests; (2) the development of an adequate security policy and sound national and military strategies; (3) the determination of the missions of the armed forces and the security forces; and (4) the establishment of doctrine and its translation into operations. Moreover, this knowledge, contingency planning, and timely warnings are the prerequisites for efficient and effective national crisis management.

Intelligence services provide the basis for this knowledge. They must also, at all times, be able to warn of impending crises and detect possible surprises, dangers, threats or attacks in advance. With smaller military forces, the warning function grows in importance. Sufficient time is needed to adapt the defence forces, should full reconstitution be required again. Very early warning thus becomes a necessity.

The rapid evolution of the strategic, political, and economic environment since the end of the Cold War has furthered the quest for information on security issues that governments will have to pursue. With conventional military threats diminishing, new risks and dangers connected with proliferation, globalization and destabilization, multiply the security challenges, make assessments more complex, developments less predictable, and crises and conflicts less calculable. With transnational risks and dangers predominating, national security is becoming ever more dependent on regional and global stability and the solidarity of like-minded nations. Since geographical distance can no longer provide adequate security, states have to influence crises and conflicts and focus security and foreign policy ever more on conflict prevention, crisis management, crisis reaction and peacekeeping in coalition with the able and willing.

2.2. *Coping with New Risks, Dangers, and Threats*

The set of tasks assigned to intelligence services are more complex, more volatile, and more numerous than they were during the Cold War. What has dramatically changed for intelligence services is the number and diversity of risks, dangers and threats: apart from the inequality of states, where in some sovereignty is a myth, if not hypocrisy,¹⁹ there are states with rogue governments which promote destabilization in their strategic environment, produce weapons of mass destruction, protect terrorists, and sponsor the assassination of their political opponents abroad; and there are the 'failing states' provoking endemic conflict and mass-migration. Moreover, there is the growing number of powerful non-state entities. While most multinationals or charitable NGOs are honourable, others, along with some financial institutions or monopolistic media organizations, may be more questionable. Quite another set are international terrorist organizations, ideological, ethnic or religious extremists, mafias, and large criminal organizations, which present a serious and dangerous threat to all societies. Taking advantage of the opening of borders and skilfully exploiting the discrepancies between various national laws and judicial procedures, terrorists, extremists, war criminals, proliferators, weapons and drug dealers, smugglers, and specialists in the laundering and recycling of dirty money, or in the clandestine disposal of noxious waste or polluting materials, remain unpunished and prosper. Where law enforcement structures remain ineffective, the balance sheet is clearly on the side of crime and not the law. Moreover, there are some new intelligence services and, given that nowadays it is fashionable to reject the bureaucratic state and to transfer its task to the private sector for the sake of efficiency and cost reductions, all sorts of private security and intelligence organizations which might require some monitoring.

All these actors, and even more so the offenders engaged in hacking and information warfare, have made the problem of predicting what their next moves and targets are going to be many times more complicated. All means of collection have to be exploited in a systematic way to try to find intelligence and evidence, foremost about intentions, plans and capabilities, but equally about the organization, resources, communications, connections, and movements, of these widely diverse groups.

The rule for tasking intelligence services has always been to go after that which cannot be acquired better, more safely or more cheaply by any other means. Methods of collection have changed dramatically during the course of the 20th Century: satellite imaging and electronic interception are the most obvious evidence

¹⁹ Krasner, Stephen D. 1994. *Sovereignty: Organized Hypocrisy*. Princeton: Princeton University Press.

of this, and have become the tools of choice. However, other trends affecting the intelligence services – outside the US – include budget reductions resulting from fiscal realities, technological advances that help intelligence targets protect their secrets, and the need to serve a broader range of government clients with a growing variety of intelligence requirements.

Since intelligence is a scarce resource, supply and demand must be reconciled. The manner in which this is done determines how much waste and inefficiency will occur. While intelligence professionals and modern systems can do just about anything, they cannot do everything. Demand consistently outstrips supply. In the industrial world, the two approaches that have evolved to cope with this challenge are top-down central planning and bottom-up consumer-driven free markets. In response to Cold War demands, western intelligence services chose central planning to solve the problem of allocation. However, the waste and inefficiency of central planning is no longer affordable. Cost-effective intelligence requires the resiliency and discipline of the marketplace. This the more so, since the diverse array of global, regional and transnational political, economic, social, and military challenges and opportunities requires for states the transition away from *risk avoidance* to a *risk management* focus.

Another, often undervalued aspect is continuity, which is of particular importance for smaller countries. Discontinuation of competence cannot be recovered with much hope of success some years later. Politicians and officials without much exposure to the production of intelligence often think that “the services can mothball competence and keep it going on the backburner for bad times. In most cases this is not possible. Even less understood is the fact that, if intelligence is not alert when a new technology is introduced, it will find it very difficult and often impossible to catch up later. At least in the technical field, the truth almost always is that if intelligence does not hang in there, it risks being left out in the cold for a very long time, even if the government is willing to spend a lot of money”.²⁰ Hence, what is needed in order to succeed is continuity, and increased international cooperation among intelligence services.

2.3. International Cooperation

²⁰ Kettis, Par, Ambassador. 2000. The Future of Covert Intelligence. In: Shukman, Harold, ed. *Agents For Change. Intelligence Services in the 21st Century*. London: St Ermin's Press; pp. 83-84.

Historically, states have been willing to reciprocate where they share common intelligence interests and concerns.²¹ For the most part, these relationships have proven mutually beneficial.²² Even where the interests of two nations do not entirely converge, intelligence often supplies the 'quid' for other's 'quo'. Bilateral cooperation normally involves the sharing of intelligence information and analyses on topics of mutual interest. Such bilateral relations can and will, however, only be maintained and continued, if both parties strictly respect the basic agreement underlying their intelligence sharing: that the origins and details of the intelligence provided by the partner service will be protected according to its classification, and will not be passed on to third parties.²³

Though countries with smaller intelligence resources are not always able to bring to the table capabilities which match those of bigger services, they can reciprocate in other ways. In some cases, states can provide geographic and other access that would not otherwise be available. In others, intelligence services of smaller countries can provide skills, expertise, and languages bigger services would otherwise have to develop. While some states spend a greater percentage on intelligence than others, it is often unreasonable to expect quantitative comparability in such relationships. Quite apart from access and capabilities states can provide, there is often great benefit in having close and enduring friends who can be counted on in times of trouble. Intelligence services provide tangible cement for such security relationships. Since intelligence requirements of government decision-makers increasingly relate to matters that are global or transnational in nature, intelligence's relationships with other countries are expanding. One reason for this being that no national intelligence service can effectively cover all of the places where such activities may take place throughout the world. In addition, numerous special *fora* exist worldwide to deal with specific subjects by bringing together the intelligence services of different countries and which are known to a greater or lesser extent.²⁴

²¹ Richelson, Jeffrey T. 1999. *The U.S. Intelligence Community*. Exchange and Liaison Arrangements. 4th ed. Boulder: Westview Press.

²² See for example: Herman, Michael. 2001. *Intelligence Services in the Information Age*. Norway as an Intelligence Ally. London & Portland, OR: Frank Cass Publishers, pp. 139-146.

²³ The so-called 'Third-Party Rule'.

²⁴ Among the more famous in Europe are the "TREVI Group", established in 1975, bringing together the ministers of justice and interior of the EU in the fight against "Terrorisme, Radicalisme, Extrémisme et Violence Internationale", Maastricht's third pillar – involving immigration and asylum, policing, customs and legal cooperation – superseded TREVI and mandated the creation of the multinational European Police Office (Europol), operational since 1998; another one is the "Berne Club", set up in 1971 for thematic meetings on the concern of the day, which comprises 19 European countries; a third one is the "Kilowatt Group", set up in 1977 and comprising 15 countries; a fourth one is the "Conference of Western Mediterranean Interior Ministers", set up in 1982 in Rome to combat Islamic fundamentalism and organized crime, comprising 6 countries. Yet another one is "Le Groupe Informel Européen de

New non-military risks and threats, expanding international intervention, and multi-national peace operations account for the rapid expansion of requirements for intelligence contributions to international security. At the same time, they are opening the way for more advanced cooperation between security and intelligence organizations from participating and interested countries. The grave threat posed by international terrorism and the danger of a recrudescence of internal terrorism make it essential to achieve the broadest possible cooperation among different countries.

Peace operations in Bosnia and Kosovo have already represented what appears to be the new pattern of intelligence support for international intervention of all kinds. All those responsible for such operations, from the UN Secretary-General downwards, have emphasized the need for good intelligence. The UN²⁵, the EU²⁶, NATO²⁷, other supranational organizations, and their actions still depend on national intelligence inputs. National intelligence is relied upon to fill gaps, validate other sources and above all, assess. These international organizations will eventually develop machinery for supranational intelligence assessments, but it will be a long haul and will have to build on interstate exchanges. Since quite some years, the US and some

Coopération dans le Domaine de la Lutte Contre le Terrorisme" (GIECLCT) which comprises the heads of the EU member states' counterterrorist operational teams, as well as their counterparts from Sweden and Norway. There is the "Cross-Channel Intelligence Conference", founded in the early 1970s by the 4 countries adjacent to the English Channel. In addition, there is NATO's *Special Committee* which brings together the security services of the member countries. Other 'clubs' of intelligence services contributing to the limitation of weapons of mass destruction meet regularly within the framework of the Missile Technology Control Regime (MTCR), the Nuclear Suppliers Group, the Australia Group, the Wassenaar Agreement, and other groups. Furthermore, there is a developing EU-Russia intelligence cooperation aimed at fighting terrorism and sharing intelligence within the Partnership and Cooperation Agreement (PCA).

²⁵ Many failures in the history of UN field operations might have been avoided if the UN had taken a more forthright approach to intelligence and if it had possessed a stronger mandate to collect information. Though an enlightened view would see international security as an essential prerequisite to national security and the UN as an international institution that needs to be strengthened, including by increasing its capacity to gather and analyse intelligence, major states have been reluctant to give the UN a greater intelligence mandate. Many of them holding this belief, because intelligence is power and because they feel that their own power would be threatened by a UN that possessed real intelligence, especially intelligence they may themselves not have. See: Dorn, Walter A. *The Cloak and the Blue Beret: The Limits of Intelligence-Gathering in UN Peacekeeping*, at: http://www.rmc.ca/academic/gradrech/dorn16_e.html

²⁶ The EU is striving to build its own intelligence organization, see: Baker, Charles. *The search for a European intelligence policy*. e-Prints, at: <http://www.fas.org/irp/eprint/baker.html>. And: Becher, Klaus; Molard, Bernhard; Oberson, Frédéric; Politi, Alessandro. 1998. *Vers une politique européenne de renseignement*. Institut d'études de sécurité. Paris: Cahier de Chaillot No. 34. pp. 58

²⁷ There is no integrated intelligence body within the NATO-Alliance. It was national intelligence services' concern over document security that obliged NATO to abandon any idea of creating such a cell. Throughout NATO's history, intelligence, unlike other aspects of defence, has not been organized in truly integrated structures within the Alliance. NATO's limited intelligence elements have produced harmonized assessments of the military risks, dangers, and threats to the treaty area, supported by formal gateways to, as well as informal input by, the intelligence services of the member states. These arrangements are perceived as rather too cumbersome and inflexible to serve as a strategic intelligence network responsive to future requirements of international security policy. There are plans for reform of NATO's intelligence architecture, which take a much broader approach to intelligence. See: van Rensen, Peter. 1997. *Informationsbedarf der Gemeinsamen Aussen- und Sicherheitspolitik der Europäischen Union*. Ebenhausen: SWP Paper IP 3046, pp. 27-29 and 44.

other countries are committed to intelligence support for international organizations.²⁸ To some extent, this is already a *de facto* underpinning of international society.

Security has vastly expanded in other directions in the minds of international organizations, governments, and publics ever since the end of the Cold War to embrace considerations of international order, justice, and humanitarianism. Like armed forces, national intelligence is increasingly concerned with other peoples' security, not only with its own state's. Coalition forces deployed in peace operations require virtually the full range of wartime intelligence support. The concepts of graduated force, surgical strikes, low casualties and minimum collateral damage are all intelligence-dependent. Operation 'Allied Force' against the Federal Republic of Yugoslavia in 1999 has demonstrated the paradox of highly public international operations depending crucially on secret intelligence. However, the growing need for intelligence contributions to international security extends beyond conflict prevention, crisis management, crisis reaction, peace operations, information operations, and negotiating peace settlements, to other groups of world-wide and long-term security issues. The fight against terrorism, where intelligence is the most critical resource, is one such case; the limitation of weapons of mass destruction and other arms proliferation is another. A third category is the support of the many agreements that now exist for arms control and other confidence-building measures. International sanctions are a fourth category of wide-ranging, intelligence-driven cooperation²⁹. A fifth category is the assistance to law enforcement in the fight against the drugs trade, money laundering, and other forms of international organized crime. A sixth category is violations of Human Rights. Interventions for natural or other disaster relief and humanitarian assistance constitute a seventh category. Moreover, there is the growing need for international intelligence cooperation in order to protect critical national infrastructures and for defence against cyber attacks.

2.4. The Categories of Intelligence

Intelligence can be grouped in different ways. Generally two categories of intelligence are distinguished:

²⁸ US intelligence is the main contributor to UN and to NATO operations. During IFOR/SFOR and the Kosovo operations in the former Republic of Yugoslavia the US provided by far the largest part of necessary intelligence.

²⁹ International arrangements between intelligence services underpin these political agreements in these four categories. National intelligence tips off collaborating nations, or is used to keep them from backsliding.

- *Security intelligence*, which is information that is relevant to *internal security*: for the protection of the state, territory and society from foreign-influenced activities, such as subversion and espionage, or politically motivated violence. It is collected by internal intelligence services to help maintain public safety and ensure internal security.³⁰
- *Foreign intelligence*, which is information that is relevant to *external security* and for warning purposes. The maintenance of external security requires knowledge of the risks, dangers, and threats as well as of the opportunities and likelihood of events and outcomes. Hence, information is needed about intentions, capabilities and activities of foreign powers, organizations, non-state groups, and their agents that represent actual or potential risks, dangers, or threats to the state and its interests abroad. This information is collected by external intelligence services to help promote and safeguard national interests, including political, economic, military, scientific, social and security interests.

Purposes and targets of *foreign intelligence* and *security intelligence* collection functions differ. So too do the nature and extent of the risks to which they give rise. It is important that control and accountability arrangements reflect these differences. Thus, because of the intrusive nature of the powers of the internal intelligence service, and the fact that collection is executed domestically, potentially against the own citizens, the function requires strict controls to ensure that internal security and safety are appropriately balanced against the rights of individual citizens and residents.³¹

2.5. The Functions of Intelligence

Generally, intelligence services have three basic functions: *collection*, *analysis*, and – intrinsic to the entire intelligence process – *counterintelligence*. *Covert action*, the more occasional fourth one for external intelligence services, is increasingly disputed as an appropriate intelligence function in a modern democratic state.³²

³⁰ For example, the British Security Service (MI5), which is a security intelligence agency, also has the mission of safeguarding the economic well-being of the UK against threats from overseas. See: <http://www.mi5.gov.uk/function.htm>

³¹ Johnson, Loch K. 2002. *Bombs, Bugs, Drugs and Thugs: Intelligence and America's quest for security*. Ch. 9. Balancing Liberty and Security. New York: New York University Press. pp. 199-222.

³² Caparini, Marina. 2002. *Challenges of control and oversight of intelligence services in a liberal democracy*. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF), Geneva 3-5 October 2002, p. 2.

2.5.1. Collection

Collection is the bedrock of intelligence: the acquisition of information about persons, places, events, and activities, which is needed by the government but cannot be obtained through publicly available sources, diplomatic and other contacts. Without collection, intelligence is little more than guesswork.³³ Collection management systems are used for each of the three principal collection disciplines: *human intelligence* (HUMINT), which is information collected by humans – by spies, agents, and insiders, or gleaned from defectors, ‘walk-ins’, informers, diplomats, businessmen, travellers, and the media, etc.; *signals intelligence* (SIGINT) comprising data and information collected through intercepts of radio, radar, or other electronic emissions, including laser, visible light, and electro-optics³⁴; and *imagery intelligence* (IMINT) which is data and information collected via photography, electronic, infrared, ultra-violet or other image-capturing technologies, from land, sky, or space.³⁵

Human intelligence can be further divided into *overt* and *clandestine collection*. The skills and techniques for clandestine human intelligence are quite different from those required for overt human collection³⁶, and therefore organizations and responsibilities differ. So too is organizing the reporting and distribution of intelligence collected by each of the other disciplines. Since cartography and mapping have come to depend heavily on imaging, an argument can be made for lumping military and other mapping within this collection discipline.³⁷

Theoretically, all collection capabilities³⁸ should be engaged against the same target in order to ensure independent confirmation of the facts obtained by one discipline. Due to numerous complexities and competing requirements this is not always

³³ Lowenthal, Mark M. op. cit. pp. 54-86.

³⁴ For some of the best coverage see: Bamford, James. 2001. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency – From the Cold War through the Dawn of a New Century*. New York: Doubleday. And: Bamford. 1982. *The Puzzle Palace: a Report on America's Most Secret Agency*. Boston: Viking.

³⁵ For information on airborne and satellite imagery see: US National Commission for the Review of the National Reconnaissance Office. November 14, 2000. *Report: The National Commission for the Review of the National Reconnaissance Office*. Washington D.C.: GPO. Also at: <http://www.nrocommission.com> And: Best, Richard A. 2000. *Airborne Intelligence, Surveillance, and Reconnaissance (ISR): The U-2 Aircraft and Global Hawk UAV Programs*. Washington D.C.: Congressional Research Service, Library of Congress. Also: *Space Reconnaissance and the Management of Technical Collection*. At: <http://www.fas.org/irp/offdocs/int015.html>

³⁶ Steele, Robert David. 1996. Open Source Intelligence: What Is It? Why Is It Important to the Military? *American Intelligence Journal*. Vol. 17, nos. 1 and 2; pp. 35-41.

³⁷ Odom, William W. 2003. *Fixing Intelligence. For a more Secure America*. New Haven and London: Yale University Press; pp. 137-138.

³⁸ For other collection disciplines see: USAF Intelligence Targeting Guide. February 1998. Air Force Pamphlet 14-210 Intelligence; Attachment 3: Sources of Intelligence, at: <http://www.fas.org/irp/doddir/usaf/afpam14-210/part16.htm>

possible or practical, and often very costly. Thus, open source or publicly available information is needed to identify gaps in the knowledge, to confirm that the information is not otherwise available, to ensure that the need justifies using expensive or risky collection capabilities to obtain it, and then to task intelligence collectors.

Intelligence collection systems should not be used for collecting publicly available information. Although it will often be collected as a collateral by-product during the course of intelligence-gathering, public information should be obtained through other means than clandestine ones. The different intelligence collection capabilities should only be used to collect information that can reasonably be determined, or that has been previously validated to be of importance to the policymaker or the intelligence user. Moreover, possible political costs should be rigorously weighed against the benefits. Hence, senior policy officials must be involved in this process.

2.5.2. Analysis

Analysis is the term used for the process of *collation, analysis and evaluation* of raw and 'all-source' information and its transformation into intelligence: into warning and situation reports, analyses, assessments, estimates, and briefings.³⁹ Analysis and production are best performed close to the users of the intelligence product. In exercising collection management, analysis can draw on the collection disciplines to provide raw or processed information for evaluation, and the tailoring of the products precisely for the users' needs. These products should contain what is known (the facts), how it is known (the sources), what drives the judgments (linchpin assumptions), the impact if these drivers change (alternative outcomes), and what remains unknown. The overarching goal is to minimize the uncertainty with which policymakers must grapple in making decisions about national security and foreign policy. Analysis also must help to make sense of complex issues and to call attention to emerging problems or threats to national interests. The importance thereby is not only to determine what is accurate, but also what is relevant to the policymaker's needs.⁴⁰

³⁹ For a good coverage of analysis see: MacEachin, Douglas J. 1994. *The Tradecraft of Analysis: Challenge and Change in the CIA*. Washington D.C.: Consortium for the Study of Intelligence. And: Johnson, Loch K. October 1996. Analysis for a New Age. *Intelligence and National Security*, 11, pp. 657-671. Also: *Analysis. Directorate of Intelligence in the 21st Century. Strategic Plan*. August 1996. Washington D.C.: CIA; Unclassified; For Public Re-lease. And: Nielson, Harold. October 1995. The German Analysis and Assessment System. *Intelligence and National Security*. Vol. 10, no. 4; pp. 54-71.

⁴⁰ Davis, Jack. 1996. A Policymaker's Perspective on Intelligence Analysis. *Studies in Intelligence*. Vol. 38, no. 5; pp. 7-15. At: <http://www.cia.gov/csi/studies/95unclass/Davis.html>

Intelligence services should not satisfy requests for analysis if they know in advance that the information obtained through intelligence will provide little of relevance to the overall analysis of a subject. Neither should they accept requests when such analysis could be readily accomplished using publicly available sources, unless the expertise of intelligence analysts or of the service would add significantly to the analysis of the open source material.

2.5.3. Counterintelligence

Counterintelligence is the national effort to prevent foreign intelligence services and foreign-controlled political movements and groups, which are often supported by intelligence services, from infiltrating the state's institutions, the ranks of the armed forces and civilian departments, at home and abroad, in order to engage in espionage, subversion and sabotage.⁴¹ Moreover, targets may include citizens or residents who have no formal government affiliation. Counterintelligence also deals with acts of terrorism, regardless of whether they are initiated at home or abroad. Thus, it straddles the foreign and domestic boundary. Counterintelligence consists of offensive and defensive measures of protection; defensively through inquiries and vetting of one's own civil servants and employees, through investigations, monitoring of known or suspected agents, and surveillance activities to detect and neutralize the foreign intelligence service presence; offensively through the collation of information about foreign intelligence services and their *modus operandi*, through recruiting agents, and initiation of operations to penetrate, disrupt, deceive and manipulate these services and related organizations to one's own advantage.

Counterintelligence is an integral part of the entire intelligence process designed to make sure that what is collected is genuine, through the continuous evaluation of sources and information. It differs from intelligence gathering in that it exists to counter a threat, whether from hostile intelligence services or from non-state groups, and is thus to some degree reactive. Counterintelligence results are not generally produced in the short term, and, although a few exceptions exist, counterintelligence investigations cannot be limited to arbitrary time periods.

⁴¹ For good insights into counterintelligence see: Johnson, William R. 1994. *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer*. Bethesda, Md.: Stone Trail Press. And: Zuehlke, Arthur A. 1980. What is Counterintelligence? In: *Intelligence Requirements for the 1980s: Counterintelligence*. Godson, Roy S; ed. Washington D.C.: National Strategy Information Center. Also: Olson, James M. 2001. *A Never-Ending Necessity. The Ten Commandments of Counterintelligence*. Washington D.C.: *Studies in Intelligence*. CIA. At: http://www.odci.gov/csi/studies/fall_winter_2001/article08.html

As espionage is a crime, some counterintelligence leads to law enforcement operations. However, catching spies and uncovering foreign technical collection capabilities are more complicated activities than catching domestic and foreign criminals. The motivations and resources backing criminals are different from those backing foreign intelligence services. Criminal investigation skills, therefore, often work poorly in counterintelligence operations.⁴² Thus, while strong arguments for mixing offensive human intelligence and counterintelligence in a single organization can be made, arguments for mixing counterintelligence and law enforcement are not compelling. Even less so, since a multidisciplinary approach to collection, i.e. also exploiting SIGINT and IMINT, becomes ever more imperative for responding to today's counter-intelligence needs.

2.5.4. Covert Action

Covert actions, somewhat comparable to '*active measures*' conducted by the Soviet and other Warsaw Pact intelligence services, are activities used to influence political, military, or economic conditions and situations abroad, where it is intended that the role of one's own government will not be apparent or acknowledged publicly.⁴³ They may consist of propaganda measures, support to political or military factions within a specific country, technical and logistical assistance to other governments to deal with problems within their countries, or actions to disrupt illicit activities that threaten one's own national interests such as terrorism, organized crime or narcotics trafficking.

Covert action is an option short of military action to achieve objectives which diplomacy alone cannot.⁴⁴ Non-military covert action probably has no other logical organizational disposition except within the clandestine human intelligence collection organization.⁴⁵ Nevertheless, the overall utility of covert action is a hotly disputed issue.⁴⁶ Covert actions should only be undertaken in support of identifiable foreign policy objectives, if at all. Such actions have to complement and supplement parallel

⁴² Hulnick, Arthur S. Fall 1997. Intelligence and Law Enforcement: The 'Spies Are Not Cops' Problem. *International Journal of Intelligence and Counterintelligence*. Vol. 10, no. 3; pp. 269-286. And: Baker, Stewart L. Winter 1994/1995. Should Spies be Cops? *Foreign Policy*. No. 97; pp. 36-52.

⁴³ The CIA defines covert action as "an operation designed to influence governments, events, organizations, or persons in support of foreign policy in a manner that is not necessarily attributable to the sponsoring power".

⁴⁴ For a good account of the problem see: Berkowitz, Bruce D., & Goodman, Allan E. 2000. *Best Truth*, Chapter 5: Covert Action in the Information Age. New Haven and London: Yale University Press, pp. 124-146.

⁴⁵ Odom, William E. 2003. *Fixing Intelligence. For a more Secure America*. New Haven and London: Yale University Press, pp. 24-26.

⁴⁶ Church, Frank. January/February 1976. Covert Action: Swampland of American Foreign Policy. *Bulletin of the Atomic Scientists*. Vol. 52, no. 1; pp. 7-11. Lefever, Ernest W. Spring 1980. Can Covert Action Be Just? *Policy Review*. No. 12; pp. 115-122. Rudgers, David F. April 2000. The Origins of

overt measures of diplomacy, military activities or trade sanctions. While covert actions comprise a small part of the intelligence budget, the majority require a disproportionate share of management and oversight. The main problem is that they often create more problems than they solve. Thus, the costs of disclosure and embarrassment must be carefully assessed and, where the political costs are significant, covert actions should only be initiated by democracies in the most compelling circumstances, i.e. when the security of the state is directly threatened, when statecraft can be shown not to work, and when the potential ill effects of the action do not outweigh its possible benefits.

2.6. The Intelligence Cycle

The two main activities conducted by intelligence – *collection* and *analysis* – have to be seen in a wider perspective: one that relates these activities to the requirements and needs of the decision-makers and the use made of the finished intelligence product. This is done through the concept of the '*intelligence cycle*', which is the process by which information is acquired, converted into intelligence, and made available to policymakers.⁴⁷ The intelligence cycle usually comprises five steps: (1) *planning and direction*; (2) *collection*; (3) *processing*; (4) *production and analysis*; and, (5) *dissemination*.

(1) *Planning and direction* involves the management of the entire intelligence effort, from the identification of the need for data that is derived from the threat assessment or the priority listing of to-date unsolved strategy and policy issues, deciding which nations or groups abroad and at home warrant intelligence surveillance, to the final delivery of an intelligence product to the customer. This whole process is initiated by requests or requirements for intelligence on certain subjects based on the ultimate needs of the customer – the President, the Prime Minister, the National Security Council, ministers or other government agencies. In some cases, the requests and requirements become institutionalized.

(2) *Collection* involves the gathering of the raw data from which finished intelligence will be produced. The collection process involves open sources, secret sources, such as agents and defectors who provide information that is obtainable in no other way, and technical collection disciplines.

Covert Action. *Journal of Contemporary History*. Vol. 35, no. 2; pp. 249-262.

⁴⁷ Johnson, Loch K. 2002. *Bombs, Bugs, Drugs and Thugs: Intelligence and America's quest for security*. New York: New York University Press. p. 187.

(3) *Processing* is concerned with the conversion of the vast amount of information coming into the system to a more suitable form for the production of finished intelligence, such as language translation and decryption. The information that does not go directly to analysts is sorted and made available for rapid computer retrieval. Thus, processing also refers to sorting by subject matter as well as data reduction – interpretation of the information stored on film and tape through the use of highly refined photographic and electronic processes.

(4) *Production and analysis* refers to the conversion of basic information into finished intelligence. It includes the integration, evaluation, and analysis of all available data and the preparation of a variety of intelligence products. Such products or estimates may be presented as briefings, brief reports or lengthier studies. The ‘raw intelligence’ collected is frequently fragmentary and at times contradictory, requiring specialists to give it meaning and significance. Thus, good analysis depends upon assembling the best brains possible to evaluate events and conditions, drawing upon a blend of public knowledge and secrets purloined from adversaries. The subjects involved may concern current events, capabilities, or probable future developments, or different regions and problems, or personalities in various contexts – political, geographic, economic, scientific, military, or biographic.

(5) *Dissemination*, the final step in the cycle, involves the handling and distribution of the finished intelligence to the consumer of intelligence, i.e. the same policymakers whose needs triggered the intelligence cycle. It is a phase that is rife with opportunities for error. The information must have five essential characteristics for it to be useful: relevance, timeliness, accuracy, breadth, and purity – meaning that it is free of political spin (mis- and disinformation, propaganda, deception, etc.).

Two more phrases are mostly overlooked in the process: *consumption* and *feedback*. How, and in which form, policymakers consume intelligence and the degree to which intelligence is used are important issues. The relationship with the decision-makers should be an active and not a passive one. However, objectivity demands a certain distance and a willingness to consider all variables – not just the ones the analyst or his consumer has deemed most important in the past.⁴⁸ Though feedback rarely occurs as often as intelligence services might desire, a dialogue between the

⁴⁸ Hulnick, Arthur S. May 1986. The Intelligence Producer – Policy Consumer Linkage: A Theoretical Approach. *Intelligence and National Security Journal*, Vol. 1, no. 2, pp. 212-233. And: Haass, Richard N. 2002. Policymakers and the Intelligence Community: Support US Foreign Policy in the Post-9/11 World. *Studies in Intelligence*. Vol. 46, no. 3; pp. 1-13.

intelligence consumers and the producers should take place after intelligence has been received. Thus, policymakers should give the producers some sense of how well their requirements are being met and discuss any adjustments that need to be made to any parts of the process.⁴⁹

Like any model, this outline of the intelligence cycle is a simplification of the real world. Certain requirements can become 'standing requirements'. Policymakers are only rarely willing to specify items of information. Rather, they will indicate a desire for reports on certain situations or developments, leaving the responsibility of determining how to obtain the information required for the preparation of such reports for the intelligence services. Moreover, the intelligence services will have a certain internal need for the acquisition of information to provide for their continued operation: intelligence that will be useful in potential future operations or related to counterintelligence and security. Dissemination is the hardest part of the intelligence cycle to get right. Sharing intelligence, even within a government, is difficult due to the need to keep secret intelligence's methods and sources. Yet, getting the word out to as many responsible officials as possible is imperative for effective security and safety.

2.7. Secrecy

Transparency of the government, the state administration, and the activities of all agencies is important in a democracy, if the government wants to retain legitimacy, acceptance by, and the support of the public, the electorate and the taxpayer.⁵⁰ However, to obtain information that others would deny or keep secret, the government must rely on intelligence services that require capabilities and authorities which are unavailable to other government agencies. Intelligence services must not only use intrusive techniques, but must also have the legal power for their use. What is more, they have to do much of their collection and analysis in secret.⁵¹ Thus, secrecy is an invaluable resource. The need for secrecy means that the activities and performance of intelligence services cannot be as transparent as those of other government bodies, nor can they be subject to the same degree of public scrutiny

⁴⁹ For the 'reality' of the handling of the cycle and of consumption and feedback see: Lowenthal. op. cit., pp. 50-51.

⁵⁰ Hulnick, Arthur S. Winter 1999. Openness: Being Public About Secret Intelligence. *International Journal of Intelligence and Counterintelligence*. Vol. 12, no. 2; pp. 463-483. Robertson, K. G. 1999. *Secrecy and Open Government*. New York: Macmillan. And: Turner, Stansfield. 1985. *Secrecy and Democracy*. Boston: Houghton Mifflin.

⁵¹ Herman, Michael. 2001. *Intelligence Services in the Information Age*. London & Portland, OR: Frank Cass, pp. 4-6.

and debate. Publishing information on the allocation of resources or the successes of intelligence services would risk revealing their capabilities and targets and, in so doing, might seriously compromise their effectiveness. Thus, for intelligence services to carry out their business effectively, there are some sensitive domains of activities which have to be and to remain secret.⁵² In democracies, at least three generally agreed items of intelligence are sensitive:

1. All information pertaining to sources, operations, methods, procedures and means of collection.
2. Anonymity of the operational staff and protection of its knowledge and information.
3. Origin and details of intelligence provided by foreign services in confidence.

All intelligence services require the maintenance of secrecy on those issues. They must be able to guarantee protection of the identity of sources as well as protection of confidential information received. This must not only be for themselves and for the protection of their personnel, but also for the people from the outside world who work with the services. Secrecy is needed, because it is the only way to assure actual and potential sources of their own safety. No one will volunteer to work for an intelligence service that is unable to prevent the public disclosure of its sources.

The need for anonymity of the service's operational staff follows from the first item: sources, operations, methods, procedures and means of collection cannot remain secret, if the personnel engaged in operations are known to the public.

Intelligence services' knowledge and information need to be protected since disclosure could reveal intentions, the specific targets of the collection effort, as well as the capabilities of collection systems – disclosures that could lead to precautionary and effective countermeasures, disruption of operations, and denial of access and collection in the future. All too often intelligence successes must remain secret in order to ensure continued successful intelligence collection.

If the government is interested in, and seeks the cooperation of, its intelligence service with the intelligence services of foreign countries⁵³, maintenance of secrecy

⁵² In the US, under the National Security Act, the DCI is personally responsible for protecting the sources and methods of US intelligence.

⁵³ Richelson, Jeffrey T. & Ball, Desmond. 1985. *The Ties That Bind: Intelligence Cooperation among the UKUSA Countries*. Boston: Allen & Unwin. And: Wylie, Neville. July 1996. *Keeping the Swiss Sweet*:

of the origin and the content of information, intelligence and assessments provided is essential. All documents and carriers of intelligence remain the property of the nation providing them and cannot be further disseminated without its permission. Since intelligence information has to be made available to those foreign services under arrangements for intelligence sharing, maintenance of secrecy is equally expected from those foreign services. Hence, it is necessary to establish clear guidelines and rules for the classification, distribution and archiving of, as well as access to intelligence, with respect to citizens, one's own, and foreign government agencies.

However, not everything ought to be protected and kept secret. Only to the extent that disclosure compromises or degrades sensitive intelligence sources and methods, does intelligence disclosure become self-defeating. While publicity about intelligence, both factual and fictional, is rampant, in liberal democratic states the public believe that governments still classify too many documents and keep too many secrets. In an open society, the will of the people cannot be obstructed for long without some consequences. By far the most effective manner of accomplishing the task of public education is by letting the public benefit directly from the products of intelligence, its information and assessments. Thus, nowadays in the US official intelligence publications, some of which are extremely valuable, are available for sale to the public. Many intelligence services have web-sites on the Internet, with steadily increasing content.⁵⁴ Countries which have established codes of ethics for intelligence services present these on the web. It is obvious that not all intelligence services can offer the public data like the "*World Fact Book*" of the CIA on their official web-site⁵⁵, despite this being much used and highly appreciated in the academic world: only big services have the resources to keep such data up-dated. Nonetheless, even smaller services could sanitize some of their products and assessments of current interest, and make them available to the public, particularly when such publications can help to factually clarify controversial issues, developments, events, and government's position.

In addition to a favourable public attitude towards intelligence, which is both desirable and needed in democracies, public collaboration is also important. By providing the

Intelligence as a factor in British Policy towards Switzerland during the Second World War *Intelligence and National Security*. Vol. 11, no. 3; pp. 442-467.

⁵⁴ See for example: The U.S. Central Intelligence Agency (<http://www.cia.gov/>). The British Security Service (MI5) (<http://www.mi5.gov.uk/>). The German Bundesnachrichtendienst (<http://www.bundesnachrichtendienst.de/start.htm>). The Canadian Security and Intelligence Service (<http://www.csis-scrs.gc.ca/>) and the Russian Intelligence Service (<http://www.fsb.ru/>).

⁵⁵ See: <http://www.cia.gov/cia/publications/factbook/goes/af.html>

public with a telephone, fax and e-mail number, services can encourage significant public support.

2.8. The Missions of Intelligence Services

Traditionally, democratic states separate *internal* and *external* security, and thus also divide internal and external intelligence services. This can be justified by different categories of intelligence, by the fact that different rules and laws apply to intelligence operations on national soil and abroad, and by different missions.

2.8.1. The Mission of Internal Intelligence Services

Whilst the task of *internal intelligence* is generally to obtain, correlate and evaluate intelligence relevant to internal security, the missions may vary depending on the country. Almost all internal intelligence services have a common primary mission which is to provide support and assistance to the police and other law enforcement agencies, criminal justice, customs and border guards, and other regulatory agencies of the state. This is achieved by collecting *security intelligence* and building up a detailed body of knowledge for the prevention and countering of covertly organized threats, acts, and activities in the following domains:

- espionage⁵⁶
- sabotage and subversion⁵⁷
- terrorism
- political, ethnic, and religious extremism
- organized crime⁵⁸
- narcotics production and trafficking

⁵⁶ Including economic espionage, which can be defined as the use of, or facilitation of, illegal, clandestine, coercive or deceptive means by a foreign government or its surrogates to acquire economic intelligence? Economic espionage exposes the targeted state's companies to unfair disadvantages, jeopardizing the jobs, competitiveness of the state, and hampering its R&D investment.

⁵⁷ Includes covert, unlawful acts which are directed towards the destruction or overthrow of the constitutionally established system of government and activities which are directed against it by unconstitutional means.

⁵⁸ The UN estimates the place and cost of various trans-national criminal activities in developed states at 2% of their GNP which, in 1998, led to organized crime being labelled as one of the three major challenges facing the world today.

- money faking and money laundering
- proliferation of weapons of mass destruction
- illegal arms dealing
- illegal immigration
- arms and other smuggling
- electronic attacks, hacking, and dissemination of child-pornography, etc.

Often, internal intelligence services also have a mission to conduct background security checks on, or to do the vetting of, nominees for sensitive government positions.

In carrying out their mission, internal security services draw on the following principal sources of secret intelligence: (1) interception of communications, (2) eavesdropping, which involves covertly monitoring the speech of targets under investigation, (3) own agents within the target organization, and (4) surveillance.

2.8.2. The Mission of External Intelligence Services

While the task of *external intelligence* is generally to obtain, correlate and evaluate *foreign intelligence* relevant to *external security* and for warning purposes, the missions vary from one country to another. External intelligence services must take into account changing needs and aspirations of governments, as well as national realities and requirements. However, certain core missions are common to almost all services. These are:

Support of Security Policy and Foreign Policy

Support of security and foreign policy decision-makers will continue to be the principal mission for external intelligence services. This entails providing advance warning of developments that will or could affect national security or national interests in time to frame an appropriate response and, in particular, to avoid crises and conflicts that might require the use or intervention of the armed forces. Foreign intelligence is critical for determining which of several options, steps and measures may be most effective in achieving national security and foreign policy objectives.⁵⁹

⁵⁹ See: Shpiro, Shlomo. December 2002. *Stabilität im Nahen Osten? Der Beitrag der Geheimdienste zur*

Foreign intelligence can also be instrumental for assisting diplomatic initiatives in bilateral and multilateral treaty negotiations.

Detection of Activities Abroad That Threaten Security and National Interests

An equally important mission of external intelligence is to focus on identifying existing or developing risks, dangers, and opportunities abroad, in particular of 'transnational activities' which could threaten the lives of nationals, means of transport and installations abroad, and national interests. Good and timely foreign intelligence, especially on the activities of terrorist groups, proliferators⁶⁰, international organized crime, and narcotics producers and traffickers, can serve as the basis for diplomatic initiatives, other national responses, or countermeasures. Moreover, it can frequently be key to the efforts of other governments to disrupt such activities or to bring them under control.⁶¹

Information Warfare

External intelligence is ever more necessary to support the task of ascertaining superiority, if not dominance, in 'Information Warfare',⁶² as well as providing protection against electronic attacks. This mission has grown with the explosion in information systems and information technology and will become increasingly important. Information warfare refers to offensive and defensive activities undertaken by governments, groups, or individuals to gain electronic access to information systems in other countries, either for the purpose of obtaining data in such systems, manipulating, or fabricating such data, or bringing the systems down, as well as protection against such activities.⁶³ Government and public telecommunications, transportation, financial transfers, water, energy, power supplies, and other industrial systems have become critically dependent on a complex set of interconnected automated information and control systems. Many of these systems are potentially vulnerable to computer-based disruption, manipulation, or corruption by hostile

Konflikt-prävention. *Internationale Politik*, No.12, pp. 39-44.

⁶⁰ Sokolski, Henry. Spring 1994. Fighting Proliferation with Intelligence. *Orbis*. Vol. 38, no. 2; pp. 245-260.

⁶¹ Johnson, Loch K. 2002. *Bombs, Bugs, Drugs and Thugs. Intelligence and America's quest for security*. New York: New York University Press; pp. 19-22, 44.

⁶² *Information Operations*. 15 June 2000. US Army Field Manual FM 100-6. Washington D.C.: US Department of the Army. And: Fairbanks, Walter P. June 1999. *Information Superiority: What Is It? How to Achieve It?* Research Report. Cambridge MA: Harvard University. Center for Information Policy Research.

⁶³ Arquilla, John. Summer 1994. Strategic Implications of Information Dominance. *Strategic Review*. Vol. 22, no. 3; pp. 24-30.

individuals, groups, or countries.⁶⁴ While the scope of actions required to deal with the protection of computer networks in the public and in the private sector would exceed the capabilities of intelligence services, the collection of intelligence on information warfare threats from abroad is the basis upon which to build an effective governmental structure to coordinate efforts for the protection of the critical national infrastructure.⁶⁵

Support to Defence Planning

External intelligence will continue to support defence planning, which entails providing intelligence on foreign capabilities in order to shape the size, nature and disposition of the armed forces and to guide military R&D and future military acquisition decisions.⁶⁶ This also includes necessary intelligence about foreign military doctrines, operations, tactics, combat techniques, and weaponry performance to train and protect the armed forces.

Support for Military Operations

One traditional mission of external intelligence is providing support to operations of the armed forces, which encompasses not only warning of any attack on national space, territory and infrastructure, but also providing intelligence required for planning and carrying out military operations of all kinds. Whilst in the past it largely consisted in providing order of battle information on opposing forces, this mission has been expanding to an ever more complex task. Due to the rapidly changing nature of warfare, the main mission has become to ensure transparency of the battlespace and targeting support for stand-off weaponry of pinpoint precision in order to win wars ever more quickly – which tends to reinforce an intelligence process that has increasingly shifted resources and attention towards support for war fighters and away from critical but longer-term problems. This raises the question of the proper

⁶⁴ House of Commons. Defence Committee. 24 July 2002. *Defence and Security in the UK*. Sixth Report of Session 2001-02. Volume I: Report and Proceedings of the Committee. London: The Stationary Office Limited. 93 pp.

⁶⁵ There are legal and ethical issues that have yet to be resolved, including how to discern between international and domestic cyber attacks – differences that dictate which intelligence or security service would respond and the rules governing that response. In most western countries, policymakers and implementers alike are still struggling with the legal aspects and rules of engagement regulating information operations. One particularly dicey issue is how to conduct computer network attacks whilst limiting potential unintentional consequences against non-combatants – a key restraint under international law. However, true defense against a determined cyber terrorist may not be possible unless the system being defended is able to strike back once an imminent attack is detected. Lowenthal. *op.cit.* p. 200.

⁶⁶ Herman, Michael. December 1998. Where Hath our Intelligence Been? The Revolution in Military Affairs. *RUSI Journal*, No. 143.

balance between strategic intelligence geared to cross-cutting threats such as terrorism, and tactical intelligence that directly supports the military. However, while force protection and support of forces in, or with the prospect of, combat are of the highest priority, and in the future it will become much more important to have intelligence that enables the goals to be achieved, yet avoids any commitment of military forces – hence, victory without war. Even more demanding, a ‘fourth-generation warfare’⁶⁷ is manifesting itself in highly compartmentalized, cellular, predatory adversaries. Loose coalitions of terrorists, criminal actors, guerrillas, insurgent warlords, and rogue regimes operating in networks outside the framework of traditional nation-states will challenge national security capabilities that were designed to operate within that framework. Urban operations, crime, and terrorism will be part of the same operational environment. Emerging and mutating into a form which blurs distinctions between peace, war, crime, civil and criminal, combatant and non-combatant, fourth-generation warfare moves beyond terrorism, suggesting that terrorism will take advantage of that type of warfare’s three main characteristics: the loss of the nation-state’s monopoly on war; a return to a world of cultures and nation-states in conflict; and internal segmentation or division along ethnic, religious, and special-interest lines within societies. This adds to the complexity of threats. Intelligence will be the foundation for determining the kind of war a state might be entering and thwarting those who would undermine national and international security.

Economic Intelligence

The collection and analysis of economic data is another traditional mission of external intelligence services.⁶⁸ Since liberal democratic policy and practice prohibit intelligence services from engaging in industrial espionage and from clandestinely collecting trade secrets and proprietary information of foreign commercial firms to benefit private firms in one’s own country⁶⁹, activities have to focus on those areas

⁶⁷ Lind, William S.; Schmitt, John F., Major, and Wilson, Gary I., Colonel. December 1994. Fourth Generation War-fare: Another Look. *Marine Corps Gazette*; pp. 34-37. And: Gould, Harold A. & Spinney, Franklin C. October 15, 2001. Fourth-Generation Warfare Is Here. *Defense Week*. Also: Richards, Chester W. May 2001. *A Swift, Elusive Sword. What if Sun Tzu and John Boyd did a National Defense Review?* Washington D.C.: Center for Defense Information.

⁶⁸ Porteous, Samuel D. Fall 1995. Economic/Commercial Interests and the World’s Intelligence Services: A Canadian Perspective. *International Journal of Intelligence and Counterintelligence*. Vol. 8, no. 3; pp. 275-306. And: Zelikow, Philip. January 1997. American Economic Intelligence: Past Practice and Future Principles. *Intelligence and National Security*. Vol. 12, no. 1; pp. 164-177. Also: Johnson. *Op. cit.* pp. 32-41.

⁶⁹ Augustini, Jeff. Winter 1995. From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA For Economic Espionage. *Law and Policy in International Business*. Vol. 26, no. 2; pp. 459-496.

that could affect national interests. These include energy and other resources, related economic problems, foreign economic potentials and conditions, worldwide economic trends, as well as obtaining intelligence to support trade negotiations. Although much more data is now widely available, there are countries where such information is still restricted, unavailable, or unreliable. Furthermore, there are situations abroad where the availability of energy resources and the stability of the currencies can be influenced by the actions of foreign governments or groups, or where the nation's commercial firms are put at a competitive disadvantage in obtaining contracts with foreign governments. The latter is often a result of unfair trade practices or unscrupulous actions like bribery and 'kickbacks' undertaken by foreign competitors, or where a foreign government is otherwise involved in the transaction. In these cases, intelligence can be crucial to decision-making and for diplomatic action with the governments concerned to correct the situation. Identifying such situations and activities abroad is a legitimate mission for external intelligence. However, the collection and analysis of economic intelligence remains a mission that requires particularly close coordination between producers and consumers of intelligence in order to ensure that the intelligence contribution adds value.⁷⁰

Support to Monitoring of Treaties and Other Agreements

External intelligence is also essential for monitoring treaties, agreements⁷¹, and all kinds of sanctions to which the state is party or which are of national interest, and to gauge their effectiveness. This involves tracking the activities of individual foreign trading and transport companies, including their ties to international banks and their use of various communications channels.⁷²

In carrying out their mandates, external intelligence services draw on all possible and available sources and the full range of techniques of secret intelligence.

2.9. The Organization of Intelligence Services

Historically, democracies have striven to maintain a clear distinction between external and internal security. The basic concept has been that internal challenges can, and, for the preservation of the democratic system must, be met by institutions

⁷⁰ Porteous, Samuel D. Fall 1996. Looking Out For Economic Interests: An Increased Role For Intelligence. *The Washington Quarterly*. Vol. 19, no. 4; pp. 191-206. And: Lowenthal. op.cit. pp. 196-197.

⁷¹ Scalingi, Paula L. October 1995. Proliferation and Arms Control. *Intelligence and National Security*. Vol. 10, no.4; pp. 149-161.

⁷² Shulsky, Abram N. 1987. Intelligence and Arms Control Policy. *Comparative Strategy*. Vol. 6, no. 2;

and processes that are themselves governed by laws – broadly accepted by the society and understood as limiting government as well as citizens – and subject to controls of public accountability and openness.

For internal intelligence, the criterion for surveillance and investigation in a free society is the question of violence. Internal intelligence is justified in targeting an organization if it, or its influence, has led to violence, or if there is a reasonable expectation that it will. However, the application of law and the exercise of executive power against violence is the field of law enforcement alone. Coordination and cooperation between these organizations has to be ensured at the ministerial level.

Whilst the distinction between internal and external intelligence services has never been absolute, and whilst some threats – such as terrorism, organized crime, drug trafficking, and smuggling – have long been recognized as combining domestic and foreign elements, one of the defining characteristics of constitutional democracy has been limiting the role of external intelligence services, and methods of operations characteristic to them, in internal issues of law enforcement and in the political life of the country. This is precisely because of the danger that the practices of external intelligence could infect the law-based norms of internal intelligence.

Counterintelligence is an intrinsic mission for each of the intelligence services. There is no need for an independent counterintelligence service⁷³, which might tend to become another bureaucracy interfering, delaying, disrupting and attempting to usurp the counterintelligence functions of each of the services. However, there may be a need for a centralized counterintelligence program, the purpose of which is to integrate, promote, improve and coordinate the counterintelligence operations, investigations and research of each of the services.

Close cooperation of both external and internal intelligence services is required, if the counterintelligence effort is to be effective. For example, a group of extremists carrying out armed attacks may be planning those attacks within the country, and seeking to develop operational intelligence to support this policy (internal intelligence), but could be supported from a neighbouring state where the group carries out its training and planning (external intelligence). A centralized counterintelligence program establishing authoritative coordination and cooperation between the internal and external intelligence service on counterintelligence matters, which

pp. 145-164. And: Lowenthal. Op. cit. p. 159.

⁷³ For another view see: Odom. Op. cit. pp. 167-184.

inevitably cross borders, will preserve the legitimate jurisdictional demarcation between domestic and external counterintelligence responsibilities.

Different intelligence needs often lead to the creation of several services instead of one comprehensive organization. The ministry of defence will often have an intelligence service of its own⁷⁴, concerned with more technical issues such as the assessment of the military potential of neighbouring states, defence industries, military personalities, etc. In order to determine its own requirements in weapons, the ministry intelligence must know the nature of potential hostile forces as well as the characteristics of the target base.⁷⁵ Size, capabilities, location and readiness of those forces must be continually monitored – either as a guide to planning requirements or as a means of warning against possible attack. Much of this information is also important in the negotiation and for the monitoring of arms limitation agreements. Hence, *Defence or Military Intelligence* can also be viewed as a third natural branch in addition to external and internal intelligence.⁷⁶

Different collection methods, especially using sophisticated technical means, can also give rise to specialized intelligence organizations. These include imagery, signal and cryptology intelligence agencies. The US NSA⁷⁷, the Russian FAPSI⁷⁸, and the British GCHQ⁷⁹ are the biggest and probably most expensive of their intelligence agencies.

Since risks, dangers and threats are of expanding transnational reach and impact, ever more information is collected by different services and means on the same subjects. The traditional limits between external, internal, and also police intelligence, are becoming increasingly blurred. The missions and objectives overlap, enhancing the opportunities for misunderstandings and rivalries. There is convergence, notably

⁷⁴ Eberbach, Heinz-Eugen. 2002. Neuorientierung des Militärischen Nachrichtenwesens der Bundeswehr. *Europäische Sicherheit*. No. 10; pp. 13-21.

⁷⁵ See: *Vision 2010*. A Strategic Plan for the Defense Intelligence Agency.

⁷⁶ Odom. Op. cit. pp. 89-114. And: Schmitt, Gary. June 24-30, 1996. Pentagon Needs Own Spies: Military Requires Personal Intelligence Touch. *Defense News*; p. 45.

⁷⁷ *National Security Agency*, housing the biggest and most sophisticated computer complex in the world at its HQ in Fort Meade, Maryland. See: Bamford, James. 2001. *Body of Secret: Anatomy of the Ultra-Secret National Security Agency – From the Cold War through the Dawn of a New Century*. New York: Doubleday. And: Aid, Matthew M. Autumn 2000. The Time of Troubles: The US National Security Agency in the Twenty-First Century. *Intelligence and National Security*. Vol. 15, no 3; pp. 1-32.

⁷⁸ Successor to the Soviet SIGINT organizations of both the KGB and the GRU, which consisted of 40 SIGINT regiments, 170 SIGINT battalions and over 700 SIGINT companies, using SIGINT Satellites, more than 60 ships, aircraft of different types and some 500 SIGINT ground stations, and employed about 350'000 intercept operators, processors, cryptanalysts and other technical specialists, the majority of them military personnel. Recently reorganized again.

⁷⁹ *Government Communications Headquarters* in Cheltenham with two missions: SIGINT and Information Assurance. See also: *About GCHQ > FAQ. Frequently Asked Questions*. At: <http://www.gchq.gov.uk/about/index.html>

in countering terrorism and organized crime. Hence, the separation of internal and external intelligence services is becoming more artificial, and thus questionable. Another type of cooperation seems to be necessary at the European and the international level.

While separation might still be a good solution for greater powers with many huge intelligence services, it will require an ever greater effort for coordination and control, better regulated access to each other's information, and assurance of the production of *joint assessments*. This is why smaller countries with fewer resources might prefer to have just one intelligence organization. This avoids wasting efforts, resources and time; solves the risk of unhealthy competition between different agencies; simplifies contacts, information-exchange and cooperation with foreign intelligence services; facilitates high subordination of intelligence in the state's hierarchy and hence co-operation and coordination with other ministries and government agencies; and it also alleviates control and oversight of intelligence. Amongst others, the Spanish CNI⁸⁰ and the Dutch AIDV⁸¹ are examples of democratically controlled 'fused' intelligence services, which have found their own solutions to overcome the problem that different rules and laws apply to intelligence operations on national soil and abroad.

However, it is a good rule that intelligence must be separate from law enforcement. Law enforcement and intelligence have fundamentally different purposes. Whilst the goal of law enforcement is to get a conviction in a specific criminal case, the task of internal intelligence is to collect as much information as possible on potential threats to the state and society. The internal intelligence service thus might prefer not to arrest an identified criminal if this would harm its capacity to collect further information. Intelligence services might also not want to divulge their information in an open judicial process for fear of betraying the sources of their information.

The function of criminal intelligence, however, does require skills which are similar to those used by intelligence agencies. In certain circumstances, targets of internal intelligence services might also be involved in organized crime, so the interests of two organizations would overlap. Yet intelligence services usually have no authority to conduct criminal investigations, no power of arrest, and no power to search homes. Hence, when it is clear that a crime has been committed, the collection of

⁸⁰ Formerly the *Centro Superior de Información de la Defensa (CESID)*, now *Centro Nacional de Inteligencia (CNI)*.

evidence and execution of arrests should be carried out by a specialist branch of the police force.

Nonetheless, the requirements of national security and protection of the state may occasionally be at odds with established concepts of privacy, civil liberties and civil rights that the same state grants its citizens.⁸² Clearly, if domestic intelligence services had no special powers, they would find the protection of the state very difficult. Conversely, domestic services with unlimited powers might find the protection of the state easy, but this would cause unacceptable damage to the rights, civil liberties and privacy of citizens.

In a democratic state, a trade-off between these diverging interests has to be found in a manner that is politically and legally sound. This implies a conscious decision about what is permitted and what is not. The government must therefore lay down general principles for what is acceptable, ensure that these principles are transparent, known to the public, and adhered to by the intelligence services. Comparable considerations apply, in a different fashion, to external intelligence services.

3. The Legal Framework

The ability to control information is an important power in any state, whether democratic or despotic. Since the collection of information that is unavailable by any other means, restricted and controlled dissemination of the knowledge gained from it, and operating behind a cloak of secrecy is the mainstay of intelligence, such services are always suspected to have the potential to become a threat to the government and other actors in a democracy. Intelligence services may provide a means of detecting and averting potentially dangerous situations, but they can also be misused as a means of secretly bringing pressure to bear. Thus, controlling and overseeing intelligence effectively is important.⁸³

In a modern democratic society, there is a need for a system of checks and balances to ensure compliance with the laws governing the activities of intelligence services.⁸⁴

⁸¹ *Algemene Inlichtingen - en Veiligheidsdienst*.

⁸² Strickland, Lee S. 2003. Civil Liberties vs. Intelligence Collection: The Secret Foreign Intelligence Surveillance Act Court Speaks in Public. *Government Information Quarterly*. Vol. 20, no. 1; pp. 1-12.

⁸³ "Sed quis custodiet ipso custodes?" – but who will guard the guards? – in the times of the old Roman Empire, the poet and satirist Juvenal had already asked this. Also: Dedijer, Stevan. June 1978. Watching the Watchmen: Parliaments and National Intelligence Services. *Bulletin of the Atomic Scientists*. Vol. 34, no. 5; pp. 40-43.

⁸⁴ Webster, William H. September 1988. The Role of Intelligence in a Free Society. *University of Miami*

While it is the task of the executive power to supervise their management and that of the judicial power to sanction any cases of non-compliance with the law, it is up to the legislative power to provide the legal framework for intelligence and to scrutinize their compliance with the law.⁸⁵

Democratic control of intelligence services should begin with the enactment of a clear and explicit legal framework. Since in democracies, oversight⁸⁶ is a shared responsibility and since the concept of legislative oversight normally is established in the state's constitution, ideally the role of intelligence should also be defined in the constitution, representing the apex of the system.

The essence of legislative oversight is the ability to gain access to information, usually held by the executive, which is relevant to the functioning of the government. The specific circumstances of each country determine the type of scrutiny exercised by the parliament.⁸⁷ Parliamentary chambers have various powers of information and scrutiny, allowing them to supervise the activities of their government. Control over the budget for the entire government is the most fundamental lever of legislative oversight. In reviewing the budget submission and crafting alternatives or variations, the legislative gets to examine the size and shape of each ministry and agency, the details of each program, and the plans for spending money. No other activity offers the same degree of access or insight. Other powers may take the form of questions, resolutions, inspections, inquiries, or study missions. Such classical methods of scrutiny are to be found in practically all modern parliaments of truly democratic states. These powers are set down in the rules of procedures of the legislative, and can be executed in open or closed sessions. In Europe, the Assembly of Western

Law Review. Vol. 43; pp. 155-162.

⁸⁵ This is a problem which was brought to the attention of European countries at the OSCE Summit in Budapest in 1994, at a time when the new eastern European republics were in the process of establishing their democratic institutions, when the states that signed up to the Code of Conduct on politico-military aspects of security recognized "the democratic political control of military, paramilitary, and internal security forces as well as of intelligence services and the police to be an indispensable element of stability and security". See also: Leigh, Ian. August 2002. *Democratic Control of Security and Intelligence Services: A Legal Framework*. DCAF Working Paper No. 115. At: http://www.dcaf.ch/publications/Worling_Papers/115.pdf And: Born, Hans & Tuler, Matias. 2002. *Parliamentary Democracy and Intelligence. Comparing Legal Frameworks of United Kingdom, Canada, Ukraine, Czech Republic, Turkey and South Africa*. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, held in Geneva 3-5 October, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

⁸⁶ Oversight has two definitions that are distinct, if not opposites: (1) supervision or watchful care – as in "we have oversight of that activity". (2) failure to notice or consider – as in "we missed that. It was an oversight". In overseeing intelligence, the legislative and the executive try to act in the sense of the first definition and to avoid acting in the sense of the second. See: Lowenthal. Op. cit. "A Linguistic Aside: The Two Meanings of Oversight". p. 154.

⁸⁷ Farson, Stuart. Summer 2000. *Parliament and Its Service: Their Role in Scrutinizing Canadian Intelligence*. *Intelligence and National Security*. Vol. 15, no. 2; pp. 225-258.

European Union (WEU) adopted a recommendation calling “for the definition of a proper European intelligence policy for which the member states must define harmonized national policies and create more similar national intelligence structures”.⁸⁸

In order to establish intelligence organizations in state statutes, national law should be enacted defining:

- The basic missions of the intelligence services⁸⁹;
- the areas of responsibilities of these services;
- the limits of their competences;
- the methods of operation and the restrictions imposed on their activities⁹⁰;
- the organizational structures in general;
- the relations among the intelligence and security services associated in an intelligence community;
- the means by which the services will be controlled and held accountable⁹¹;
- the mechanisms of executive and judicial control and supervision, and of legislative oversight; as well as,
- the legal means provided to deal with complaints in cases of violation of rights.

The law has to set limitations which, in addition to data protection and other applicable laws, achieve the proper balance between security and individual freedom, between the collective interests of society and the protection of rights of

⁸⁸ Recommendation 707 adopted in June 2002. For a stock-taking see also: WEU. 4 December 2002. *Parliamentary oversight of the intelligence services in the WEU countries – current situation and prospects for reform*. Paris. Forty-Eighth Session. Document A/1801.

⁸⁹ Bowman, M. E. Fall 1995. Intelligence and International Law. *International Journal of Intelligence and Counter-intelligence*. Vol. 8, no. 3; pp. 321-335. And: Damarest, Geoffrey B. Spring 1996. Espionage in International Law. *Denver Journal of International Law and Policy*. Vol. 24, no. 2/3; pp. 29-51.

⁹⁰ See: Recommendation by the Council of Europe Parliamentary Assembly (1402/1999) stating that the law should regulate “which kinds of operational activities carrying a high risk of violation of individual rights may be used in which circumstances (...)”.

⁹¹ See also the project of a model law on intelligence oversight Dr. Hans Born, Geneva Centre for the Democratic Control of Armed Forces (DCAF) is preparing, and which will be derived from an international seminar on intelligence oversight at the Norwegian Parliament, Oslo, 19-20 September 2003. At: www.dcaf.ch/legal/intro.htm. The model law will compare the legislative and executive oversight mechanisms of Argentina, Germany, Norway, Poland, South Africa, South Korea, the US, and the UK.

individual citizens⁹², and the acquisition of essential information. Ideally, the law should not be construed as authorizing any illegal activity nor should it, if possible, provide exemptions from any other law.

Dependent on the subordination of the intelligence services, the president, the prime minister, or the ministers responsible must have responsibilities under the law. In addition, each intelligence service has to have a statutorily defined relationship with their superiors and a legally defined position in relation to them.

Since laws cannot be changed frequently, and, in democracies, are not likely to be modified rapidly, statutes or acts should only regulate the enduring or longer lasting aspects of intelligence services. However, a system of statutory regulation, coordination and control is needed to guide intelligence work. The statutory regime should not only have a bearing on how services collect and administer intelligence, but also on how they must use it. Services should be accountable for the ways they use intelligence. The statutory regulation should define what information is sensitive, deal with classification levels and authority⁹³, downgrading and declassification, safeguarding and archiving⁹⁴ of classified information, etc. Moreover, intelligence services have to protect sources and methods from unauthorized disclosure if the disclosure would lead to loss or harm of life, or loss of intelligence capability. What is essential is that a defensible standard for withholding information must be set, and it must be subject to independent judicial review.

In addition to the law, *executive orders* or *ordinances* can be used to define functions, organizational matters, list particular duties and responsibilities, establish procedures, coordination measures, define and specify assistance, cooperation, and liaison among the intelligence and security services as well as with ministries, agencies, and foreign intelligence services, regulate need-to-know issues, the dissemination and the sharing of intelligence, and impose restrictions on access to the services, etc.

Moreover, there is a need for *directives* and *ministerial* or *agency regulations* by which all those subjects more prone to rapid modifications can be regulated, such as:

⁹² Salinas, Carlos M. 1998. Human Rights and Intelligence Reform. *Foreign Policy in Focus*. Vol. 3, no. 20; pp. 1-4.

⁹³ In the US, classification is currently based on Executive Order 12958. 'Classified National Security Information', issued in April 1995, amended with Executive Order 13142 in November 1999.

At: http://www.archives.gov/isoo/rules_and_regulations/executive_order_12958.html

⁹⁴ Aldrich, Richard J. 1995. British and American Policy on Intelligence Archives. *Studies in Intelligence*. Vol. 38, no. 5; pp. 17-26. And: Wark, Wesley K. March 1992. In *Never-Never Land?: The British*

- Collection and analysis requirements;
- objectives and priorities of the intelligence services;
- plans and programs;
- training, visits and travel; and,
- resource allocation, etc.

Such *directives, ministerial or agency regulations* can be established in two varieties: unclassified and – where appropriate and needed – classified.

Finally, '*freedom of information legislation*' might be called for, which requires establishing rules related to public access to information.⁹⁵

4. Democratic Control of Intelligence Services

A state's system of 'democratic control' is the product of its system of government, politics, history, and culture. Arrangements that match the legal and constitutional traditions of the home country are needed, and not necessarily those that appear the most attractive from another. In the same way that there are many different political systems and cultures, many different norms and practices of 'democratic control' exist.⁹⁶ There is no single model for 'democratic control', neither is there a definitive normative model for democratic control of intelligence services.

Regardless of the particular form of control adopted in democracies, direct and most relevant 'democratic control' of intelligence services and their activities is exercised by executive, legislative and judicial entities. Every element plays its specific role within the whole package of control, accountability, supervision and oversight, the purpose of which is to provide *assurance of legality, proportionality and propriety* for activities that are necessarily conducted in secret.⁹⁷

Archives on Intelligence. *The Historical Journal*. Vol. 35, no. 1; pp. 195-204.

⁹⁵ See: Freedom of Information Act in the US and in Canada. And: Wark, Wesley K. Prof. October 2002. *Canada's Access to Information Act and the Canadian Security and Intelligence Community*. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, held in Geneva 3-5 October, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

⁹⁶ Rindskopf, Elizabeth R. 1988. Intelligence Oversight in a Democracy. *Houston Journal of International Law*. Vol. 11, no. 1; pp. 21-30.

⁹⁷ Caparini, Marina. 2002. *Challenges of control and oversight of intelligence services in a liberal*

Within these packages, executive control and supervision plays the decisive role. The higher the echelon of executive control and supervision, and the greater the seriousness with which it executes its tasks, the lesser the likelihood of problems accruing to the government from judicial supervision and legislative oversight. It is the executive which is fully responsible for the proper controls and auditing of the intelligence services, thus creating the necessary base for transparency and parliamentary oversight.

Countries influenced by the British Common Law tradition, tend to emphasize the judicial aspect of control, whereas in continental Europe and in those countries that have experienced repressive powers of intelligence services at some point in their recent history, more legislative oversight is favoured. Most democracies have implemented some degree of legislative oversight. Some parliaments may actively exercise oversight functions, requesting reports and briefings, while others may receive a ministerial report or briefing only in the context of the annual budget vote, or not at all. While few countries come close to providing the degree of legislative oversight that the US and Germany have, France has yet to let parliament participate in the oversight of the intelligence services.⁹⁸ Others, like Norway, have an independent committee for the monitoring and supervision of intelligence, surveillance and security services⁹⁹, the members of which are elected by parliament. The committee reports to parliament in the form of annual and special reports. It also deals with complaints from private individuals and organizations that believe that the secret services have committed injustices against them. In Canada too, parliamentary involvement is limited. The only body specifically designed for and assigned to the task of ongoing external review in the intelligence community is the Security Intelligence Review Committee of no less than three, and no more than five Privy Councillors, who are not sitting members of parliament. They have two mandates: to provide an external review of the Canadian Security Intelligence

democracy. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, held in Geneva 3rd-5th October, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

⁹⁸ Parliamentary oversight will soon be established. See: Faupin, Alain, Major General (ret). 2002. Reform of the French Intelligence Services after the End of the Cold War. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services', held in Geneva 3rd-5th October, organized by the Geneva Centre for the Democratic Control of Armed Forces. And : Denécé, Eric. Mars 2001. Le contrôle parlementaire des services de renseignement. Interview d'Arthur Paecht, député du Var, vice-président de la Commission de la Défense et des Forces armées à l'Assemblée nationale. Paris : L'Harmattan. *Renseignement & Opérations Spéciales*. No. 7; pp. 21-28.

⁹⁹ Committee for Monitoring of Intelligence, Surveillance and Security Services, responsible for the supervision of the Norwegian Police Security Service, the Norwegian Defence Security Staff and the Norwegian Intelligence Service = the EOS services. The 7 members conduct their work independently of parliament (Storting) and parliamentarians are not permitted to be members.

Service (CSIS), and to examine complaints concerning security clearances, immigration, citizenship and other matters involving CSIS investigations.

A number of countries have created an *Ombudsman* institution¹⁰⁰, a method of controlling the administration, which generally relies on the legislative for its effective operation; often confirmed by, and accountable to parliament. The Ombudsman can be given powers to investigate alleged violations of human rights by intelligence services, to negotiate with civil servants, to report to the legislature, and to inform the public about the results of the inquiries. Though he does not normally have the ability to issue administrators with binding judgments, the Ombudsman may make suggestions to the legislature that further action be pursued, such as providing redress for a citizen regarding legitimate grievances, or general suggestions for improving procedures and policies. Whilst being an officially sanctioned institution, the Ombudsman is generally free of most bureaucratic impediments and constraints, enjoys access and credibility by other branches of government, and provides a platform for the people.

In addition, though more as an informal mechanism of supervision, vibrant, responsible and independent media, and other actors within civil society, have a role to play.

The organization and the mechanisms of executive control and accountability, of legislative oversight, and of judicial control and supervision will be presented, and the role informal and indirect supervision by the public can play will be briefly sketched. There will be no definitive answers to such questions as: How much intelligence is enough? How much oversight is needed? What is the proper balance between liberty, security and safety? When should legislators, the media, or the public be supportive or openly critical of sensitive intelligence operations? In some way, answers will always be dependent on the personalities and conditions of the times.

4.1. Executive Control and Accountability

However necessary it may be, secrecy needed for intelligence activities creates a scenario for the potential or perceived abuse of intrusive powers by intelligence

¹⁰⁰ The Ombudsman originated in Scandinavian countries. Ombudsmen are now found in many other countries: Hungary and Poland; the UK and New Zealand; Israel; India; Japan. In Canada, exceptionally, there are a number of specialized Ombudsmen: Prison, Transportation, Human Rights Commission, Privacy Commission, and the Official Languages Commission. In the US, Ombudsmen are also found at the State and Provincial level of government. See: Caparini, Marina. 2002. *Setting up Mechanisms for Democratic Oversight (of the Security Sector)*. Session on Accountability. Tools for

services, as well as the perception that inadequate attention may be given to obtaining value for the money spent. To gain the benefits and avoid the risks, *control* and *accountability* arrangements must balance, and be seen to balance the need to protect and promote national interests with the need to safeguard individual rights and freedoms. At the same time, these arrangements need to ensure an appropriate focus on achieving their desired results.

Control, in the narrowest sense, means ensuring that specific procedures are followed. In the broadest sense, it means creating the conditions that lead to the achievement of agreed standards of performance, including the desired results as well as compliance with law and policy.¹⁰¹ Control may be exercised by both formal and informal means. In general, formal means are used to ensure the conformity of intelligence activities with policy and procedures, proper authorizations, funding, audit, and review, while informal means focus on ethics¹⁰², values, and leadership, etc.

Accountability refers to a relationship based on the obligation to demonstrate and be responsible for performance in light of agreed expectations. Among the prerequisites for effective accountability one finds:

- Clear and agreed roles and responsibilities;
- clear and agreed expectations of what is to be done and how, what is not to be done, and what is to be achieved;
- performance expectations that are balanced by the relevant capacities of each party – e.g. authorities, skills and resources;
- timely and credible reporting of performance achieved in light of expectations; and,
- review of and feedback on the performance reported, such that achievements are recognized and necessary corrections made.

Arrangements for *control and accountability* can operate entirely within the executive,

Accountability. p. 6.

¹⁰¹ Hastedt, Glenn. 1986. Controlling Intelligence: The Role of the DCI. *International Journal of Intelligence and Counterintelligence*. No. 1; pp. 25-40.

¹⁰² Ericson, Paul G. 1992. The Need for Ethical Norms. *Studies in Intelligence*. Vol. 36, no.5; pp. 15-18. And: Godfrey, Drexel E. Jr. April 1978. Ethics and Intelligence. *Foreign Affairs*. No. 56; pp. 624-642. Also: Hulnick, Arthur S. & Mattausch, David D. Spring 1983. Ethics and Morality in United States Secret

or can comprise elements that are either in part, or wholly, external to the government.

The most important aspect of *executive control* is the need for competent political guidance of the intelligence services from the people they serve.¹⁰³ Thus, policymaker direction must be both the foundation and the catalyst for the work of intelligence. If intelligence does not receive direction, the chances of resources being misdirected and wasted increase. Intelligence services need to know what information to collect and when it is needed. They need to know if their products are useful and how they might be improved to better serve policymakers. Guidance must come from the top. Hence, policymakers need to appreciate what intelligence can offer them to a much greater extent and become more directly involved in the ways in which intelligence capabilities are used.

As an arm of the government, intelligence services must act according to the policies of the government of the day and in pursuit of objectives relevant to these policies. However, if too close a link between policy and intelligence exists, that is say, when it becomes policy-driven or when there is political interference in operational activities¹⁰⁴, intelligence services may become susceptible to being used by political actors as a tool to retain power and also to undermine or discredit opponents. Thus, the misuse of intelligence services with their extraordinary powers by an elected government for its own political ends must be excluded. To this end, intelligence services should be at arms length from policymakers should not be affiliated with any party, and they must be neutral or depoliticized.

The relationship between those who collect and evaluate intelligence and those who use it in the preparation of state policy – the providers and the consumers – is of great importance.¹⁰⁵ Different countries, with different needs, inevitably conduct the

Intelligence. *Harvard Journal of Law & Public Policy*. Vol. 12, no. 2; pp. 509-522.

¹⁰³ Davis, Jack. 1995. A Policymaker's Perspective on Intelligence Analysis. *Studies in Intelligence*. Vol. 38, no. 5; pp. 7-15. At: <http://www.cia.gov/csi/studies/95unclass/Davis.html>. And: Knott, Stephen. Summer 1998. Executive Power and the Control of American Intelligence. *Intelligence and National Security*. Vol. 13, no. 2; pp. 171-176. Also: Sciaroni, Bretton G. Spring 1989. The Theory and Practice of Executive Branch Intelligence Oversight. *Harvard Journal of Law & Public Policy*. Vol. 12, no. 2; pp. 397-432. And: Lowenthal, Mark M. Winter 1992. Tribal Tongues: Intelligence Consumers - Intelligence Producers. *The Washington Quarterly*. Vol. 15, no. 1; pp. 157-168.

¹⁰⁴ Gates, Robert M. 1992. Guarding Against Politicization. *Studies in Intelligence*. Vol. 36, no. 5; pp. 5-13. And: Leadbetter, Wyland F. Jr. & Stephen, Bury J. Spring 1993. Prelude to Desert Storm: The Politicization of Intelligence. *International Journal of Intelligence and Counterintelligence*. Vol. 6, no. 1; pp. 43-56.

¹⁰⁵ Heymann, Hans Jr. Winter 1984. The Intelligence – Policy Relationship. *Studies in Intelligence*. Also: Hulnick, Arthur S. May 1986. The Intelligence Producer – Policy Consumer Linkage: A Theoretical Approach. *Intelligence and National Security*. Vol. 1, no. 2; pp. 212-233. And: Betts, Richard K. January 1988. Policy-Makers and Intelligence Analysts: Love, Hate or Indifference? *Intelligence and National*

relationship between their intelligence services and their governments differently.¹⁰⁶ The functioning of the US intelligence cycle in practice changes with every administration and president. While Truman was ignorant about intelligence and deeply suspicious of espionage, Eisenhower's wartime experience was responsible for his peacetime enthusiasm for intelligence in all its forms, which was instrumental for the stabilization of the Cold War between the mid-1950s and the early 1960s.¹⁰⁷ The transition from Bush to Clinton was almost equally dramatic. Bush regularly rang up the desk officer at the CIA and provided the feedback which all intelligence services require from policymakers if they are to do their jobs effectively. Clinton, by contrast, had little interest in intelligence and found it progressively more difficult to find suitably qualified candidates willing to become the DCI. If he has maintained morale in the intelligence agencies, the secret has been well kept. Churchill's enthusiasm for intelligence and his wartime passion for ULTRA¹⁰⁸ is common knowledge. Indeed, this passion remained as undimmed as Thatcher's interest in intelligence. Many other examples clearly show that political leaders whose interest in and understanding of intelligence predate their arrival in office are, with inevitable exceptions, likely to handle it better than those who are introduced to it on, or shortly before, their advancement.

Since personalities play an unpredictable role¹⁰⁹, there must be some fuses – institutional functions which bring in consistency, which do not vary from one government to the other, resulting in inconsistent, infrequent guidance, and sometimes no guidance at all, leaving intelligence to fend for itself. The principle source of external guidance for intelligence should be the body of officials directly subordinated to and advising the top decision-makers – the president, the prime minister, or an inner circle of cabinet ministers responsible for foreign, defence and internal security policy, economy, foreign trade, and possibly finance and justice. The institutional role

Security. Vol. 3, no.1; pp. 184-189. Also: Davies, Philip H. J. October 1995. Organizational Politics and the Development of Britain's Intelligence Producer/Consumer Interface. *Intelligence and National Security*. Vol. 10, no. 4; pp. 113-132. And: Timmerman, Kenneth R. December 1999/January 2000. Shoot the Messenger. *The American Spectator*. Vol. 32, no. 12; pp. 68-70.

¹⁰⁶ Gardiner, Keith L. January 1991. Squaring the Circle: Dealing with Intelligence – Policy Breakdowns. *Intelligence and National Security*. Vol. 6, no. 1; pp. 141-153.

¹⁰⁷ Andrew, Christopher. 1996. *For the President's Eyes Only. Secret Intelligence and the American Presidency from Washington to Bush*. London: Harper Collins Publishers. And: Andrew. October 1995. American Presidents and their Communities. *Intelligence and National Security*. Vol. 10, no. 4; pp. 95-112.

¹⁰⁸ British wartime decryption of German communications encrypted by ENIGMA machines at Bletchley Park.

¹⁰⁹ Thomas, Stafford T. Summer 1994. Presidential Styles and DCI Selection. *International Journal of Intelligence and Counterintelligence*. Vol. 7, no. 2; pp. 175-198. And: Warren, Ward. Fall 1995. Policies, Presidents, and DCIs. *International Journal of Intelligence and Counterintelligence*. Vol. 8, no. 3; pp. 337-344.

of that body should not change with the government elected. Ideally, this could be a National Intelligence Council.¹¹⁰ That said, no matter what structure they are, it should remain clear that the top intelligence chiefs report directly to the top decision-makers.

Intelligence failures derive far less from the collection and analysis than from the use made of it.¹¹¹ Coordinating 'all-source' information in a form which makes it accessible to, and usable by, policymakers, whilst at the same time giving appropriate weight to dissenting opinions, is the intelligence equivalent of squaring the circle. So far, no fully satisfactory method for achieving this miracle appears to have been devised. Yet national intelligence assessments should be inter-departmentally agreed assessments with a broad governmental perspective that cuts across ministerial boundaries. The British Joint Intelligence Committee may be such an assessment system.¹¹² With all its faults – notably the tendency for blandness that invariably results from the quest for consensus – it might be better than the US President's NSC at coordinating assessments by intelligence services, State, Defence and Treasury Departments representatives, resolving turf battles, and gaining the confidence of top policymakers.

Inevitably, intelligence is an activity where there will at times be the temptation, and perhaps even the need, to transgress the conventional limits of moral or legal conduct in the hope of achieving some greater aim. Though this may be justified on occasions, it is natural that there should be misgivings by others who may be unaware of what is at stake. There have been occasions when which the zeal of intelligence officers has led them into actions that may be prejudicial to some wider interests. Since the secrecy which surrounds the work of the intelligence services can produce temptations to act independently, there must be a clear *tasking system*, controlled on behalf of those for which they are collecting information. As a principle, no intelligence operations should be conducted, unless there is an agreed requirement.

¹¹⁰ Lowenthal, Mark M. 2003. *Intelligence. From Secrets to Policy*. Washington D.C.: CQPress. pp. 139-152.

¹¹¹ Travers, Russ. 1997. A Blueprint for Survival: The Coming Intelligence Failure. *Studies in Intelligence*. No. 1; pp. 35-43. And: Betts, Richard K. October 1978. Analysis, War and Decision: Why Intelligence Failures Are Inevitable. *World Politics*. Vol. 31, no. 1; pp. 61-89. And Betts. Spring 1998. Intelligence Warning: Old Problems, New Agendas. *Parameters*. Vol. 28, no. 1; pp. 26-35.

¹¹² Herman, Michael. October 1995. Assessment Machinery: British and American Models. *Intelligence and National Security*. Vol. 10, no. 4; pp. 13-33. And: Lowenthal. Op.cit. p. 154.

Generally, the greater the ministerial interest in, and attention to, the work of the intelligence service exists and develops, the more intimate the service will become with the conduct of the daily business of the government and the more the service will be subject to checks and balances. However, this by itself is not sufficient. The services must have assurance of the legality of the actions they take.

Intelligence services need a *statutory regime* which arranges the authorization of the ways in which they collect intelligence so as to ensure that *issues of necessity* and *proportionality* are properly considered ahead of the event. The most intrusive of these methods should require the minister's signature. In some countries the role of authorization falls to the judiciary. Nonetheless, the executive is bound to be in a better position to determine what should be the policy to adopt on internal and external security and national defence than a tribunal, no matter how eminent.

Just as the principle, or doctrine, of minimum force should govern the exercise of military power, so should minimum trespass operate in the intelligence field. It should govern the actions of external intelligence in gathering information on foreign powers, and should also govern the activities of internal intelligence and security services in trespassing on the privacy of individuals and of civilian organizations. Conversely, supervision should infringe as little as possible on the rights of an intelligence service in maintaining the necessary confidentiality regarding that organization's activities.

One of the main tasks of executive control and accountability is to make sure that the intelligence services function properly: that they ask the right questions, collect the right information, respond to the decision makers' needs, are rigorous in analysis, and have on hand the right operational capabilities.¹¹³ Of particular importance is that executive control and supervision has to identify intelligence failures and take action to prevent them from occurring in the future.

The source of executive control should be either the president or the prime minister, since they are ultimately responsible for the integrity and security of the state and for related intelligence matters. There are practical reasons why these, the ministers responsible, or the National Security Council, might not be able to give full attention to all of the control, supervisory and accountability tasks. Hence, governments in democracies will normally appoint individuals or establish committees or boards mandated with control and supervision of intelligence activities.¹¹⁴ Individuals can be

¹¹³ Lowenthal. Op. cit. pp. 153-155.

¹¹⁴ Idem.

appointed as Inspector General, Controller, Efficiency Advisor, etc., who report to the president, the prime minister or minister. Best practice is to have an independent statutory Inspector General for each of the intelligence services who may also be required to make reports to the legislative oversight committees.

Committees or boards can be established, sometimes with jurisdiction extending across the entire intelligence community, who ideally report to the president, the prime minister, or the ministers responsible, or alternatively to the National Security Council.¹¹⁵ These can be composed of members from outside the government, who are employed on the basis of their ability, knowledge, diversity of background and experience. However, no member should have any personal interest in, or any relationship with, any intelligence agency. These could be united in a *National Intelligence Council*, mandated with coordination and control. Some countries have separate committees for *intelligence supervision* and for *policy review* to scrutinize performance and policy of intelligence services.¹¹⁶

The mandate of an *intelligence supervisory board* can be:

- To periodically review the internal guidelines of each service concerning the legality or propriety of intelligence activities.
- To periodically report on its findings and any activities that raise serious questions of legality or propriety.
- To forward to the attention of the Attorney General reports received concerning activities in which a question of legality has been raised.
- To conduct such investigations of the intelligence activities of the services as it deems necessary to carry out its functions.

The mandate of a *policy review committee* can be:

- To establish requirements and priorities for intelligence.
- To review the intelligence program and budget proposals and report to the government, the minister or the prime minister on whether the resource

¹¹⁵ Lowenthal, Op. cit. p. 154: "Outside of the intelligence community itself, the NSC Office of Intelligence Programs is the highest level organization within the executive branch that provides day-to-day oversight and policy direction of intelligence".

¹¹⁶ As is the case in the US: e.g. with the President's Foreign Intelligence Advisory Board.

allocations for intelligence correspond with the intelligence requirements of the government.

- To promote collaboration between the services and provide checks and balances within the system.
- To conduct periodic reviews of intelligence products, evaluate the quality of the product, develop policy guidance to ensure quality intelligence and to meet changing intelligence requirements.
- To make recommendations on intelligence matters and to submit an annual report.

In carrying out their work, these review bodies are limited to specific mandates. Since security considerations impose limits on the extent of legislative scrutiny of intelligence services, it is especially important for the ministers concerned to have the information and the support they need so as to adequately dispatch their fundamental democratic responsibility and accountability. To this end, ministers have to provide policy direction, authorize sensitive operations, be appropriately informed of performance and to have an assurance, either from internal or external review mechanisms, which operations remain within the prescribed legal and operational policy limits. Furthermore, if ministerial direction is to be meaningful, every effort has to be made to ensure timely approvals.¹¹⁷

Audit is another important part of executive control. An external audit serves three purposes in terms of accountability: Firstly, to assess compliance with the law, ensuring that those given executive authority exercise this authority in accordance with their assigned responsibilities. This involves reviewing behaviour, identifying poor administration and those who should be held accountable. The second purpose of auditing is to assess performance in public management in order to contribute to organizational learning. The third purpose is compliance auditing, which involves scrutinizing accounts to see if money has been spent as allocated and to assess the efficiency and effectiveness of financial allocations. In democracies, an external audit of the accounts is normally done by the Auditor General or the National Audit Agency.

¹¹⁷ Operations of many intelligence services are all too often affected by a lack of timely decisions. See: Whitaker, Reg. April 1992. *The Politics of Security Intelligence Policy-Making in Canada: II 1984-1991. Intelligence and National Security*. Vol. 7, no. 2; pp. 53-76.

A mostly undervalued, if not totally forgotten aspect of control is that which results from international cooperation with foreign intelligence services. Foreign services are in a privileged position to judge the performance, value, reliability and credibility of the cooperating intelligence services. If the latter were repeatedly caught in blatantly slanting intelligence and evaluations, or in inflating a threat to serve particular ends, they would probably not be asked again for contributions, advice, or cooperation. Retaliation would follow by reducing the 'do ut des' exchange to lower grade intelligence. While a significant amount of self-discipline is already built into international cooperation, executive control could profit from the feedback given by collaborating foreign intelligence services on their evaluation of the intelligence exchange and the value of cooperation.

Also, intelligence services personnel who have a strong inclination to do the right thing, and whistleblowers – individuals who report on unlawful activities that have transpired within the services – can act as internal controls.¹¹⁸

4.2. Legislative Oversight

The term *oversight* describes a system of accountability in which those vested with the executive authority in an organization have their actions reviewed, sometimes in advance, by an independent group that has the power to check those actions. To be truly democratic, political control must involve accountability to democratically elected representatives – that is to parliaments.¹¹⁹ The legislature is elected to represent the people and to ensure government by the people under the constitution. It does this by balancing security and liberty, in part by providing a national forum for public consideration of issues, by passing legislation, and by scrutinizing and overseeing executive action. In all aspects of government, and the expenditure of public money, parliaments have an essential role in monitoring and scrutinizing policy and budgets. The budget represents the culmination of intelligence requirements and, at the same

¹¹⁸ In the US, the Intelligence Community Whistleblower Protection Act became law in 1998. The Act established procedures by which intelligence community employees may report a complaint or urgent concern. They must first do so through channels in the intelligence community, but are free to inform the Intelligence Oversight Committees if the community has taken no action by a specific time. Even then, the employees must inform executive branch officials that they are going to Congress and must handle their information in accordance with proper security procedures.

¹¹⁹ See: Assembly of Western European Union. 4 December 2002. *Report: Parliamentary oversight of the intelligence services in the WEU countries – current situation and prospects for reform*. Paris: WEU. Document A/1801. Also: Jackson, William H. Jr. July 1990. Congressional Oversight of Intelligence. Search for a Framework. *Intelligence and National Security*. Vol. 5, no. 3; pp. 113-147. Also: Johnson, Loch K. The U.S. Congress and the CIA: Monitoring the Dark Side of Government. *Legislative Studies Quarterly*. Vol. 5; pp. 477-499. And: Sturtevant, Mary. Summer 1992. Congressional Oversight of Intelligence: One Perspective. *American Intelligence Journal*. Vol. 13, no. 3; pp. 17-20. And: Van Wagenen, James S. 1997. Critics and Defenders: A Review of Congressional Oversight. *Studies in*

time, it represents the contribution required from the taxpayer – the electorate at large to whom parliamentarians are most directly responsible. Though legislative oversight is policy-related and, in theory, unlimited, the choice is not between executive or legislative sovereignty over intelligence. The challenge is to use the best attributes of both branches in the service of the nation's security.¹²⁰

Few members of parliament have expertise in national security or intelligence matters at the time they are elected. Those in the executive branch, by contrast, have been selected for their positions precisely because of their expertise in some aspects of national security affairs. Hence, any arrangement that removes the ultimate responsibility for accountability for the conduct of government business from ministers in parliament would be a mistake. To substitute somebody else as the final arbitrator of what should happen is quite simply wrong.

The role that parliament can play in the development and implementation of national security policy can be grouped to four tasks: (1) *oversight*, (2) giving a *second opinion*, (3) ensuring *transparency*, and (4) providing a *link between intelligence and society* at large.

Oversight is a function of a legislature which flows from the separation of powers and is the power to hold the executive accountable.¹²¹ Monitoring the implementation of legislation goes to the heart of the oversight role. However, oversight is a process, not an event. It should be both proactive and reactive: proactive in anticipating issues; reactive to initiate hearings and inquiries when problems or scandals occur, and to determine whether legislation is effective and having the desired results. It should also ensure that the laws give other branches of government and civil society sufficient powers to supervise intelligence activities.

Parliamentary *oversight of intelligence* involves two elements: holding the government accountable for the intelligence *funds* it requires and for *the way it spends these funds*; in other words, ensuring that the intelligence resources are used in the most efficient and cost-effective manner; and influencing the *development and*

Intelligence. No. 1; pp. 97-102.

¹²⁰ Knott, Stephen. Spring 2000. The Great Republican Transformation on Oversight. *International Journal of Intelligence and Counterintelligence*. Vol. 13, no. 1; pp. 49-63.

¹²¹ Also see: Robertson, K. G. Summer 1998. Recent Reform of Intelligence in the United Kingdom: Democratization or Risk Management. *Intelligence and National Security*. Vol. 13, no. 2; pp. 144-158. Also: Gill, Peter. April 1996. Reasserting Control: Recent Changes in the Oversight of the UK Intelligence Community. *Intelligence and National Security*. Vol. 11, no. 2; pp. 313-331. U.S. Senate Select Committee on Intelligence. *Legislative Oversight of Intelligence Activities: The U.S. Experience*. 1994. Report, 103rd Congress, 2nd Session. Washington D.C.: GPO.

implementation of intelligence policy. The degree to which parliaments achieve both accountability¹²² and influence varies widely, depending on the strength of their parliamentary processes. All parliaments hold their governments accountable in the sense that parliament must approve the funds required by the executive – both in terms of the amount budgeted, and in terms of the distribution of spending within the budget. Yet, intelligence is not just another form of public expenditure. Intelligence brings with it certain inherent problems that can restrict and hamper the involvement of the entire parliament. This explains the existence in most democracies of *special oversight committees* either of both houses or as a single *ad hoc* body, normally of a small group of legislators, for intelligence services, and are set up as sub-committees, special or select committees.

These *special* or *select committees* have various powers of information and scrutiny allowing them to supervise the activities of their government in this field.¹²³ None have powers comparable to those of the US Congress. Next to tight control over the budget, hearings – requesting information from responsible officials and obtaining alternative views from outside experts – constitute together with the following six powers the levers essential to the US legislative oversight process: (1) to confirm or reject nominations; (2) to advise and consent to an act of treaty¹²⁴ ratification; (3) to levy reporting requirements on the executive; (4) to investigate – a power serving as effective tool in exposing shortcomings and abuses, offering recommendations for change, and in helping craft new policy directions; (5) to withhold action on issues that are important to the executive; and, (6) to get prior notice of *covert action*.¹²⁵

Parliamentarians have a strong sense of what the people will accept, and some of them possess a considerable amount of foreign policy expertise. In a few countries they are even users and consumers of intelligence products, notably in the US.¹²⁶ Thus, parliament can provide a second opinion, which is carefully tendered in the executive – closed – sessions of the oversight committees. On sensitive matters

¹²² Johnson, Loch K. January 1997. The CIA and the Question of Accountability. *Intelligence and National Security*. Vol. 12, no. 1; pp. 178-200. And: Johnson. Spring/Summer 1995. The Evolution of CIA Accountability. *American Intelligence Journal*. Vol. 16, no. 1; pp. 43-46.

¹²³ Leigh, Ian. 2002. *The UK's Intelligence and Security Committees*. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, 3-5 October 2002, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

¹²⁴ The ability to monitor adherence to treaty provisions can be a mission for intelligence.

¹²⁵ Lowenthal. Op. cit. pp. 155-173.

¹²⁶ McCullough, James. Spring 1998. Commentary on 'Congress as a User of Intelligence'. *Studies in Intelligence*. pp.71-74. At: <http://www.cia.gov/csi/studies/spring98/mccullou.html>. And: Snider, Britt L. Spring 1998. Sharing Secrets with Lawmakers: Congress as a User of Intelligence. *Studies in Intelligence*. At:

http://www.cia.gov/csi/studies/spring_98/Congress.html Also: Glennon, Michael J. 1998. Congressional

which can involve great costs and dangers for the nation, a second opinion can be vital.

Another important aspect of the oversight committees' work is that through their debates, hearings and reports, legislators can make intelligence more transparent, and thus more visible to the public.¹²⁷ Although the proceedings of the committees are generally kept secret, much of the information is disclosed to the public through annual reports. Public support is best achieved by the free and informed discussion of intelligence issues in general, which in turn necessitates a substantial degree of openness and transparency. Openness should be encouraged whenever possible. What can be disclosed to the public, however, will necessarily depend on the circumstances? The role of the committees is *to balance security and liberty*, and care must be taken that disclosure does not damage the ability of intelligence services to accomplish their mission. Moreover, information that is required for national security purposes is highly specific and often cannot be divulged in advance or subjected to frequent public debate. Neither can intelligence services be controlled too meticulously, since this would hamper their operational efficiency. Thus, in most countries, openness has not always been easy to achieve. As a subject, intelligence lends itself to secrecy and exclusivity. The provision of adequate information has often been limited for reasons of national security, and open debate has often been restricted by a tendency to believe that intelligence affairs are best left to the professionals. National security reasons will continue to be used to restrict information, but less often and with less justification than during the Cold War. In addition, greater transparency can also be achieved through questions put to the ministers responsible for intelligence services.

Parliament, moreover, has a role to play by providing a link between the services and the public at large.¹²⁸ An intelligence oversight committee's authority is a constant reminder for the intelligence services to perform their task correctly and it also assures the public members of the committees that the services are not left to their own devices. The nature of intelligence limits the information that can be provided to the public. As representatives of the public, the parliamentary oversight committees need access to secret information. Thus, they should have the right to request

Access to Classified Information. *Berkeley Journal of International Law*. Vol. 16, no. 1; pp. 126-137.

¹²⁷ Gill, Peter. January 2003. *Democratic and Parliamentary Accountability of Intelligence Services after September 11th*. DCAF Working Paper No. 103. At: http://www.dcaf.ch/publications/Working_Papers/103.pdf

¹²⁸ Born, Hans. May 2002. *Democratic and Parliamentary Oversight of the Intelligence Services: Best Practices and Procedures*. DCAF Working Paper No. 20. At:

reports, and hearings as well as to conduct investigations to expose shortcomings or abuses. As a general rule, under such procedures as the president or the prime minister may establish (including those conferred by law upon the executive, legislature and judiciary to protect sources and methods), intelligence services should:

- Keep the oversight committees fully and currently informed of their intelligence activities, including all significant anticipated activities;
- Upon request, provide the oversight committees with any information or document in the possession, custody or control of the service; and,
- Report information relating to intelligence activities that are illegal or improper, and corrective actions that are taken or planned to the oversight committees in a timely fashion.

In order to be able to perform their task, the members of parliamentary oversight committees must have the trust of both the intelligence services and the public. Ideally, the committees should bring a perspective to the oversight function that is not replicated by the control and review bodies within the executive branch.¹²⁹ Furthermore, oversight should not become so burdensome and intrusive that it has a negative effect on intelligence operations. Since all too often legislative oversight tends towards micromanagement of executive decisions, the parliament's oversight committees must not have the authority to direct the intelligence services to initiate certain investigations or to pursue certain cases. The question of which persons, groups, events, and activities to investigate is an executive branch decision. Moreover, the committees are political bodies;¹³⁰ they are subject to political expediency and subject to overreact. Thus, the members should hold the responsibility of avoiding any overreaction in times of crisis, and the intelligence services should have the responsibility of retaining their focus on their missions and not letting the committees push them into following new objectives.

Another critical issue of legislative oversight is the *balance between independence and criticism* on the one hand, and the *maintenance of a working relationship*

http://www.dcaf.ch/publications/Working_Papers/20.pdf

¹²⁹ See: *UIP and DCAF - Parliamentary Oversight of the Security Sector. Principles, mechanisms and practices*. 2003. Handbook for parliamentarians, No. 5. Born, Hans, ed. and Lead Author. Geneva/Belgrade: Goragraf; pp. 190.

¹³⁰ Ott, Marvin C. Spring 2003. Partisanship and the Decline of Intelligence Oversight. *International Journal of Intelligence and Counterintelligence*. Vol. 16, no. 1; pp. 69-94.

between the committees and the intelligence services on the other hand. Intelligence is one of the only areas of government activity where risk-taking and innovative thinking, within the confines of applicable law and policy, should be encouraged. It is a domain that relies heavily on the professional judgment and candour of the intelligence personnel. It is also an area that is highly dependent upon the cooperation of other agencies, foreign governments, and individuals. What the overseers do in public has an effect which goes beyond the circumstances of a particular inquiry or investigation. While the committees are naturally eager to demonstrate that their oversight is effective, they must always be aware of the inherent danger that their statements and actions might distort the public's perception of intelligence, create an unfavourable impression among potential sources, agencies of cooperation, foreign services and governments, and undermine the morale of intelligence personnel. Thus, legislative oversight has to be determinedly non-partisan and discreet, and hearings should be fair. The oversight committees should be more inquisitorial than adversarial, and they should broaden the range of oversight beyond the intelligence services to users of intelligence.

Access to information will increase as confidence grows. True, there always looms the danger of leaks.¹³¹ However, experience shows that if the members are trustworthy, services will be honest and frank with them. Hence, those mandated with the oversight have to make it clear that they can be trusted with sensitive information and can produce reports that are thorough, focused and rigorous, yet in no way compromising to the nation's security. Though it is the nature of oversight that parliamentary reports are generally negative where executive agencies are concerned, the committees ought to ensure that a balanced picture is presented to the public, giving credit where credit is deserved and defending intelligence services where their performance has been inaccurately portrayed or their integrity unfairly maligned. Intelligence services cannot credibly defend themselves.¹³² At the same time the committees must avoid becoming the advocate for the intelligence services.

¹³¹ Hyde, Henry J. 1988. Leaks and Congressional Oversight. *American Intelligence Journal*. Vol. 9, No. 1; pp. 24-27.

¹³² One element of the French approach to legislative oversight: ...il est nécessaire de prévoir des dispositifs de protection, non seulement des informations vitales pour la sûreté de l'Etat, mais aussi des hommes qui les servent dans des conditions difficiles, voire dangereusesLes services ont par ailleurs besoin de reconnaissance, il faut les valoriser... See: Denécé, Eric. Mars 2001. Le contrôle parlementaire des services de renseignement. Interview d'Arthur Paecht, député du Var, vice-président de la Commission de la Défense et des Forces armées à l'Assemblée nationale. Paris: L'Harmattan. *Renseignement & Opérations Spéciales*, No. 7; p. 24.

The question of competence is more complicated. By its very nature, intelligence is governed by qualities that are unique and are not easily comprehended by outsiders. For some parliamentarians, membership of the intelligence oversight committee is not attractive, because it generally offers fewer opportunities for public profiling. Others seem “somehow afraid of taking over greater responsibilities and thus also increased risks”¹³³ – wary of consenting to operations that might prove embarrassing and fearing that, should a new intelligence scandal occur, they could take equal blame for it.¹³⁴ Parliamentary involvement with intelligence is also affected by the nature of parliamentary work. Competing pressures and responsibilities mean that few legislators can devote the time needed to give them real intelligence expertise. If members are appointed for fixed terms, they often have to rotate off the committees at the very point that they have begun to master the complex subject matter. Knowing that their tenure is limited, some use their time on other committees. As a consequence, an unfortunate loss of expertise and continuity occurs, weakening the effectiveness of the committees. Thus, some countries do not limit committee membership by fixed terms of tenure and assign new members to fill spaces resulting from normal attrition. Others, who believe that allowing more members to serve on the committees through a system of rotating assignments would increase the understanding of the intelligence mission in both houses, opt for greater reliance on well-qualified staffs and assistance by investigators with wider access to intelligence. Whatever the preferences: while the right of the political opposition to participate in oversight should be laid down, it is a good rule that committee members should be appointed by the leadership of both houses of parliament, rather than by their respective party structures. A background security check should be made on them before they are appointed, and they should take an oath to maintain secrecy.¹³⁵

Experience shows that, over time intelligence services come to appreciate what the committees expect, and the committees will appreciate the concerns of the services and be willing to accommodate them. The champions of oversight want reliable safeguards to preserve liberty; its critics seek more effective secret operations to shield the nation from enemies at home and abroad. The rub comes from this obvious conclusion: a modern democratic state wants and deserves both civil liberties and a shield against foreign dangers. So, the search continues to find the right formula for

¹³³ Haering, Barbara. 2002. *Investigating the Strategic Intelligence Service of Switzerland. Experiences of a Parliamentarian*. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, 3-5 October 2002, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF). p. 6.

¹³⁴ Lowenthal, op.cit. pp. 167-169.

power sharing in this most difficult of government domains – knowing full well that no formula exists, only the hope that in a spirit of comity, parliament, the executive, and the judiciary will continue in their quest for a *modus vivendi* in which liberty and security are taken into account.

4.3. Judicial Control and Supervision

The law must regulate intelligence activities and establish procedures to guarantee its proper execution, protection and transparency. Without a legal framework, legislative oversight, executive control, and judicial supervision would have no reference point and their work would not make any sense. The independence of these three branches of government from one another dramatically strengthens the functioning of their various supervisory roles.¹³⁶

Judicial control and supervision is limited in comparison to ‘*unlimited*’ legislative oversight.¹³⁷ It deals with legal issues, as opposed to policy issues. The judiciary reviews and interprets the constitutionality of all laws. Its role in controlling intelligence is modest, but from time to time can be significant when the conduct of intelligence activities is reviewed. The very fact that intelligence activities could be subject to an independent court review creates a type of ‘*anticipatory control*’. Though the judiciary is more deferential to the executive branch in intelligence matters, judicial control can act as arbiter of government secrecy in powerful ways.

Government secrecy in a western liberal democracy is generally undesirable. It can destroy the legitimacy of government institutions and can cripple the accountability of politicians and public servants. It can hide abuses of the fundamental rights of the citizen. Secrecy within governments tends to excess. Judicial control has to counter-balance the swing toward such excess and it must improve the problems of government secrecy by providing a secure forum for the review of intelligence activities under a number of laws, as surrogates for the public.

Intelligence services are not above the law – and penalties must be provided by the law. If there are no enforcement measures for accountability, there can be no democracy. Under the rule of law, the activities and functions of intelligence services cannot extend beyond those that are necessary for protecting the democratic

¹³⁵ Also see Lowenthal, Op. cit. p. 162.

¹³⁶ Manget, Frederic F. 1996. Another System of Oversight: Intelligence and the Rise of Judicial Intervention. *Studies in Intelligence*. Vol. 39, no. 5; pp. 43-50.

¹³⁷ Idem.

constitutional order. The constitutional order includes the catalogue of fundamental freedoms and rights and effective measures to protect those rights from any violations. No intelligence service can arbitrarily threaten those rights and freedoms; should it do so, it threatens the constitutional order instead of protecting it.

Thus, in democracies, 'best practice' is that intelligence services consider themselves to be bound by the Constitution and laws of the country – including treaty obligations and other international agreements entered into by the state – in the same way as they are bound by executive orders, guidelines, and numerous ministerial or agency directives. A 'good practice' is to establish guidelines for *internal intelligence*, ideally approved by the Attorney General, that govern the collection, analysis, and dissemination of information on citizens and aliens admitted for permanent residence in the state. Another 'good practice' is to have guidelines for *external intelligence* that limit the use of personnel from humanitarian organizations, such as the ICRC or national Red Cross organizations, those engaged in aid and development, as well as the use of clergy, journalists, and academics¹³⁸ for operational purposes.

In democracies, intelligence services are normally prohibited by law from having any police, *subpoena*, or law enforcement powers. Moreover, as a 'good rule', a court order, ideally from a special court, is regularly required before intelligence services can carry out electronic surveillance and physical searches for any external intelligence or counterintelligence purposes within the country. By following this practice, the court must be persuaded that the target of investigation is a threat to the security of the state, and that other techniques have been useless in gaining the necessary information.¹³⁹

Another 'best practice' is to make sure that particular measures employed to acquire *internal intelligence*, apart from being responsive to legitimate governmental needs, are to be conducted in a manner that preserves and respects established concepts of privacy, civil liberties and civil rights. It is here that supervision is most necessary. There is a need for protecting human rights and other liberties of citizens who are suspects, while at the same time establishing protection against grave dangers to other citizens who are likely to be victims. Judicial control has to set limits intended to achieve the right balance between protection of individual rights and acquisition of

¹³⁸ Hulnick, Arthur S. Winter. 1986-1987. CIA's Relations with Academia: Symbiosis Not Psychosis. *International Journal of Intelligence and Counterintelligence*. Vol. 1, no. 4; pp. 41-50.

¹³⁹ Sandberg, Justin M. Winter 2002. The Need for Warrants Authorizing Foreign Intelligence Searches of American Citizens Abroad: A Call for Formalism. *The University of Chicago Law Review*. Vol. 69, no. 1; pp. 403-427.

essential information. Thus, collection procedures established are normally approved by the highest judicial authority, generally the Attorney General. Such procedures ensure that information is collected by the least intrusive means possible, and limit the use of information to lawful governmental purposes.

Moreover, operations by the *internal* intelligence agency may be subject to judicial examination by a tribunal after the event, to investigate complaints about the service by members of the public, and to review the warrants issued by the minister. 'Best practice' here is that judges have full access to classified information, as long as the information is relevant to the question of guilt or innocence in the given case. This implies that claims to secrecy need to be supported by a justification of why it would be harmful to have the information disclosed.

For judicial control and supervision to be effective, the Attorney General should:

- Receive and consider reports from the services.
- Report to the ministers responsible, the prime minister or the president in a timely fashion on any intelligence activities which raise questions of legality.
- Report to the ministers responsible, the prime minister or the president on decisions made or actions taken in response to reports from the services.
- Inform the ministers responsible, the prime minister or the president about legal opinions affecting the operations of intelligence services.
- Establish or approve procedures for the conduct of intelligence activities. Such procedures ensure compliance with law, protect constitutional rights and privacy, and make sure that any intelligence activity within the state or directed against any citizen is conducted by the least intrusive means. The procedures can also ensure that the use, dissemination and storage of information concerning citizens which is acquired through intelligence activities, is limited to that necessary for the achievement of governmental purposes.

In addition to the policy restraints on their activities, intelligence services and their employees are subject to the judicial process. Like other government agencies and employees, they can be sued for actions undertaken during the course of their official duties. Though in most countries it is extremely rare for an individual who has acted in the interest of protecting national security to be prosecuted for violating the law:

those who violate laws and policies can be held liable, be *subpoenaed* in civil and criminal cases, or subjected to administrative sanctions, and they must produce information when ordered to do so by the courts.

A different and weaker form of judicial oversight can be established by allowing intelligence services staff to go to employment tribunals. The establishment of the office of Ombudsman for the protection of civil rights may also be an effective tool for controlling the services.

4.4. Informal and Indirect Supervision by the Public

Civil society organizations – NGOs, lobbies, pressure and human rights groups, political parties, professional, cultural, and other advocacy or special interest associations – and the media, can perform a useful supervisory function of intelligence services. Supervision by the public can help to ensure that the objectives of an intelligence service are beneficial for the society as a whole,¹⁴⁰ rather than only for a specific political party or an elite group of individuals. Mobilizing civil society actors is one way for accountability institutions to strengthen their position *vis-à-vis* the political executive.

Since a well-informed citizenry helps to make the government responsive and accountable, a structural factor that may facilitate supervision and transparency is the possibility that information about intelligence activities becomes available after a certain period of time. For example, this could occur through ‘freedom of information’ legislation and rules on the release of classified materials after a set period of time. This possibility of *delayed transparency* may facilitate democratic control. Hence, declassification of documents is important, because if documents are not made public, civil society has few other mechanisms for supervising the intelligence services. In the United States and in Canada, where intelligence agencies – like other government agencies – are subject to the Freedom of Information Act,¹⁴¹ media and citizens groups use such rights to examine areas of governmental activity that have long been immune from public scrutiny. The success of NGOs in helping to

¹⁴⁰ Vitkauskas, Dovydas. June 1999. *The Role of a Security Intelligence Service in a Democracy*. Chapter III, Opening up to the public scrutiny. Brussels: NATO. Democratic Institutions Fellowship Programme. pp. 49-51.

¹⁴¹ Certain of the CIA’s operational files are exempted by law from the requirements of the Freedom of Information Act to search for records in response to a request from the public. Information classified pursuant to Executive Order is exempted by the Act from disclosure and, since most information held by intelligence agencies is classified, relatively little substantive information concerning intelligence activities is released under the Act.

pass legislation on access to information is evidence of the powerful that role civil society can play in supervising intelligence services.¹⁴²

It is very important that the threats to the country are outlined in a concrete way, and that the public is informed and educated about these threats. This will result in an increase in public support for intelligence services, as well as greater control and supervision.

Civil society organizations can play a role in articulating the demand for an accountable government and can draw public and political attention to infringements of civil liberties and human rights. Lobbies, advocacy and special-interest groups can serve to educate and inform the public, and to challenge or support government policy decisions. It is important that civil society groups build efficient institutions that work to consolidate democracy. Though consensus-building in civil society can be very challenging at times, an increase in consensus and cooperation, particularly between political parties, is beneficial to the country.

Human rights organizations can make effective changes to intelligence services through providing victims of internal intelligence and security services with access to information from security files,¹⁴³ through litigation, the drafting of new laws, and efforts to educate the public about intelligence issues. While they should stay informed about intelligence and civil liberties issues and monitor changes in the laws so that they can assert pressure on parliament, human rights groups also have a responsibility to educate the media about the complexities of intelligence issues, to urge them to cover public debates and produce in-depth articles and commentaries that can enhance public understanding and awareness about intelligence.

The role of the media is more controversial. Generally, the informal supervision they may exercise primarily tends to occur through the lens of scandal. All too often, the media makes a great play of intelligence leaks, whistle-blowing and failures, while remaining thrilled by secrecy. Through their capacity to reveal illegal activities and abuses of power, electronic and print media can shape public opinion and draw the attention of actors controlling the more formal mechanism of control and

¹⁴² Banisar, David. 2002. *Freedom of Information: International Trends and National Security*. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, 3-5 October 2002, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

¹⁴³ As happened in Poland, in Germany (in the former GDR), and in other East European countries. See: Majtényi, László. 2002. *Reconciliation and Developing Public Trust: Opening State Security Files to the Public*. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, 3-5 October 2002, organized by the Geneva Centre for the Democratic Control of Armed

accountability.¹⁴⁴ When internal control does not check questionable behaviour, and external control does not identify and challenge it,¹⁴⁵ investigative journalism can serve as a sort of ‘*unofficial opposition*’ or ‘*fall-back accountability mechanism*’. However, unless journalists are specialized in intelligence and security issues, there is also the danger of sensationalism and personalization of intelligence issues. Moreover, examples abound of occurrences where the media behaved in a manner that has not so much been deferential as irresponsible.¹⁴⁶ Albeit few, there are times when the media should show restraint in the national interests.¹⁴⁷ On the other hand, there are also cases where the media are misused as instruments for the proliferation of slander or disinformation campaigns through ‘*information*’ or ‘*products*’ originating from intelligence services.¹⁴⁸

Just as ethics and morals change in other areas, so too, do they change in the media. Intelligence services are enclosed by both real and figurative walls, as daunting for journalists as for scholars and other outsiders. Expectations that the media will be able to break down these walls with any frequency is unrealistic, nor would most citizens want the nation’s secrets to be so easily breached. Yet, despite many obstacles to media supervision of intelligence, there are always some reporters who will report to the public and to parliament, providing more information than the intelligence services would wish to have disclosed, information which editors will happily highlight on television or print on their front pages. In the post-Watergate era of ‘investigative journalism’, it is difficult to imagine that many reporters or media outlets would be willing to suspend publication or drop a story entirely on the basis of imagined or suspected scandals involving intelligence. Thus, leaks, and the ever more common erosion of security discipline, whilst regrettable, might make media

Forces (DCAF).

¹⁴⁴ See the Papers presented at the Conference on “*The Role of the Media in Public Scrutiny and the Democratic Oversight of the Security Sector*”, held in Budapest, 6-8 February 2003, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF). At: http://www.dcaf.ch/Media_Budapest0203/ws_papers.htm

¹⁴⁵ Unlike in most other democracies, in terms of intelligence, the British Government can enforce prior restraint on the publication of articles deemed injurious to national security.

¹⁴⁶ See the ‘Baltimore Sun’ series of articles about the US National Security Agency’s activities, which finally gave rise to expanded interests in, and complaints about ECHELON by the EU.

¹⁴⁷ There are cases in the past where the US media have come upon intelligence activities and agreed not to report on them for the sake of national security. Thus, reporters discovered Cuban exile training camps in Florida prior to the Bay of Pigs affair. The media also learned about the construction of the ‘*Glomar Explorer*’, built by the Hughes Corporation for the CIA to retrieve a sunken Soviet submarine in the Pacific. In this case the secret was kept but for one year and the blown by the ‘*Los Angeles Times*’ in 1975.

¹⁴⁸ See: Zybortowicz, Andrzej. 2002. *Transformation of the Polish Secret Services: From Authoritarian to Informal Power Networks*. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, held in Geneva 3-5 October 2002, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

supervision increasingly feasible by transferring disclosure authority to the newsroom.

5. Transformation and Reform of Intelligence Services

5.1. Challenges That States in Transition Face When Reforming Their Intelligence Services

Change is hardly ever easy. Redirecting intelligence services from a repressive agenda to one that upholds new democratic principles and accepting democratic control is a particularly difficult task. This is prominently evident for governments which have been slow to enact reforms and which – mainly due to economic problems, short-comings of privatization, and other legacies of the past – see themselves confronted with mounting social unrest and waning popular support.

Some reforms have been hampered due to the lack of democratic experience¹⁴⁹ and the weakness of the law. The weakness of the law is particularly visible in the ‘*security sector*’, where the major institutions have all too long claimed primary responsibility for security from foreign enemies and a chiefly undefined range of domestic challenges. In most countries of transition, that claim is bolstered by the absence of civilian knowledge of and experience in the military, intelligence, and national security domain. Thus, assembling the most knowledgeable *civilian* brains is one of the prerequisites for reform. Moreover, a sufficient number of civilians need to be trained, and outside advice and assistance might be required.

As is the case in other transitional countries around the world,¹⁵⁰ Central and Eastern European countries have chosen to deal with the reform of secret services in a variety of ways. What was then Czechoslovakia, for example, dismantled the STB – the communist secret police of some 17’000 by mid-February 1990, reengaged some former secret service officials who had been fired after the 1968 invasion, and permitted some others to remain¹⁵¹ – purged, later on, when the OPCD was trimmed

¹⁴⁹ Transitions do not necessarily result in stable democratic regimes. The main focus should be on democratic consolidation, reflecting the fact that structures and processes are becoming stable. If the elected government does not control intelligence, it is by definition, not a consolidated democracy. See: Linz, Juan J. & Stepan, Alfred. 1996. *Problems of Democratic Transition and Consolidation: Southern Europe, South America, and Post-Communist Europe*. Baltimore: John Hopkins University Press; pp. 5-6.

¹⁵⁰ For example: Argentina, South Africa, Bolivia, Chile, and Peru.

¹⁵¹ See: Cerny, Oldrich. 2002. *Czechoslovak (Czech) Intelligence after the Cold War*. Paper presented

to roughly 1'000, and replaced by those who volunteered after 1989. Germany, at reunification, passed a law which prohibited GDR intelligence and security officials from continuing to hold office. While in Hungary a good number of intelligence officers were permitted to remain, in Poland, all secret service agents were dismissed during the year following the first free elections. A commission of 140 deputies and senators was formed to assess whether or not members of the former services would be reassigned. Of the 24'000 members of the disbanded civilian SB, 14'000 decided to apply, some 10'000 qualified, but only 4'000 of them ended up working in the newly established State Protection Agency UOP.¹⁵²

Although every transition is unique and no two countries' experiences are identical, many of the problems and challenges confronting intelligence services of states in transition around the world are analogous:

- Historically, most intelligence services of countries now in transition from authoritarian to democratic rule have been repressive and functioned outside the rule of law. They were used to consolidate power, to identify and closely watch dissidents, to neutralize their opposition to government, and seek to generate domestic apathy through a variety of means, including a controlled media.
- In these countries, intelligence mainly meant counterintelligence,¹⁵³ which is, protecting the state's secrets from outsiders. As almost anything could be defined as a state secret, the scope of that which had to be controlled was immense. Also, whilst in most instances intelligence services linked internal opposition to putative foreign enemies, their overwhelming focus was more domestic opposition, and less other states.
- The most negative legacy of intelligence services in the new democracies was their involvement in human rights abuses. At times the information they collected on

at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, held in Geneva 3-5 October 2002, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

¹⁵² See: Zybortowicz, Andrzej. 2002. Transformation of the Polish Secret Services: From Authoritarian to Informal Power Networks. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, held in Geneva 3-5 October 2002, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

¹⁵³ In the USSR, now Russia, scholars have coined the term 'counterintelligence state' to capture the sense of its pervasiveness. A totalitarian country like the USSR had to control the flow of information. The Soviet regime was so worried about the threat of samizdat that in 1971 the average citizen could not get near a Xerox machine, never mind a computer. For a good description of the 'counterintelligence state' see Waller, Michael J. 1994. *Secret Empire: The KGB in Russia Today*. Boulder: Westview Press; p. 13.

their own people was obtained by using abusive methods and used in arbitrary and violent means to eliminate domestic opposition.

- Often, a good number of personnel of intelligence services remain clandestinely working in other ministries or in embassies abroad. Moreover, there is a high level of politicization and a desire within these services to maintain autonomy and a nationalistic policy, while relations with *civil society* remain hesitant, or very particular.
- Most services remain reactive rather than proactive. They lack a modern doctrine, a code of conduct, standards and operational efficiency, and are, moreover, compromised by rivalries between the different organizations, and generally much too wasteful and expensive.
- Most intelligence officers who have been raised in a regime of secrecy, not really knowing who is doing what, find it difficult to adjust to greater openness. The political culture of intelligence organizations, inward-looking and emphasizing 'need-to-know', will not willingly give up information, least to the public, without a clear understanding of the objective.
- All too often there is a lack of professionalism, little strategic capability and analytic capacity in, and largely insufficient coordination between the different intelligence services of the country – the latter seemingly being the universal problem of intelligence.
- Most services find themselves with a greatly oversized workforce that is not aligned with current needs, but lack the ability to correct the situation.
- Lingering problems are that old categorizations of the country's enemies do not disappear on their own from the minds of the functionaries, that intelligence services predominantly still function without a clear legal basis of budgetary allotment, that the process for allocating resources to intelligence is often flawed, and that growing costs for personnel preclude needed investments in new technologies.
- Given that organizational structures in most intelligence services remain inefficient, much greater use of modern management skills and practices is needed.

- Aside from ideological settings, the recent history of intelligence in countries of transition has, moreover, been marked by high levels of corruption and illegal activities, such as extortion and racketeering.

For the public, however, there are two major problems. One issue is that there is little awareness of intelligence functions. Most civilian politicians, let alone the public at large, do not know enough about intelligence to be able to have an informed opinion about it. Moreover, this lack of information is combined with fear, which perpetuates the lack of information.

The other problem is that the *modus operandi* of many of these services, operating under the umbrella of various ministries but often with overlapping areas of competence, lack transparency and civilian oversight mechanisms. Thus, the danger in countries of transition is that new intelligence services are perceived likely to remain essentially the same as old ones.¹⁵⁴ The result being that official denials of any connection between the new services and their infamous predecessor are for the most part unable to dispel the suspicion that they are splinter organizations of the former, resuscitated under new names and with more specialized functions.

However, the longer the required changes and a new statute take to compete with the lingering traditions and rampant corruption, the greater the number and extent of pressures by those who blame intelligence for being far too slow, if not incapable, of restructuring, reorienting, and adapting their activities to the new risks, dangers, and threats. Therefore, it is necessary *to develop a programme* to systematically and courageously replace all the unwanted aspects of the old system with a new apparatus.

5.2. Replacing the Old System With New and Democratically Controlled Intelligence Services

The prerequisite for the *development of such a program* is a clear vision of the ideal situation for the intelligence services in both law and policy. The basic principles reflecting the anticipated ideal situation have to be defined by law. The law guiding intelligence activities should confer a clearly defined mission upon each of the intelligence services, and limit *regular* intelligence collection to specific categories of security concern, whilst at the same time recognizing human rights and the

¹⁵⁴ See: Zybertowicz, *op. cit.* p. 3, who adheres to the view that one of the upshots of the transformation in Poland (as well as in many other post-Soviet countries), is that informal elite groups rather than

fundamental freedom of citizens. The problem is that the best of recommendations enacted into law can only become effective in a setting that either takes the law, or the political process of reaching an agreement on it, very seriously. Both of these forces have to overcome ideology, old threat and security perceptions, institutional traditions, a long history of deference to the 'security sector' and to the military in particular, as well as self-interest. Yet, respect for the law simply because it has been enacted, is unlikely to be adequate to hold back this array of forces. Open democratic processes, public debate about the terms of legislation and a sense of shared decision-making, are a more important and more promising force. Public debate will broaden the number of people informed about the issues, trusting that democratically chosen leaders can and must set the goals and limits of the 'security sector'. Such consensus-building is one of the key elements for institutional reform. An increase in consensus and cooperation between political parties is beneficial for the country. In many cases, the participation of individuals from distinct sectors of society will prove to be a significant contribution to consensus-building.

Exposing these issues in public debates can, moreover, create public demand for professionalism, which, in the final analysis, is much of the answer to these shortcomings. Professionalism can bring more public support, a belief in democratic values and service to the public, greater concern for efficiency, an ethical code of conduct, pride and self-respect, and non involvement in – and independence of – politics, to the intelligence services and their activities.

A number of countries have successfully begun the process of intelligence reform by agreeing on *basic principles* to which laws and institutions are expected to conform.¹⁵⁵ Public discussions on the issues and principles have also been a pattern adopted by some regional institutions and international bodies protecting human rights, leading to a democratic determination of what the subject matter of intelligence should be, and a parliamentary law controlling intelligence functions.¹⁵⁶

democratic institutions exert real influence on the state decision-making process.

¹⁵⁵ For an interesting case study about intelligence services in new democracies see: Deletant, Dennis & Kieran, Williams. 2001. *Security Intelligence Services in New Democracies: The cases of the Czech Republic, Slovakia and Rumania*. Houndmills: Palgrave Publishers Limited.

¹⁵⁶ OSCE Summit in Budapest in 1994, when the states that signed up to the Code of Conduct on politico-military aspects of security recognized "the democratic political control of military, paramilitary, and internal security forces as well as of intelligence services and the police to be an indispensable element of stability and security". And: WEU. 4 December 2002. *Parliamentary oversight of the intelligence services in the WEU countries – current situation and prospects for reform*. Paris. Forty-Eighth Session. Document A/1801. See the parts on Hungary, p. 12; Poland, p. 14; Czech Republic and Estonia, p. 15; Latvia and Lithuania, p. 16; Romania, pp. 16-17; Slovakia, p. 17; Slovenia, p. 18;

The best results can be achieved whenever the transformation of intelligence services is guided by the following *five basic principles*, according to which the services should:

1. Provide effective intelligence essential to the security of the state;
2. Have an adequate legal framework within which to operate under the rule of law that recognizes human rights and the fundamental freedoms of the citizens;
3. Have an effective management system, ensuring responsible direction and respect of the rule of law;
4. Be effectively accountable to the president, the prime minister, or to ministers who are responsible to the parliament; and,
5. Be open to internal and external review and to parliamentary oversight, to ensure that they do not abuse their powers and that these are not misused by the government.

The real test of democratic control is the ability of intelligence services to respond to real challenges without compromising these *basic principles*.

The *program* to systematically and courageously replace all the unwanted aspects of the old system with a new apparatus will have to include the following five elements:

1. Clear guidance and coordination of intelligence services;
2. Control, supervision, and oversight of the services;
3. Professionalization of the services;
4. Strengthening of the relationship between legislation and reform; and,
5. Practical measures to enforce the program of change and reform.¹⁵⁷

5.2.1. Clear Guidance and Coordination of Intelligence Services

Guidance must come from the very top. Ministerial guidance of the intelligence services must be ensured, as opposed to arms length knowledge of their functioning.

¹⁵⁷ For further elaboration on these elements in a recent case study see: Bozhilov, Nikolai. 2002. *Reforming the Intelligence Services in Bulgaria: The experience from the last decade*. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, held in Geneva 3-5 October 2002, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

In addition, a *National Intelligence Council* or comparable coordinating body should be established with the following responsibilities:

- To define national threats, dangers, and risks together with the *National Security Council* and to develop specific proposals for areas of collection that the different intelligence services should respond to;
- To make recommendations on the national priorities of intelligence collection, the allocation of assignments and clearly defined missions among the different services with no overlap, to the president, the prime minister and the ministers responsible;
- To ensure that the intelligence services have procedures that are sufficiently clear for internally authorizing operations, and that these intelligence services are therefore able to be audited for effectiveness, should the president, the prime minister, or the minister responsible wish to confirm the legality of a particular operation; and,
- to permanently coordinate collection, and to encourage appropriate intelligence-sharing among the intelligence services.

5.2.2. Control, Supervision, and Oversight of Intelligence Services

Internal, external, and judicial control and supervision as well as parliamentary oversight must be established as important mechanisms for supporting and encouraging the implementation of the *defined program of change*.

Internal and external control and supervision can take any number of forms:

- Inspector Generals can control whether the services comply with the priorities and carry out their specific missions, but only those missions. They can be charged with gathering particular information about intelligence activities and reporting to the executive and to the legislature on their effectiveness and lawfulness.
- The minister to whom the intelligence service reports can be provided with a staff capacity that is adequate for monitoring the service in terms of its effectiveness, and also checking its compliance with restrictions. This staff also needs to have access to all information about the service's activities.

- Separate committees for *intelligence supervision* and for *policy review* can be established, and composed of members from outside the government, who are employed on the basis of their ability, knowledge, experience, or reputation for integrity, to scrutinize intelligence services' performance and policy.
- An Ombudsman can be appointed, either with a very general charge or with a more specific one that is reviewing allegations of intelligence abuse.

Parliamentary oversight must be established. The most preferred way for this to be achieved is through special or select committees of legislators – including members of parties who oppose the administration in elections – who have to pass a background security check, take a secrecy oath, and who are neither associated with the services nor with those to whom the services report. The committees must have the power and will to deter violations of law or failures of performance. This can be achieved by granting them access to budget authority and documents, as well as the right to the conduct of investigations. Proposals for change, for the modification of procedures and for the removal of the heads of the intelligence services from their positions may be addressed to the ministers to whom the services report. Adequately trained staff should be made available to support the committees.

Judicial control must review and interpret the constitutionality of all laws, set limits intended to achieve the proper balance between the protection of individual rights, the acquisition of essential information, and reviewing the warrants issued by ministers, etc.

5.2.3. Professionalization of Intelligence Services

Professionalism can be encouraged through a number of measures:

- open and careful recruitment, training, assignment career planning, and inspiring leadership;
- the establishment of a single intelligence school that will provide a basic curriculum for candidates from all services and which will serve the threefold goals of conveying ideals of professionalism, inculcating devotion to the public service, and enhancing cooperation among the services;

- assignments and promotions must reflect an intelligence officer's willingness to operate both within democratically chosen fields of national security concern and in democratically acceptable ways;
- new inspiring managers reflecting the new professionalism must be selected and held accountable for motivating personnel, inculcating action for the collective interest of the nation, imposing high standards of performance, personal compliance with strict moral obligations and ethical rules of the intelligence profession, and discipline – including firing or transfers, as a response to misbehaviour.

5.2.4. *Strengthening the Relationship Between Legislation and Reform*

The legislation should include a directive for the executive to establish a *separate and independent commission* for the *review of change and reform*, with the mission:

- to establish and to publicize specific measures of the critical objectives of change and intelligence reform each time before any legislation is adopted, and reporting any changes and performance of the services to the president, the prime minister, the parliament, and the public;
- to conduct public hearings on the results of these reviews and the conclusions reached by this independent commission, which should then be taken into account during the budget processes of both the executive and legislative branches.

5.2.5. *Practical Measures to Enforce the Program of Change and Reform*

To enforce the programme of change and reform, sustained focus should be maintained on the following *practical measures*:

- If necessary, the existing legislation will have to be amended rapidly in order to clearly define the state's intelligence and security vision and framework by law.
- The essential elements of the new intelligence organization will have to be effectively marketed to the public and within the intelligence services.
- Managerial ability and competences must be developed and strengthened to enable the services to overcome the difficulties of transformation and professionalization.

- A clear tasking system, agreed standards of performance for results as well as for compliance with law and policy must be established.
- Individuals at managerial levels must be systematically phased out if they are working against the goals or outside of the perimeters of the new organization.
- Every new 'incident' of abuse, or violation reminiscent of past behaviour, should be used as an opportunity to accelerate change, reform and professionalization.
- Short-term commissions of inquiry or ministerial task forces can be convenient and effective tools for investigating abuse and defining change and reform more clearly.
- Task forces can be used short-term to assist ministers in developing focused ministerial directives, which will help to prevent making uncoordinated, piecemeal changes.
- Comprehensive reviews of internal procedures should be undertaken to control whether these fall in line with new legislation and ministerial directives.
- Clear ministerial guidance must be provided regarding intelligence priorities to inform major planning and spending cycles of the services, and to enforce financial transparency.
- Enforcement of control and accountability¹⁵⁸ is critical during transition. Thus, any funding of activities for which no completely convincing proof of the need exists should cease immediately.
- A professional quality control should be established if quality, relevance, timeliness and therefore utility of intelligence products to the policymaker are to be improved.

5.3. *The Threats to Security and the Impact of September 11th, 2001*

¹⁵⁸ Relationship based on the obligation to demonstrate and be responsible for performance in the light of agreed expectations. Among the prerequisites are: (1) clear and agreed roles and responsibilities; (2) clear and agreed expectations of what is to be done and how, what is not to be done, and what is to be achieved; (3) performance expectations that are balance by the relevant capacities of each party – e.g. authorities, skills, and resources; (4) timely and credible reporting of performance achieved in the light of expectations; (5) review and feedback on the performance reported, such that achievements are recognized and necessary corrections made.

The events of 9/11 – which in the US are partly seen to be due to an intelligence failure¹⁵⁹ – have forced the issue of intelligence reform on the agenda of both *old* and *new democracies*. How best to mobilize information and intelligence to protect a state's security? Most of the discussions about reforming the use of intelligence in the fight against terrorism have focused on problems of information sharing within the governments. However, only by understanding the nature of the intelligence challenge in dealing with counterterrorism can an appropriate 'architecture' or organizational structure suitable to the task be developed. The intelligence challenge has four key components: (1) collecting timely, relevant and, in the best case, actionable information; (2) collating or bringing together information from the full spectrum of sources; (3) analyzing the information – '*connecting the dots*' and the '*joining of all the pieces of a larger puzzle*'; and (4) disseminating that information to all those who need to act on it – policymakers, law enforcement officials, first responders, and the public – in a form that allows them to use that information to accomplish their mission.

Every country has to create its own definition and explicit parameters for national security and intelligence. Whether in old or new democracies: practical orientation measures are needed to ensure a changed threat perception as the basis for intelligence action. It is very important that the threats are outlined in a clear way, and that the public is educated about these threats, thus resulting in an increase in support for the intelligence services.¹⁶⁰ Intelligence collection ought to be limited to matters of security concern, and the list of such matters should be reviewed periodically. The critical subject matters for secret intelligence collection depend on what hostile forces endanger the nation and its interests at any time. It is their hostility and their potential for violence that create risks where open intelligence collection would prove inadequate. The most important consideration is that whatever security threats are thought to justify, secret intelligence activities should be authorized by democratically chosen executive and legislative officials who are publicly accountable for their actions. Intelligence services should not select the subject matter of intelligence collection, although recommendations both will and should come through these sources.

¹⁵⁹ This led the US Congress to conduct investigations. Public hearings by a Joint Inquiry began on 18 September 2002. See: CRS Report RL 31650; The Intelligence Community and 9/11: Congressional Hearings and the Status of the Investigation; GPO. A final report is to be prepared by mid-2004.

¹⁶⁰ See: WEU. 4 June 2002. Report: *The new challenges facing European intelligence – reply to the Annual Report of the Council*. Forty-Eighth Session. Paris: Document A/1775; 20 pp.

Fiscal and financial pressures have forced the transition in security strategy from *risk avoidance* to *risk management*, to be handled with a threat-based security system, whereby specific emergent risks are assessed and minimized. Thus, *prevention* is now the primary justification for the existence of intelligence services.

Among the new factors of the geopolitical situation, the rising power of 'non-state' actors, the facts that the majority of risks and dangers are transnational and an increasing number of threats are asymmetrical in nature, and then September 11, as a defining moment and political watershed, have deeply modified the former conditions for intelligence practices, and now call into question some of the most fundamental premises of structuring intelligence institutions in democracies.

While a strict separation between external intelligence, internal intelligence, and law enforcement proved workable enough in democracies during the Cold War, 9/11 has changed many of the current rules.¹⁶¹ International terrorism is not only challenging the whole concept of an ordered, free, civil society, internationally and nationally, as well as democratic-constitutional premises of how states protect themselves; it challenges this institutional and legal dichotomy of intelligence services at the core, because it combines features of both internal and external threat and because it operates at an uneasy juncture between them. Though terrorism is not unique or unprecedented in blurring traditional internal/external and state/non-state lines, neither traditional external nor internal models of how to organize and effect protection are fully applicable. This is why counterterrorism initiatives can fall into the categories of significantly helping to combat terrorism, significantly interfering with democratic values, or gaining support from the public and allies. The challenge is to ensure that democratic values are not compromised by steps taken to deal with terrorism.

As it happened, the imperatives of the mission of protecting against terrorism have swung the pendulum away from the protection of the rights of the individual towards protection of the community and ensuring communal safety:

¹⁶¹ See: Gill, Peter. 2002. *Democratic and Parliamentary Accountability of Intelligence Services after September 11*. Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, held in Geneva 3-5 October 2002, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF).

- In the US, the USA Patriot Act¹⁶², signed into law in October 2001, substantially dismantles the regulatory firewall between internal and external intelligence, which was erected in the late 1970s in the wake of the Watergate investigations of intelligence abuses. The CIA and the FBI are now much freer to share information. Non-citizen terrorist suspects can be detained for up to seven days without a hearing, those who are certified as presenting a threat can be held indefinitely, and aliens found to have raised funds for terrorist organizations can be deported. The FBI has been granted greater leeway in gaining access to electronic communications. The US Treasury is empowered to order banks to determine and reveal sources of suspicious accounts, can sanction uncooperative institutions, while US banks are prohibited from dealing with unregulated offshore banks.
- The UK Parliament passed laws comparable to the USA Patriot Act in December 2001¹⁶³, including requirements that communication companies retain accessible records of calls made and e-mails sent as well as the more controversial power of indefinite detention applicable to suspected international terrorists. The UK, moreover, enhanced financial surveillance and restriction authorization, provided for greater inter-agency exchange of intelligence, plans to tighten asylum criteria and to vest immigration officials with the authority to reject asylum claims of those from countries determined to be safe.
- Germany¹⁶⁴ increased law enforcement access to personal and financial data, authorized the prosecution of foreigners associated with foreign terrorist organizations, and the deportation of those perpetrating political violence or otherwise threatening the 'basic order of democratic freedom'.
- France, Italy, Spain, and other countries have strengthened statutory counter-terrorism regimes already in place by new legislation.

The result of the new rules is that they make it substantially easier for the authorities to get access to information about individuals that is held by third parties, such as

¹⁶² Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. For a detailed legal analysis consult the Congressional Research Service (CRS), *Report for Congress: The USA Patriot Act: A legal analysis*. At: <http://www.fas.org/irp/crs/RL31377.pdf>

¹⁶³ Anti-terrorism, Crime and Security Act 2001, which received royal assent on 14 December 2001. At: <http://www.hmso.gov.uk/acts/acts2001/20010024.htm> And: Wood, Edward. 2002. The Anti-Terrorism, Crime and Security Act 2001. Disclosure of Information. House of Commons Library. Research Paper 02/54.

¹⁶⁴ The German Cabinet adopted two comprehensive anti-terrorism packages in September and December 2001.

financial institutions, employers, schools, or health care providers. Departures from constitutional norms justified on anti-terrorism grounds may also subtly alter the culture of the internal intelligence and security institutions themselves. Increasingly, security and intelligence services are allowed to put citizens under surveillance without notifying the suspect, which could constitute a dangerous precedent for infringement of civil rights. Thus, it could be more difficult for citizens, ombudsmen and NGOs to hold governments and their agencies accountable for their activities as they are not necessarily informed about the surveillance activities. Furthermore, immigrants, asylum seekers and foreigners seem more likely to become the target of anti-terrorism measures, with the inherent danger that uncontrolled practices could heighten the tension between different ethnic groups in societies, and erode the legal norm that everyone should be treated equally before the law.

Although the changes in domestic law enforcement and internal intelligence surveillance powers, which were expected to be more radical immediately after 9/11, have turned out to be surprisingly modest, democracies need to strengthen, not to abandon the institutional pillars created. When the value system of democracy is under attack, the system needs to be reinforced. Thus, the swing of the pendulum away from the protection of individual rights towards protection of the community must be counterbalanced through a corresponding increase in democratic control and parliamentary oversight over intelligence, otherwise all are bound to lose, particularly the states in transition.¹⁶⁵ On the other hand: rigid adherence to what are claimed to be constitutional principles can, if applied without perspective – or common sense – be as great a danger to the constitutional order as profligate departures from those principles.

Fortunately, the fact remains that both the US and European governments face significant constraints on their respective capacities for internal intelligence, surveillance, and for policing terrorism domestically. In Europe, the constraints are increasingly robust standards of human rights enacted by the Council of Europe, as well as a chequered history of exposed excesses of the security forces against domestic terrorists. In the US, these include the constitution, its bias against armed forces involvement in domestic security, and the high degree of media scrutiny to which its law enforcement agencies are subjected.

¹⁶⁵ See: Winkler, Theodor, The Implications of 11 September: A Year On. In: *Proceedings of the Second Geneva Centre for the Democratic Control of Armed Forces (DCAF) – IISS Workshop*; Welcome Speech; London, 11-13 July 2002.

Basically, it is mainly the *internal* intelligence services which cause problems with their powers of intrusion on private spaces or communications for intelligence purposes, much less the external intelligence services. External intelligence, focusing predominantly on foreign intelligence about prospective threats, can operate relatively free of legal constraints on how it collects information and what it does with it after acquiring it. Secrecy of methods, protection of sources, and even obscuring that intelligence services are operating at all, are basic principles of activities of external intelligence services. Accountability of external intelligence, to the degree it exists, is usually itself largely effected within a high degree of secrecy.

Hence, combining internal and external intelligence functions – common in former intelligence services of countries in transition – creates the possibility that *internal* intelligence services and law enforcement will be infected by the secrecy, deception, and ruthlessness that the collection of foreign intelligence requires. It is here that control, supervision, and oversight are particularly needed. Clearly dividing responsibilities among the different services reduces that risk. It also creates a tension and competition between the separate services which is itself a safeguard against abuse.

A sharp distinction must be retained between intelligence and law enforcement. Unlike intelligence, law enforcement lives within a very different system of rules and traditions. In a democracy, the most important of these is the idea that before the state can use coercive power, it must provide justification to an impartial body: the judicial branch. Before a state can act on this information against its own citizens, there must be a measure of due process which implies a degree of transparency. The ideal of enforcement of criminal law in an open, democratic society is that the agencies charged with that task should focus on identifying responsibility after crimes have already been committed. They should place the highest value on the collection of information in forms that can be used within the criminal justice system, whether to advance a post-incident investigation or as evidence in a formal, individualized legal proceeding seeking to impose judicial punishment for specific, proven violation of enacted laws. The more law enforcement is brought within the democratic and constitutional process, the more emphasis there is on law enforcement itself being bound in its investigatory work and in how it uses the information it collects by laws and on making law enforcement accountable to the public and to constitutionally responsible political authority. Inculcating those values must remain high on the agenda of reform of law enforcement systems.

Introducing more law enforcement goals to *internal* intelligence operations can provide important guidance on two significant challenges that the new playing fields of counterterrorism and anti-terrorism present: (1) ensuring appropriate and better measurable performance standards; and (2) ensuring greater respect for democratic values.

6. Summary of Conclusions

Several conclusions can be drawn:

1. Intelligence services can and should be defined and regulated by a combination of public law and classified regulations.
2. A system of control, supervision, and oversight is necessary to ensure that the approaches employed for intelligence collection meet defined standards that are acceptable to the society they serve.
3. Legal limitations can be imposed on intelligence collection without weakening their appropriate functions necessary for a democracy. 'Sources and methods' can be legally regulated and subject to oversight without compromising the secrecy needed for their protection.
4. For effective control, supervision, and oversight, laws alone are not enough. There must also be effective ways of interpreting and enforcing these laws, using independent entities and making them publicly accountable. The separation of powers arrangement can create an unusually effective structure to ensure independent control and oversight.
5. Without such control and supervisory structures – laws and independent bodies – the intelligence collection function will be less, not more, effective. Intelligence services will be tempted to resort to less rigorous standards and means of collection and rely upon rather less reliable and legally questionable means of information collection.
6. Reform of intelligence need not conflict with counterterrorism efforts. The events of 9/11 have made it more critical than ever to ensure that both the democratic structures that guarantee democracy are not threatened, and counterterrorism and intelligence operations remain effective.

The central dilemma for intelligence services around the world concerns how to act as a protectorate of democracy, whilst at the same time engaging in secret operations that cannot be disclosed to the public. In democratic societies, all services are forced to confront the problem of achieving a balance between secrecy and openness. Maintaining a degree of transparency of intelligence activities is the best way to ensure democratic accountability and control, which are necessary for raising public awareness and support for the intelligence services. However, one needs to be ever vigilant: the nature of intelligence is such that the balance between secrecy and democracy will always be a delicate one to strike.

Bibliography

General Works

- Aid, Matthew M. and Wiebes, Cees. 2001. *Secrets of Signal Intelligence during the Cold War and Beyond*. Portland OR: Frank Cass.
- Albats, Yevgenia. 1994. *The State within a State: The KGB and Its Hold on Russia – Past, Present, and Future*. New York: Farrar, Strauss and Giroux.
- Andrew, Christopher. 1986. *Secret Service: The Making of the British Intelligence Community*. London: Sceptre.
- Andrew, Christopher and Gordievsky, Oleg. 1991. *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev*. New York: HarperCollins.
- Berkowitz, Bruce D. and Goodman, Allan E. 2000. *Best Truth. Intelligence in the Information Age*. New Haven & London: Yale University Press.
- Black, Ian & Morris, Benny. 1991. *Israel's Secret Wars: A History of Israel's Intelligence Services*. New York: Weidenfels.
- Caldwell, George. 1992. *Policy Analysis for Intelligence*. Center for the Study of Intelligence. Washington D.C.: CIA.
- Central Intelligence Agency. July 1995. *A Consumer's Handbook to Intelligence*. Doc. No. PAS 95-00010. Washington D.C.: CIA.
- Clark, Robert M. 1996. *Intelligence Analysis: Estimation and Prediction*. Baltimore: American Literary Press.
- Dearth, Douglas H. and Goodden, Thomas R. eds. 1995. *Strategic Intelligence: Theory and Approach*. 2nd ed. Washington D.C.: DIA, Joint Military Intelligence Training Center.
- Eftimiades, Nicholas. 1994. *Chinese Intelligence Operations*. Annapolis: U.S. Naval Institute Press.
- Elkins, Dan. 1997. *An Intelligence Resource Manager's Guide*. Washington D.C.: Joint Military Intelligence Training Center. Defense Intelligence Agency.
- Henderson, Robert D'A. 2002. *Brassey's International Intelligence Yearbook*. 2002 ed. Washington D.C.: Brassey's.
- Herman, Michael. 1996. *Intelligence Power in Peace and War*. New York: Cambridge University Press.
- Johnson, Loch K. 1996. *Secret Agencies: U.S. Intelligence in a Hostile World*. New Haven: Yale University Press.
- Kahn, David. 1996. *The Codebreakers*. Rev. ed. New York: Scribner.

- Kent, Sherman. 1949. *Strategic Intelligence for American World Policy*. Princeton: Princeton University Press.
- Knight, Amy. 1996. *Spies without Cloaks: The KGB's Successors*. Princeton: Princeton University Press.
- Koehler, John O. 2000. *Stasi: The Untold Story of the East German Secret Police*. Boulder: Westview.
- Laquer, Walter. 1985. *A World of Secrets: The Uses and Limits of Intelligence*. New York: Basic Books.
- Lindgren, Davit T. 2000. *Imagery Analysis in the Cold War*. Annapolis: U.S. Naval Institute Press.
- Lowenthal, Mark M. 1994. *The U.S. Intelligence Community: An Annotated Bibliography*. New York: Garland.
- Lowenthal, Mark M. 2003. *Intelligence. From Secrets to Policy*. 2nd ed. Washington D.C.: CQPress. A Division of Congressional Quarterly Inc.
- Moynihan, Daniel Patrick. 1998. *Secrecy: The American Experience*. New Haven: Yale University Press.
- Nye, Joseph S. 1994. *Estimating the Future*. Washington D.C.: Consortium for the Study of Intelligence.
- Raviv, Dan and Melman, Yossi. 1990. *Every Spy a Prince: The Complete History of Israel's Intelligence Community*. Boston: Houghton Mifflin.
- Richelson, Jeffrey T. 1999. *The U.S. Intelligence Community*. 4th ed. Boulder: Westview Press.
- Shulsky, Abram N. and Schmitt, Garry J. 1983. *Silent Warfare: Understanding the World of Intelligence*. 2nd rev. ed. Washington D.C.: Brassey's.
- Smith, Michael. 1996. *New Cloak, Old Dagger: How Britain's Spies came in from the Cold*. London: Gollancz.
- Steele, Robert D. 2000. *On Intelligence: Spies and Secrecy in an Open World*. Oakton VA: OSS Academy.
- Steury, Donald P. ed. 1994. *Sherman Kent and the Board of National Estimates*. Washington D.C.: History Staff, Center for the Study of Intelligence. CIA.
- Thomas, Gordon. 1999. *Gideon's Spies: Mossad's Secret Warriors*. New York: St. Martin's.
- Treverton, Gregory F. 2001. *Reshaping National Intelligence for an Age of Information*. New York: Cambridge University Press.
- Urban, Mark. 1996. *UK Eyes Alpha: The Inside Story of British Intelligence*. London: Faber & Faber.
- Waller, Michael J. *Secret Empire: The KGB in Russia Today*. Boulder: Westview Press.

Conference Papers¹⁶⁶

Banisar, David. Freedom of Information International Trends and National Security.

Born, Hans. Parliamentary Oversight of Intelligence Services. The Need for Efficient and Legitimate Intelligence.

Born, Hans and Tuler, Matias. Parliamentary Democracy and Intelligence: Comparing Legal Frameworks of United Kingdom, Canada, Ukraine, Czech Republic, Turkey and South Africa.

Bozhilov, Nikolai. Reforming the Intelligence Services in Bulgaria. The Experience from the Last Decade.

Caparini, Marina. Challenges of Control and Oversight of Intelligence Services in a Liberal Democracy.

Černý, Oldřich. Czechoslovak (Czech) Intelligence After the Cold War.

Faupin, Alain. Reform of the French Intelligence Services after the End of the Cold War.

Gill, Peter. Democratic and Parliamentary Accountability of Intelligence Services after September 11th.

Haering, Barbara. Investigating the Strategic Intelligence Service of Switzerland: Experience of a Parliamentarian.

Leigh, Ian. The UK's Intelligence and Security Committee.

Lotz, George. Intelligence Oversight: Balancing National Security and Constitutional Rights.

Majtény, László. Reconciliation and Developing Public Trust: Opening State Security Files to the Public.

Szabó, Károly F. Parliamentary Overview of Intelligence Services in Romania.

Wark, Wesley K. Canada's Access to Information Act and the Canadian Security and Intelligence Community.

Watts, Larry L. Control and Oversight of Security Intelligence in Romania.

Wijnen Riems, Joy M. Historical Overview: National Security Service (BVD) to General Intelligence and Security Service (AIVD).

¹⁶⁶ Papers presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, held in Geneva 3-5 October 2002, organized by the Geneva Centre for the Democratic Control of Armed Forces (DCAF). Available at: http://www.dcaf.ch/news/Intelligence%20Oversight_051002/ws_papers/ws_papers.htm

Wijnen Riems, Joy M. Developments Relating to National Security (Annual Report 2001).

Zybertowicz, Andrzej. Transformation of the Polish Secret Services: From Authoritarian to Informal Power Networks.



Established in 2000 on the initiative of the Swiss government, the Geneva Centre for the Democratic Control of Armed Forces (DCAF), encourages and supports States and non-State governed institutions in their efforts to strengthen democratic and civilian control of armed and security forces, and promotes international cooperation within this field, initially targeting the Euro-Atlantic regions.

The Centre collects information, undertakes research and engages in networking activities in order to identify problems, to establish lessons learned and to propose the best practices in the field of democratic control of armed forces and civil-military relations. The Centre provides its expertise and support to all interested parties, in particular governments, parliaments, military authorities, international organisations, non-governmental organisations, academic circles.

Geneva Centre for the Democratic Control of Armed Forces (DCAF):
rue de Chantepoulet 11, P.O. Box 1360, CH-1211 Geneva 1, Switzerland
Tel: ++41 22 741 77 00; Fax: ++41 22 741 77 05
E-mail: info@dcaf.ch
Website: <http://www.dcaf.ch>