ACTIVITY REPORT 2008
ACTIVITY REPORT 2009

ACTIVITY REPORT 2008
ACTIVITY REPORT 2009

Investigations and Recommendations

Belgian Standing Intelligence Agencies Review Committee

Belgian Standing Intelligence Agencies Review Committee

intersentia
Antwerp – Oxford – Portland

The Dutch and French language versions of this report are the official versions. In case of conflict between the Dutch and French language versions and the English language version, the meaning of the first ones shall prevail.

Activity Report 2008. Activity Report 2009. Investigations and Recommendations
Belgian Standing Intelligence Agencies Review Committee

Belgian Standing Intelligence Agencies Review Committee
Rue de la Loi 52, 1040 Brussels – Belgium
++32(0)2 286 28 11
info@comiteri.be
www.comiteri.be

ISBN 978-94-000-0091-9
D/2010/7849/86
NUR 823

CONTENTS

LIST OF ABBREVIATIONS

ATG	Mixed Anti-Terrorist Group (*Antiterroristische gemengde groep – Groupe interforces anti-terroriste*)
CANPAN/CANVEK	Advisory Committee for the Non-Proliferation of Nuclear Weapons *(Commissie van advies voor de niet-verspreiding van kernwapens – Commission d'avis pour la non-prolifération des armes nucléaires)*
CBRN	Chemical, biological, radiological and nuclear weapons
Classification Act	Act of 11 December 1998 on classification and security clearances, certificates and advice (*Wet betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen – Loi relative à la classification et aux habilitations, attestations et avis de sécurité)*
CRI	Centrally registered informant
CUTA	Coordination Unit for Threat Assessment (*Coördinatieorgaan voor de dreigingsanalyse – Organe de coordination pour l'analyse de la menace*)
Data Protection Act	Act of 8 December 1992 on privacy protection in relation to the processing of personal data (W*et tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens – Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*)
DRC	Democratic Republic of the Congo
ECHR	European Court of Human Rights
FANC	Federal Agency for Nuclear Control *(Federaal agentschap voor nucleaire controle – Agence fédérale de contrôle nucléaire)*
FPS	Federal public service
GCCR	Governmental Coordination and Crisis Center
GISS	General Intelligence and Security Service of the Armed Forces (*Algemene Dienst inlichting en veiligheid van de Krijgsmacht – Service général du renseignement et de la sécurité des Forces armées*)

HUMINT	Human intelligence
Intelligence Services Act	Act of 30 November 1998 on the intelligence and security services (*Wet houdende regeling van de inlichtingen- en veiligheidsdienst – Loi organique des services de renseignement et de sécurité*)
MCI&S	Ministerial Committee for Intelligence and Security (*Ministerieel Comité voor inlichting en veiligheid – Comité ministériel du renseignement et de la sécurité*)
MONUC	UN Mission in the Democratic Republic of the Congo
MTCR	Missile Technology Control Regime
NATO	North Atlantic Treaty Organisation
NGD	National General Database
NSA	National Security Authority *(Nationale Veiligheids-overheid – Autorité nationale de sécurité)*
OI	Occasional informant
POC	Point of contacts
RD CUTA	Royal Decree of 28 November 2006 (see the Threat Assessment Act)
Review Act	Act of 18 July 1991 governing the review of police and intelligence services and of the Coordination Unit for Threat Assessment (W*et tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse – Loi organique du contrôle des services de police et de renseignement et de l'organe de coordination pour l'analyse de la menace*)
SEP	Scientific and economic potential
SIGINT	Signal intelligence
SITCEN	EU Joint Situation Centre
Special Intelligence Methods Act	Act of 4 February 2010 on the data collection methods by the intelligence and security services (*Wet betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten – Loi relative aux méthodes de recueil de données par les services de renseignement et de sécurité)*
Special Investigative Act	Act of 6 January 2003 on particular methods to be used by police services designated by the Minister of Justice in the framework of investigations (*Wet betreffende de bijzondere opspringsmethoden en enige andere onderzoeksmethoden – Loi concernant les*

	méthodes particulières de recherche et quelques autres méthodes d'enquête.
Standing Committee I	Standing Intelligence Agencies Review Committee (*Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – Comité permanent de contrôle des services de renseignement et de sécurité)*
Standing Committee P	Standing Police Monitoring Committee (*Vast Comité van Toezicht op de politiediensten – Comité permanent de contrôle des services de police)*
State Security	State Security (*Veiligheid van de Staat – Sûreté de l'Etat*)
Threat Assessment Act	Act of 10 July 2006 on Threat Assessment (*Wet betreffende de analyse van de dreiging – Loi relative à l'analyse de la menace*)

INTRODUCTION

The Belgian Standing Intelligence Agencies Review Committee (hereafter Standing Committee I) is a permanent and independent review body. It was set up by the Review Act of 18 July 1991 and has been operational since May 1993.

The Standing Committee I is responsible for reviewing the activities and functioning of the two Belgian intelligence services: the civil intelligence service, State Security, and his military counterpart, the General Intelligence and Security Service. In addition, it supervises the functioning of the Coordination Unit for Threat Assessments and his various supporting services.

The review relates to the legitimacy (supervision of observance of the applicable laws and regulations), effectiveness (supervision of the efficiency of the intelligence services), and coordination (the mutual harmonisation of the work of the services concerned). With regard to the supporting services of the Coordination Unit for Threat Assessments, the review only relates to their obligation to pass on information on terrorism and extremism.

The Standing Committee I is a collective body and is composed of three members, including a chairman. They are appointed by the Senate. The Standing Committee I is assisted by a secretary and his administrative staff, and by an Investigation Service.

The Standing Committee I performs its review role through investigations carried out on its own initiative or on the request of the Senate, the Chamber of Deputies or the competent minister or authority. Additionally, the Standing Committee I can act on request of a citizen and of any person holding a civil service position, as well as any member of the armed forces, who has been directly concerned by the intervention of one of the intelligence services.

The Standing Committee I and its Investigation Service have many powers. For example, the reviewed services must send, on their own initiative, all documents governing the conduct of the members of the service, and the Committee can request any other text or document. The fact that many documents of the intelligence services are classified in accordance with the Classification Act of 11 December 1998, does not detract from this. Indeed, all employees of the Committee hold a security clearance of the "top secret" level. The Committee can also question anybody. The members of the reviewed services can be summoned if necessary and required to testify under oath. Furthermore, the supervisory body can make all useful findings and seize all objects and documents in any

location. Finally, the Committee can demand the assistance of experts and interpreters, and the assistance of the police.

Pursuant to Article 35 of the Review Act of 18 July 1991, the Standing Committee I annually draws up a general activity report. These activity reports are drawn up in Belgium's national languages Dutch and French and can be found on the website of the Committee (www.comiteri.be). With increased globalisation in mind, the Standing Committee I wishes to meet the expectations of a broader public. The sections of the activity reports 2008 and 2009 that are most relevant to the international intelligence community (the investigations, the recommendations and the table of contents of the complete activity reports), have therefore been translated into English.

Guy Rapaille, Chairman
Gérald Vande Walle, Counsellor
Peter De Smet, Counsellor
Wouter De Ridder, Secretary

1 September 2010

ACTIVITY REPORT 2008

TABLE OF CONTENTS OF THE COMPLETE ACTIVITY REPORT 2008

PREFACE

"Experientia mutua omnibus prodest" or "*Mutual experience benefits all*". With this piece of wisdom in mind, and with the full support of its parliamentary Monitoring Committee of the Senate, in 2008, the Standing Committee I took the first steps towards establishing a 'European Centre of Expertise for parliamentary review bodies of intelligence and security services'.

What is the aim of this Centre? Reviewing intelligence and security services is not an easy task, for many reasons. Moreover, democratic review in this field is a rather recent phenomenon. In addition, intelligence work – unlike the democratic review of this work – has a strongly international character. With its initiative, the Committee intends to take these findings into account as much as possible by creating a platform – in the form of a secure, interactive website – where parliamentary review bodies can exchange questions and best practices and where they can share information about legislation, investigation reports and scientific reports with their homologous review bodies.

After all, even though 'who reviews what and how' differs from country to country, there is common ground which means that the exchange of information and knowledge can bring added value for all concerned.

The idea of setting up the Centre of Expertise was launched during a meeting with homologous review bodies in Norway. The Committee's plans were taken up there by the *UN Special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*. He expressed them as follows in his final report of 4 February 2009 on '*The role of intelligence agencies and their oversight in the fight against terrorism*': "*The Special Rapporteur supports the idea, developed by the Belgian Standing Committee I, of setting up a permanent knowledge-sharing platform for (parliamentary) review bodies of intelligence services, where best practices on legislation, jurisprudence and general developments in the field can be shared, thereby supporting the professionalization of the review bodies of Member States.*"

Of course, the establishment of this Centre of Expertise will take time. It requires thorough preparation and the approval and cooperation of the homologous European services. With this in mind, in 2008 the Committee contacted other parliamentary review bodies, resulting in mainly positive opinions. In 2009, continued investments will be made towards setting up the Centre. In this regard, the Standing Committee I has only one goal in mind: a better democratic review of the operation of the intelligence and security

services. Even though the Standing Committee I always strives for extensive professionalism when carrying out its assignments, it is fully aware that this Centre of Expertise will mean added value for the Committee itself. Foreign examples and solutions can indeed act as inspiration for the Committee to carry out its own core assignments.

Guy Rapaille,
Chairman of the Standing Intelligence Agencies
Review Committee

1 June 2009

CHAPTER II
INVESTIGATIONS

In 2008, the Standing Committee I initiated nine investigations: five as a result of a complaint by a private individual[1], two on its own initiative, one at the request of the Minister of Justice and a last one at the joint request of the Minister of Justice, the Minister of Defence and the Monitoring Committee of the Senate. Two of these investigations – with regard to an aspect of the operation of the Coordination Unit for Threat Assessment (CUTA) – were carried out jointly with the Standing Committee P in accordance with the Review Act of 18 July 1991.

Also in 2008, nine investigations were completed and three interim reports were drawn up for one particular investigation.[2] In addition, investigation procedures were initiated in thirteen different cases. This chapter will first discuss the completed investigations (II.1 to II.10). Then follows a summary and a brief description of the investigations in which important investigative steps were taken in the course of the operating year 2008 but which could not be completed as yet (II.11).

Finally, it is worth mentioning that in 2008 the Standing Committee I enlisted the help of one external expert who was requested to formulate an advisory opinion within the framework of the investigation into the fight against proliferation (II.4).

II.1. THE TERROR ALARM AROUND THE TURN OF THE YEAR[3]

In December 2007, the CUTA declared the highest level of threat for Brussels based on indications of a 'serious and very imminent' threat of a terrorist attack.

---

1 The Committee received a total of fifteen complaints from private individuals. Five of those resulted in the initiation of an investigation. Eight complaints were not acted upon because they appeared to be – following a verification of a number of details – manifestly unfounded (Art. 34 of the Review Act) or because the Committee was not competent for the matter in question. In these last cases, the complainants were referred to the competent authority. For two of the complaints, it could not be decided till end 2008 what action needed to be taken.

2 This concerns the investigation into the Belliraj case (II.3).

3 For the complete version of this investigation report, refer to: *Print.*, House of Representatives, 2007-2008, 1385/1 and Senate, 2007-2008, 872/1.

This created a great deal of commotion; some even claimed that this assessment had been prompted by political motives. This led to the initiation of a joint investigation by the Standing Committee I and the Standing Committee P into the manner in which the CUTA had assessed the terror threats during the turn of the year 2007-2008. Likewise, the intelligence and police services were questioned by their respective review bodies regarding their contribution.

II.1.1. THE VARIOUS THREAT ASSESSMENTS

In its weekly assessment of 12 December 2007, under the heading '*Assessment of the terrorist threat during the end-of-year period/holidays*' (free translation), the CUTA had stated that the terrorist threat should be considered as average (Level 2[4]). It was only at certain locations that an '*increased vigilance and a physical police presence was advised*' (free translation). But a few days later – on 17 December – there was a sudden change in this assessment. On that day, the Federal Prosecutor's office informed the Director of the CUTA about the status of a judicial inquiry conducted by the Brussels Federal Judicial Police. Several police sources had evidently referred to an upcoming attack, mentioning the location (the Grand Place in Brussels and the streets and squares giving out onto the Grand Place), the time (end-of-year period) as well as the resources to be used by the terrorists. Since the Federal Prosecutor considered this information to be serious and reliable, he took the initiative to arrange a meeting with the CUTA and the Federal Police with the intention of allowing the Coordination Unit to draw up an ad hoc threat assessment. The intelligence services were not invited to this meeting. Since the Federal Prosecutor did not want to jeopardise the investigation, he invoked the so-called embargo procedure (see II.1.3.4) so that the judicial information would only be communicated to the Director of the CUTA.[5] During or as a result of this meeting, the Director drew up a new assessment and the threat level for the Brussels-Capital Region was raised to 'Level 4'[6] from the end of the Islamic Festival of Sacrifice (i.e. 21 December 2007).[7] This assessment was immediately sent out, though not to all regular addressees of the CUTA. Only the Prime Minister, the Minister of the Interior,

---

4 This means that the '*threat against the person, the group or the event which is the subject of the assessment is not very plausible*' (Art. 11, § 6, RD CUTA – free translation).

5 What these elements precisely were, was not communicated to the Committees by the Director of the CUTA. He wanted to invoke the secrecy of the ongoing judicial inquiry (see II.1.3.1). However, the Federal Prosecutor did inform the Standing Committee P about the specific information involved.

6 This means: '*very serious*', *i.e. 'if it appears that the threat against the person, the group or the event which is the subject of the assessment is serious and imminent*' (Art. 11, § 6, RD CUTA – free translation).

7 Although several elements contributed to this decision, it appeared that this decision was *almost* entirely prompted by information from a judicial inquiry.

the Minister of Justice, the Federal Prosecutor, the Director-General of State Security, the Head of the General Intelligence and Security Service (GISS), the Governmental Coordination and Crisis Centre (GCCR), Federal Police/DJP/Terro and the Federal Judicial Police of Brussels received a copy.[8] The decision not to inform all the services was prompted by the concern that this would jeopardise the ongoing investigation. For the same reasons, veiled wording was used in the assessment and it was classified as 'SECRET – Act of 11.12.1998'.

On the next day – 18 December 2007 – several consultations took place. In the morning, State Security and the GISS attended a meeting with the Federal Police. The latter wished to know whether these services had any information about the alleged attack. In the afternoon, the intelligence services attended a second meeting, this time at the invitation of the CUTA. After these meetings, State Security and the GISS questioned their field operators and informed their human sources, but without result.

A day later, after making use of the received information, State Security sent its reply to the Federal Prosecutor within the framework of its cooperation with the judicial authorities. The CUTA was, however, not informed at that time.

On 19 December 2007 also, the CUTA drew up a new weekly assessment and disseminated this to all regular addressees. This retained a 'Level 2' threat for the whole country and – to avoid jeopardising the judicial inquiry – no mention was made of the assessment of 17 December which had stated that the threat level would become 'very serious' from 21 December.

Yet another event occurred on 19 December that would later give rise to discussion between State Security and the CUTA. A foreign counterpart service of the CUTA contacted the Belgian Coordination Unit to report that a certain European intelligence service had valuable intelligence at its disposal and that this service should be contacted thereto. In view of the delicate and urgent nature of the situation, the CUTA immediately contacted the foreign intelligence service.[9] The CUTA received the information by telephone but at the same time explicitly requested that this intelligence be shared with the Belgian 'sister service', State Security, which was also evidently done. Yet it was notable that, at that time, the foreign intelligence service requested State Security to treat the information – which it had earlier communicated to the CUTA without restrictions – as confidential (see below). This meant that State Security had to invoke the embargo procedure. Only after fairly long consultations with the Director of the CUTA regarding the exact wording of the information with a

---

8 Indeed, Article 11 of the Threat Assessment Act states that in case of an embargo procedure, the Director of the CUTA and the Federal Prosecutor jointly decide about which authorities are to be informed of the assessment. However, it is notable that it was the Federal Prosecutor who expressly stated that the General Commissioner of the Federal Police should not be informed of the assessment (see further under II.1.3.6).

9 Article 8, 3° of the Threat Assessment Act only states that the CUTA must maintain contacts with foreign or international homologous services.

view to its further dissemination, was the foreign intelligence officially introduced into the CUTA circuit on 21 December 2007.[10] This information was subsequently mentioned in guarded terms in an undated assessment classified 'SECRET', for which a 'Level 4' was retained. This assessment was, in consultation with the Director of the CUTA and the Director-General, only communicated to the Prime Minister, the Minister of the Interior, the Minister of Justice, the Federal Prosecutor and the Director-General of State Security. It is notable that neither the GISS, nor any police service was allowed to receive this assessment.

But an even more significant event occurred on 21 December. Within the framework of the judicial inquiry leading to the threat assessment of 17 December, premises were searched in the early hours of the morning. Naturally, as a result of this the argument of the risk of compromising the investigation lost its relevance. The applicable threat level could therefore be made public. But this did not happen immediately: on 22 December 2007, the 'Level 2' applicable with respect to the outside world since 12 December 2007 was first raised to 'Level 3'. This was done partly on the basis of information from State Security.[11] All regular addressees were informed of this assessment. It was only later that day that the threat level for Brussels was increased to 'very serious'. So, the estimated 'Level 4' (under embargo) from as early as on 17 December 2007 was confirmed after a renewed assessment of the situation. The reasons for raising this to the highest level were as follows:

- the judicial action had not provided any 'solutions' in terms of eliminating the threat, as a result of which the judicial information remained as relevant as before;
- an SMS action in certain circles provided an additional indication;
- on 22 December 2007, a supporting service and the Federal Prosecutor's office provided certain information which could not, however, be disclosed owing to the embargo;
- arrests made in the Netherlands which, though no concrete connection with the Belgian dossier could be proved, did indicate existence of a context of increased risk in the EU.

This assessment was classified as 'SECRET' and disseminated to the Chairman and the members of the Ministerial Committee for Intelligence and Security (MCI&S), the Federal Prosecutor, the GCCR, State Security, the GISS and the investigation department of the Federal Judicial Police of Brussels responsible for the fight against terrorism and extremism.

---

10 However, this information had no influence on the assessment of 19 December 2007.

11 '*Additional intelligence supplied to the CUTA necessitates the raising of the threat level: State Security informs us on 22/12/2007 at 6.16 pm of a chain of SMS messages circulating in the Muslim community in Brussels, within the framework of the threat related to Nizar Trabelsi. These messages contain a list of 'sensitive' areas to be avoided, i.e. zones which are under police surveillance, as reported in the media' (free translation).*

From 22 December 2007 onwards, the meetings and assessments followed one another in rapid succession. The concerned services also regularly exchanged information. For example, on 24 December 2007 the CUTA received information from State Security about the investigation in the Netherlands. Another assessment followed on Boxing Day. This took into account the information provided by State Security, the report of the GISS of a possible bomb attack in Brussels and elements from earlier assessments. The threat level was retained at 'Level 4'. The same level was also expressly maintained on 31 December 2007, after an assessment based on the arrests made in the Netherlands.

It was only on 3 January 2008 that the threat level was lowered once again: under embargo, the level was brought back to '3' because the end-of-year period had passed and, according to the then Director of the CUTA, because of the destabilising effect of the judicial action of 21 December 2007 on potential perpetrators.

II.1.2. THE MANNER IN WHICH THE VARIOUS PARTIES INVOLVED HAVE PERFORMED THEIR LEGAL ASSIGNMENTS

II.1.2.1. The Coordination Unit for Threat Assessment

According to the Committees, there was no indication that the CUTA had not functioned as it should have in this case. However, it was true that – owing to the secrecy of the judicial inquiry and the fact that the management of the CUTA had invoked its right to silence (see II.1.3.1) – the Committees did not have a basic view of the actual judicial information resulting in the declaration of 'Level 4'. But the Committees did receive information via the judicial authority and the intelligence services which, in the absence of any proof to the contrary, led them to conclude that there had been no dysfunction in the operation of the CUTA. Considering the content of the information apparently communicated to the CUTA, the Committees did not find it at all unreasonable that ad hoc threat assessments were drawn up as 'Level 4'. The Committees were also of the opinion that any reasonable person in the same circumstances could be expected to make a similar decision. The Committees did not have any indication whatsoever of the fact that the declared threat level was supposedly prompted or influenced by a political agenda.

As mentioned, the CUTA did not receive any information in this case from other supporting services which could either confirm or refute the available judicial information. This is because the material had been submitted under the '*single authority*' principle. This is undoubtedly significant: *cross-checking* the information and a multidisciplinary assessment – as intended by the legislator when establishing the CUTA – was therefore not possible in this case. Yet

everything pointed to the fact that the CUTA, irrespective of this handicap, has tried to perform its role as optimally as possible. In fact, the intervention of the CUTA had not been entirely fruitless. Firstly, there were the CUTA assessments which meant that the intelligence supplied by the Federal Prosecutor's office could be accompanied by crucial peripheral information of a general nature. Furthermore, the CUTA functioned as a dynamic contact point for the Federal Prosecutor and the Federal Police. Finally, for the service providing the information, the existence and *élan* of the CUTA also proved a critical and imperative platform for continuous assessment.

An additional problem in this case was the lack of an 'internal sounding board' because the intelligence had been supplied under embargo. In view of the strict wording of Articles 11 and 12 of the Threat Assessment Act, one could assume that only the Director (according to the letter of the law) and the Deputy Director of the CUTA (according to the spirit of the law as well) were allowed to be informed of this information (also see II.1.3.4). This means that there was little or no opportunity for contradiction or consultation within the CUTA. The entire assessment and decision process rested on the shoulders of the management. Enlisting the help of the available analysts within the CUTA was extremely difficult, if not impossible.

In its assessments, the CUTA applied its usual matrix comprising two criteria, i.e. the severity and the probability of the events. The Committees wondered whether this method could still be considered as a sufficient and reliable basis for threat assessments and whether one needs to look for a more sophisticated methodology. In this regard, the Committees are well aware that 'assessments' are not an exact science. Moreover, any prudent individual will always prefer certainty over uncertainty regarding the assessment of a terror threat. Furthermore, the CUTA cannot or should not be expected to verify the truthfulness of the material supplied by a supporting field service. That is not its task.

Finally, the Committees noted that, in their assessment of 12 December 2007, the CUTA had stated that a '*physical police presence is advised*' (free translation). The Standing Committee P and the Standing Committee I were of the opinion that such vague comments were out of place in a threat assessment. They are not in the least helpful for the responsible authorities and can be interpreted by them as a sort of 'umbrella' clause. The Committees are therefore of the opinion that the CUTA must either not express any views regarding the measures to be taken (see also II.1.3.9) or must strive towards being 'concrete' in order to provide added value for the responsible authorities.

II.1.2.2. The intelligence services

The Standing Committee I has been unable to establish whether or not State Security and the GISS have voluntarily withheld information or intelligence which they were obliged to communicate to the CUTA. Neither has the

Committee found any signs of obstruction, lack of cooperation or willingness to cooperate, carelessness, disloyalty or indifference. The Committees therefore concluded that the intelligence services appear to have discharged their legal assignments to the best possible extent.

It was, however, established that the intelligence services have been able to supply little relevant information. However, State Security and the GISS independently stated that this was because, despite repeated requests, they were denied – what they considered – essential, contextualised information regarding the origin of the data supplied by the Federal Police. As a result, they could not ask their sources targeted questions and no information could be collected to either confirm or refute a threat.

The Federal Prosecutor could not agree with this statement. He stated that all information relevant for the intelligence services had been communicated, albeit after taking into account the interests of the ongoing preliminary criminal investigation. In his opinion, these services were unable to deliver anything because they did not have any information. He appeared disappointed about the contribution of State Security in this dossier.

The Committees do not have any elements of information that enable them to take a standpoint in this discussion. Furthermore, the Committees are not authorised to carry out a review related to the judicial authorities. The Committees were only able to establish that there was a difference of view on this point between the intelligence services and the Federal Prosecutor's office.

II.1.2.3. The police services

Within the framework of the investigation into the operation of the CUTA and based on the meeting between the Standing Committee P and the Federal Prosecutor, no elements have emerged which could indicate that the Federal Police had not properly discharged its legal obligations with respect to the CUTA. The Federal Police appeared *prima facie* to have passed on the relevant information to the CUTA via the Federal Prosecutor's office. The Committees emphasised, however, that they have not carried out any further investigation into the actual information flow from the police, the way in which the police received its information and the *link* with the Federal Prosecutor's office.

II.1.3. POINTS OF ATTENTION

II.1.3.1. An ongoing criminal investigation and review by the Standing Committees

In this investigation, the Director of the CUTA invoked Article 24, § 2, second paragraph and Article 48, § 2, second paragraph of the Review Act for not

communicating any information supplied by the Federal Prosecutor to the Committees. These provisions state that the members of police services, intelligence services and the CUTA are bound to disclose the secrets they are aware of to the Standing Committee P and the Standing Committee I '*except if those secrets relate to an ongoing criminal investigation or judicial inquiry*' (free translation). In other words, if the information concerns an ongoing preliminary criminal investigation, any staff member *may* invoke this exception. However, this Article is stated in very general terms and implies that any staff member can make it almost impossible for the Standing Committees to carry out a quick investigation. Moreover, no form of verification is provided. This means that even a completely arbitrary application of this article will lead, at the very least, to serious delays in investigations since the Committees are obliged to wait for the completion of the criminal investigation. As a result of this, investigations can lose their strength and pertinence.[12]

In this particular investigation where, for a proper and complete understanding of the facts, it was essential that the Committees were at least given the right to inspect all assessments, the decision of the management of the CUTA has *in concreto* caused little hindrance.[13] Since, a lot of information was obtained via the Federal Prosecutor's office or State Security. But it is precisely owing to the active cooperation of these two services that the attitude of the management of the CUTA, although perfectly legitimate, did not really come over *de facto* as well-founded or convincing. Therefore, the Committees asked themselves whether some kind of *overruling* system should be considered in this respect.[14]

II.1.3.2. The Classification Act and reporting by the Standing Committees

Considering the sizeable number of classified documents, the editing of a conclusive report for the benefit of the Parliament was also seriously hampered in this investigation. This is because only those persons who are holders of a security clearance and who have a *need to know*, may receive classified information (Art. 8 of the Classification Act). There are strict penalties applicable to the members of the Committees for the violation of these provisions (Art. 11 of the Classification Act, Article 458 of the Penal Code and Article 64 of the

12 The Article, however, is also applicable in the 'opposite' sense: a member of a police or intelligence service or of the CUTA would be able to disclose these secrets *without*, for example, the Director of the CUTA or the Federal Prosecutor being able to prevent this. It seems very surprising that, for instance, a police officer can do this without the authorisation of the Federal Prosecutor.

13 But it could have also turned out differently and resulted in a showdown between the Committees and the concerned authorities.

14 Also see Chapter VIII.3.1, *Activity Report 2008*.

Review Act). Neither the Classification Act nor the Review Act provide any exceptions to this rule with respect to the Parliament.

II.1.3.3. Classification of assessments

As described above, certain assessments were classified by the CUTA. The question that arises is whether this was legally permitted. Since, information may only be classified if the inappropriate use thereof can harm one of the interests defined exhaustively in Article 3 of the Classification Act.[15, 16] Besides, the 'investigation secrecy' or the 'success of a judicial inquiry' has not been set out verbatim in this provision. With a lot of good will, one might be able to account for the classification by referring to the '*internal security of the State*' but according to the Committees, this appears forced.

II.1.3.4. Scope of the embargo procedure

Articles 11 and 12 of the Threat Assessment Act state that intelligence falling under the embargo procedure '*shall be sent exclusively to the Director of the CUTA*'. According to the Director-General of State Security, the text of the Act must be interpreted literally and the Deputy Director is to be excluded from receiving this information. But the management of the CUTA rightly feels that such a reading of the Act creates serious problems in practice. Assuming that the embargo procedure continues for a long time or that there are several ongoing embargos, it is simply impossible to expect that these will be managed exclusively and personally by the Director. This would mean that he must be permanently available. At this point, one may ask oneself what the role of the Deputy Director is. It is essential to amend this Act in order to remove this lack of clarity.[17]

II.1.3.5. Concurrence of two different embargo procedures

The embargo procedure from Article 11 of the Threat Assessment Act implies that intelligence, which in the opinion of the Federal Prosecutor could jeopardise

---

15 The defence of the immunity of the national territory and the military defence plans; the performance of the assignments of the armed forces; the internal security of the State including in the area of nuclear energy, and the continued existence of the democratic and constitutional order; the external security of the State and the international relationships of Belgium; the scientific and economic potential of the country; any other fundamental interest of the State; the safety of the Belgian nationals abroad; the operation of the decision-making bodies of the State; the safety of the persons to whom special protective measures have been granted pursuant to Article 104, § 2 of the Code of Criminal Procedure.

16 The question regarding the justification of the level of classification, also remains. Since, the classification level 'SECRET'may only be granted if the inappropriate use of this classification can cause 'serious harm' to one of the above-mentioned interests.

17 See Chapter VIII.2.1, *Activity Report 2008.*

either the criminal proceedings or the safety of persons if communicated to the CUTA, is sent exclusively to the Director of the CUTA. The Director and the Federal Prosecutor jointly decide on the items of information to be included in the assessment and the authorities who are to be then informed of this assessment. If both are of the opinion that the intelligence is indispensable for taking the necessary measures for the protection of persons, then this intelligence is included in the assessment.[18]

Article 44/8 of the Police Function Act states that the compulsory forwarding of police data to the National General Database (BNG/ANG) may be postponed if the competent magistrate, in agreement with the Federal Prosecutor, is of the opinion that this may jeopardise the course of the criminal proceedings or the safety of persons.

A simultaneous application of the above-mentioned Articles limits the possibilities for the dissemination of intelligence. Moreover, an application of the embargo procedure on the basis of the Police Function Act implies that information from the preliminary criminal investigation is not transferred to the BNG/ANG and therefore, cannot or may not reach the CUTA via that channel. This information is subsequently sent to the CUTA on the basis of Article 6 *in conjunction with* Article 11 of the Threat Assessment Act. This, however, raises the question as to what needs to be done if an embargo procedure is declared on the basis of the Police Function Act and at the same time the police services are obliged, pursuant to Article 6 of the Threat Assessment Act, to communicate all relevant intelligence. The two Articles appear contradictory or at least difficult to combine and not tuned to one another. In practice, one can probably assume that in such cases matters will be handled via the (Federal) Prosecutor's office, although the two embargo procedures differ. The embargo procedure arising out of the Police Function Act is declared by a local magistrate (public prosecutor, labour prosecutor or examining magistrate) in agreement with the federal magistrate, while the procedure arising from the Threat Assessment Act is declared by the Federal Prosecutor.

II.1.3.6. Addressees of the CUTA assessments

At the explicit request of the Federal Prosecutor, the assessment of 17 December 2007 was not sent to the General Commissioner of the Federal Police. On the other hand, certain departments of the Federal Police (DJP/Terro and the Brussels Federal Judicial Police) were informed of this assessment. But the Federal Prosecutor stated that this had not been done intentionally and that the General Commissioner may/must also be an addressee for the assessments in question. Indeed, the Standing Committees found it essential that the General

[18] Article 12 of the Threat Assessment Act provides for a similar regulation for intelligence originating from the intelligence services.

Commissioner, as the most senior police officer of the Federal Police and member of the Board for Intelligence and Security, should always be an addressee for the CUTA assessments.

Furthermore, the Committees established that there were sometimes inexplicable differences among the addressees of the CUTA assessments. Mention was made earlier of an assessment which had not been disseminated either to any police service or the GISS, without apparent cause.[19] In fact, this was also the case with regard to the involvement of certain services in crucial meetings. The Committees were of the opinion that, if the CUTA really wishes to fulfil the role of a 'crossroads for intelligence', not only must it be an addressee for all relevant intelligence but it must also ensure that it is extremely diligent in providing the necessary *feedback* to the supporting services.

II.1.3.7. Violation of the principle of professional secrecy

The frequent violations of the principle of professional secrecy in the case were criticised by the Director of the CUTA. Sometimes very detailed information has been made public via the media. The Federal Prosecutor evidently shared the same concern. Although this case is certainly not unique in this regard, such a conclusion is still alarming, especially when it involves extremely sensitive information. During their investigations, the Committees did not find any leads to help them trace the leak or leaks.

II.1.3.8. The 'passive role' of the administrative authority in case of embargo procedures declared by the Federal Prosecutor's office

As a consequence of Article 11 of the Threat Assessment Act, the Director of the CUTA and the Federal Prosecutor independently decide what information is to be communicated by the CUTA to the GCCR (amongst others) and therefore, to the Minister of the Interior. It goes without saying that a special responsibility is assigned hereby to the above-mentioned magistrates.[20] Moreover, the then Director of the CUTA considered the Federal Prosecutor's opinion as being decisive in this decision-making process since the latter had initiated the procedure: it was he who had placed elements of a judicial inquiry under embargo.

Although the information position of the Minister of the Interior has improved considerably through the creation of the CUTA, in case of embargo procedures he (as well as the GCCR) remains completely dependent on what is

---

19 This refers to the undated 'SECRET' classified assessment which was based on information supplied by State Security under embargo.

20 The Director of the CUTA is also a magistrate although he does not serve in this position during his mandate as Director.

or is not communicated to him even though he clearly retains the final responsibility for the administrative police and for the maintenance of public order. This does not place the Minister in the most comfortable position when he has to decide on the administrative policing and other security measures to be taken within the framework of the threat as he can never be sure that he has all the relevant information. However, if the Director of the CUTA and the Federal Prosecutor are of the opinion that the intelligence is indispensable for taking the necessary measures for the protection of persons, this intelligence must be included in the assessment.

Furthermore, the Threat Assessment Act states that in case of embargo procedures declared by the Federal Prosecutor, the latter shall also be involved in the decision regarding the operational administrative measures to be taken by the competent authorities. This implies that the Federal Prosecutor's office has a say in the interpretation of the administrative decision-making authority, while it is only the administrative and political authorities who will have to account to the Parliament and to the population for the success of those preventive actions. The public prosecutor's office is not subject to such control and duty of accountability.

The question is whether it is advisable under those circumstances to blindly rely on the assessment of one person (i.e. the Federal Prosecutor) who must bear a heavy burden and responsibility. The system outlined is also at odds with the conventional Belgian state structure where judicial authorities are responsible for criminal proceedings and administrative authorities are responsible for administrative measures and for public order. Whatever may be the answer to these questions, it must be stated that the ultimate end product in this dossier was almost completely influenced by the judicial pillar, even though this end product fell under the responsibility of the executive power.

In casu, a balance is sought between the requirements of the judicial inquiry and those with respect to public order and preventive policing. Naturally, the question is also who ultimately determines this balance. The available documents showed that this happened via a consultation between the Director of the CUTA and the Federal Prosecutor and that the members of the Ministerial Committee for Intelligence and Security were informed from 18 December 2007 onwards. Nevertheless, it must be noted that if the protective measures had not been sufficient, the Minister of the Interior and/or the Minister of Justice would have been the first to be held accountable and not the CUTA and/or the Federal Prosecutor.

II.1.3.9. Responsibility for countermeasures to be taken and liability in case of an incorrect assessment of the threat

The Director of the CUTA stated that he could not help but get the impression that the CUTA is being increasingly seen as having the final responsibility not just with regard to the assessment of the threat – which is logical – but also for the related security measures. And the task of the Coordination Unit is anything but that. In fact, Articles 8, 2° and 8, 3° of the Threat Assessment Act state that the mission of the CUTA consists of carrying out assessments which enable to assess whether threats can occur, how the detected threats evolve and the measures to be taken in such a case. The assessment must therefore also include those elements required for determining an adequate action. The CUTA's scope of competence is limited to suggesting possible measures.

The Director of the CUTA was also concerned about his personal civil liability for losses arising from an attack, if it should subsequently appear that the threat had not been assessed at a sufficiently high level. The reverse situation was also described as problematic: against whom is civil redress possible for the harmful consequences of a threat level that has possibly been overestimated?

II.1.3.10. The 'enthusiasm' of the police services

It appears that the police services displayed suspicion, disbelief or lack of enthusiasm in carrying out the measures associated with an assessment level '4'. At the same time, it appeared that maintaining a high level of threat for too long has a disastrous effect, because the police services evidently began to question its purpose. Although the CUTA can and may make a perfect abstraction of the response capability of and the resources available among the services responsible for maintaining order, both the Committees were convinced that there was a high sense of responsibility within the CUTA in this regard. So there seemed to be no reason for the police and security services to be 'sceptical' in this matter. It was mainly a question of overcoming this scepticism through sufficient and adequate internal communication.

II.1.3.11. A secure communication network

This investigation once again showed that there is an urgent need for a secure communication network.[21] It appeared that the CUTA had only one chauffeur who drove continuously back and forth during the period of the terror threat with the paper versions of the assessments.

---

21 This conclusion had already been reached earlier (see STANDING COMMITTEE I, *Rapport d'activités 2007*, 76).

II.2. 'RESERVED DOSSIERS' AT STATE SECURITY

In February 2006, the Investigation Service I of the Standing Committee I carried out verifications at State Security within the framework of certain investigations. In the context of these verifications, it was accidentally found that some two hundred paper dossiers came under a special regime. These partly individual (in the name of politicians and non-politicians) and partly thematic dossiers were stored in a separate cabinet and could not apparently be freely consulted by staff members of State Security. As a result of these findings, the Standing Committee I decided to initiate an investigation entitled 'Reserved dossiers'.

This term appears to have caught on among the staff at the end of the 1980s, when one referred to certain dossiers which, for one or the other – sometimes unclear – reason, were stored exclusively at the secretariat of the then Administrator-Director-General, Albert Raes. However, the investigation soon brought to light that there are or were various (sometimes overlapping) categories of dossiers that came under a special regime.

The Standing Committee I has divided these dossiers into five categories. Firstly, there are the '*reserved dossiers General Affairs*' of present or former Members of Parliament and Ministers; secondly, there are the reserved dossiers of persons other than Members of Parliament and Ministers; thirdly, there are the dossiers stored at the secretariat of Albert Raes; fourthly, there are a number of thematic dossiers which were not part of the normal circuit; finally, attention is given to dossiers which were classified to prevent them from being consulted by the politicians in question.

Each of these categories has (or had, since some categories do not exist any longer) its own reason for existence and specific issues related thereto. That is why they are described separately later on. The content and application of one of the categories of reserved dossiers, i.e. the dossiers of present or former Members of Parliament and Ministers, are discussed under heading II.2.2. The third section deals with a number of questions regarding legitimacy, while the final section includes some conclusions.

II.2.1. TYPES OF RESERVED DOSSIERS

II.2.1.1. 'Reserved dossiers General Affairs' cuncurring present or former Members of Parliament and Ministers

The Standing Committee I was already aware of the existence of individual dossiers in the name of (former) Members of Parliament and (former) Ministers.

The Committee had reported this earlier in its 1998 and 1999 Activity Reports.[22] At that time, it had come to the following conclusions:

- there was an individual dossier for eight of the fifteen then Members of Parliament of the political parties AGALEV and ECOLO. One of these had been opened when the person in question was elected as Member of Parliament. The dossier involved events and viewpoints of the person outside of his parliamentary mandate. The remaining dossiers dealt with various public activities of these persons within certain organisations (other than AGALEV and ECOLO). None of these dossiers, with one exception, contain any documents from after 1991. Not a single document dealt with the actual parliamentary work of the persons in question;
- there was a thematic dossier in the name of AGALEV/ECOLO. This primarily contained press articles on the activities of both parties. The last report dated from as early as 1988;
- the documents with intelligence obtained since the persons in question had been elected as Members of Parliament, came from open sources;
- generally speaking, it appeared that a number of the then 221 Members of Parliament had a personal dossier at State Security. The bulk of these dossiers had been opened before the concerned functionary was elected. These dossiers reflected the interest in certain movements and tendencies which State Security believed needed to be monitored at that time (i.e. before the Act of 30 November 1998);
- it also appeared that some dossiers of Members of Parliament who developed further activities related to one of the subjects to be monitored, was titled '*TE BEWAREN-A CONSERVER*' (To Be Stored);
- State Security did not initiate any investigation into actions performed within the framework of the actual exercise of the parliamentary mandate.

But the present investigation made clear that there was an additional aspect which had not been addressed as such at that time, i.e. that dossiers of Members of Parliament and Ministers enjoyed an extra degree of protection within the service.

II.2.1.1.1. The paper dossiers

According to State Security, this 'extra protection' was introduced in 1973. However, the practical methods for ensuring this protection were never set down on paper. Still according to State Security, these methods involve transferring a

22 STANDING COMMITTEE I, *Rapport d'activités 1998,* 60-68, 'Report of the investigation into the manner in which the intelligence services differentiate between the activities of Members of Parliament as environmental pacifists and as Members of Parliament' and *Rapport d'activités 1999,* 13-19, 'Report of the investigation with regard to the gathering of information on Members of Parliament by the intelligence services' (free translations).

previously existing dossier (if any) from the time of election as Member of Parliament or taking office as Minister[23] to the then '*General Affairs*' service (which was the competent authority for the archive) and removing the individual index card from the filing system. These dossiers could therefore no longer be freely consulted; they were only accessible for those staff members of State Security who could demonstrate a *need to know*. At the end of the mandate, the dossier was brought back into the normal circuit.

State Security stated that in casu it concerned previously existing dossiers and not dossiers initiated as a result of the assumption of a political mandate. With the exception of a dossier mentioned under II.2.1.1, the Standing Committee I is not aware of any indications to the contrary. The dossiers had been opened as a result of alleged subversive activities or within the framework of a security investigation initiated for the purpose of granting a security clearance.

The reason for this special treatment is evident: to minimise the risk of misuse by State Security staff by protecting the dossiers from any consultation that was not strictly necessary. In addition, all dossiers of Members of Parliament and Ministers were classified as 'SECRET – Act of 11.12.1998'. This provided an additional protection since the Classification Act states that there must be a *need to know* before classified information can be inspected and since violations of the provisions of this Act are punishable by law.

It appears that this system of verifying lists of elected persons and the classification and 'reservation' of paper dossiers by storing them in a special fire-proof case has always been applicable since then. But the Standing Committee I has the definite impression that the system has been applied less strictly over the years.

At the time of the first control in 2006, it appeared that a number of dossiers had disappeared from their storage cabinet and the consultation register to be filled in each time a dossier is consulted, was blank. Furthermore, it appeared that the dossiers did not end up in the normal circuit at the end of a mandate. Finally, the State Security staff who were questioned could not provide any ready and clear answer about the procedure to be followed with regard to the reserved dossiers. The old practice was, however, reactivated as a result of the first investigative steps taken by the Standing Committee I at the beginning of 2006. A staff notice dated October 2006 stated that the dossiers of the elected persons should be placed under the care of a security officer who shall be responsible for their storage and for monitoring consultation. This concerns both 'active' dossiers (in other words, dossiers which are still being maintained and can be used within the framework of the intelligence activities of the service) as well as dossiers which, because of their age, have been closed.[24] But a new round of

23 Later, the dossiers of holders of political mandates in the regional and European spheres were also handled in this manner.

24 These last-mentioned dossiers may be destroyed as soon as the legal obligation to do so is enforced (see further).

control carried out by the Standing Committee I in February 2008 showed that the system is clearly not functioning optimally as yet. It appeared that of the 108 'active' dossiers of politicians falling under this special regime at that time, only 56 of them were then serving a political mandate.

At the close of this investigation, State Security was still working on a staff notice which would introduce a general method for optimising the protection of dossiers of incumbent Members of Parliament and Ministers.

II.2.1.1.2. Digitised information

From the end of the 1990s, State Security started to digitise the obtained information. From 2000, this was made into a general system.

A verification conducted in February 2008 showed that information and/or intelligence was also being stored in the IT system for the 193 politicians for whom a paper dossier existed. At least 46 of them were actually serving a political mandate at that time.

It appears that there are no special protective measures within the service for this – more recent and therefore possibly more sensitive – information. However, State Security can always check which names have been looked up by which staff member. This is because a log is kept of all consultations of data in the IT system. As long as these log files are not deleted, it is possible to identify the persons who have consulted a particular file. There is also a random monthly check of all consultations of data by staff members whose names are drawn by lot.

Although the information on politicians does not at present enjoy any extra protection, this information still seems to receive special treatment. According to the Director-General of State Security, no hyperlinks are created to the names of (former) Members of Parliament and (former) Ministers mentioned in the reports of the service.[25] As a result, staff members who search for a (former) Member of Parliament or (former) Minister in the system either find nothing because there are hardly (if any) hyperlinks (i.e. for more recent information), or see the message 'Operation Parliament' appear on the screen, which means that they need to demonstrate a need to know in order to consult this information (i.e. for information before 2001).[26]

II.2.1.2. Dossiers of other persons 'reserved General Affairs'

Apparently, it was not only the dossiers of Members of Parliament and Ministers that enjoyed a special protection. A control carried out in the beginning of 2006 showed that 95 other paper dossiers were also being stored according to the method described above. This concerned dossiers which were possibly sensitive

---

25 With only one – obvious – exception: if the politician in question represented an immediate and serious threat for our legal system and our democracy, then he would be included in the information file in the normal way.

26 This 'operation' is actually a technical IT intervention (see further under Chapter II.2.1.5).

from a social, economic and political point of view, such as those of the mandate-holders of important administrative or judicial positions. In addition, this involved dossiers of family members of State Security staff. Sometimes this also involved dossiers initiated within the framework of security investigations.

Also pursuant to the investigation of the Standing Committee I, State Security stated that these dossiers would no longer be given the special protection enjoyed by the above-mentioned paper dossiers in the name of the politicians. But a control in February 2008 showed that 95 dossiers had still not returned to the normal circuit. However, a new verification in June 2008 showed that the dossiers had been moved.

II.2.1.3. Dossiers stored at the secretariat of Albert Raes

In the period when Albert Raes was heading State Security, some 'reserved dossiers' of incumbent Members of Parliament and Ministers were stored at his secretariat rather than at '*General Affairs*'.

This special method was also applicable for dossiers of certain politicians who were not serving any mandate or for persons occupying a particular socio-economic-political position. When the Administrator-Director-General left office, it appeared that there were 202 such dossiers.

The Standing Committee I has not carried out any further investigation into the methods and reasons for this practice, since this is definitely a thing of the past.

II.2.1.4. Thematic dossiers

In addition to the dossiers on persons (II.2.1.1 and II.2.1.2), thirteen thematic dossiers were found in February 2006 which were also protected from general consultation. This involved dossiers on subjects (e.g. in connection with certain extremist tendencies or movements) which were 'fed' with elements derived from the individual reserved dossiers. The dossiers contain reports of the internal and field services of State Security as well as information from open sources and reports to external services. Therefore, the documents in these dossiers which contain personal information are also present in the relevant individual dossiers.

II.2.1.5. Classified dossiers of politicians from political parties regarded as extremist

In the mid-1990s, a number of members of a political party regarded as extremist attempted to gain access to their personal dossier at State Security. This was refused by State Security on the grounds of the Open Government Act of 11 April 1994 and the Privacy Act of 8 December 1992. However, on 11 December 2000, the Council of State decided that any refusal by the service must be justified

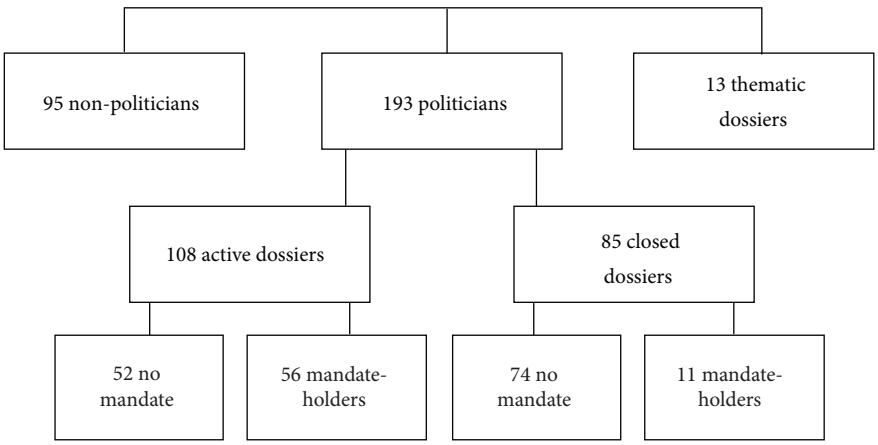
in concreto on the basis of the grounds of exception stipulated in the Open Government Act.[27] To counter this, State Security classified the entire dossier of the Members of Parliament belonging to political parties which were regarded as extremist and which had therefore attracted the attention of State Security. As a result, these dossiers became completely inaccessible without the service being required to give a reason for whether or not a particular document needed to remain secret.[28] The 'special regime' hereby invoked was not intended to provide protection against unlawful consultation by own staff, but to protect data from external parties.

Based on the same objective, the so-called 'Operation Parliament' was initiated in the beginning of 2001. This did not involve an 'operation' in the actual sense of the word, but rather a technical intervention for combining all information on politicians.

II.2.2. SOME FIGURES ON THE PAPER DOSSIERS ON POLITICIANS

In February 2008, the security officer of State Security was in charge of 301 dossiers. Of these, 193 dossiers concerned politicians. These dossiers were checked with regard to certain aspects of their content.

301 dossiers with the Security Officer



27 Council of State, 11 December 2000, no. 91.531, Dewinter.

28 Since, Article 26 of the Act of 11 December 1998 on classification and security clearances, certificates and advice (which came into effect in 2000) states that '*the Open Government Act of 11 April 1994 is not applicable to information, documents or data, material, materials or substances, in whatever form, which are classified according to this Act*' (free translation).

A minor percentage of the dossiers (6 %) had been initiated within the framework of a security investigation. The rest of the dossiers were with regard to a threat that fell under the scope of competence of State Security. 93% of these dossiers were with regard to 'extremism' as defined in Article 8, § 1, second paragraph of the Intelligence Services Act. In general – and therefore without verification or assessment of each separate piece of information – the Standing Committee I reached the conclusion that the information in the dossiers fell within the framework of the legal assignments of State Security.

In addition to documents specific to the internal operation of State Security, the dossiers contained information and/or intelligence originating from:

- the field services of State Security (in 83% of the dossiers);
- open sources such as newspapers, magazines, internet … (in 53% of the dossiers);
- the assessment services of State Security (in 18% of the dossiers);
- Belgian public services such as police services and judicial authorities (in 25% of the dossiers);
- foreign intelligence services (in 7% of the dossiers).

For each separate dossier, the date on which the documents were edited was also examined (does this involve older or more recent documents?). The oldest document found among the dossiers on politicians dated from June 1944. The politician in question does not exercise any political mandate at present. The most recent document dates from September 2007. This, however, did concern a person exercising a political mandate at that time.

With reference to the size of the dossiers, the following could be established:

- 19% contained less than 10 documents;
- 27% contained between 11 and 50 documents;
- 12% contained between 51 and 100 documents;
- 33% contained between 101 and 500 documents;
- 9% contained more than 501 documents.

The Standing Committee I was able to conclude that information and/or intelligence from the dossiers was sent not just to various internal services but also to foreign intelligence services. The internal services were mainly the Federal Public Services, police services, judicial authorities… Information was passed on in 22% of the dossiers. This usually involved a response to a request for information on persons or vehicles. But in 9% of the dossiers, information was also sent to foreign intelligence services. This mainly involved answers to questions regarding the identification of vehicles observed in connection with certain (usually categorised as left or right extremist) activities abroad or with persons who took part in such activities.[29] In each of the cases, however, State

[29] Most of the dossiers, in which data was sent to foreign intelligence services, contain some documents dating from before 1991. Only one dossier includes elements added after 2000.

Security placed a restriction on use of the data by explicitly invoking the 'third party rule'. This means that the foreign service may not disseminate this information to other services without the permission of State Security.

II.2.3. CONCLUSIONS AND POINTS OF ATTENTION

II.2.3.1. Current management of the 'reserved dossiers'

The Standing Committee I has been able to establish that State Security has made significant efforts to clearly define the problem of the so-called 'reserved dossiers' and to reduce this to a problem of managing older files. State Security has also tried to find an adequate solution. The paper dossiers were collected, listed and placed under the management and supervision of the security officer, as a result of which the current risk of misuse is limited and, if this would still occur, attributable.

The Standing Committee I also points out that, with the passage of time, these paper dossiers lose their utility for present intelligence work. Some dossiers containing information still relevant for the present legal assignments of the service may be stored further, provided that they are checked for reliability and relevance. The other dossiers must either be destroyed (see further under II.2.3.5) or transferred to the State Archives.

II.2.3.2. Advantages and disadvantages of the internal protection of certain categories of persons

The Standing Committee I wishes to point out the possible advantages and disadvantages with regard to the internal protection of certain categories of persons who exercise(d) special responsibilities. One advantage is, undoubtedly, the prevention of possible misuse by staff. On the other hand, this method can give rise to speculations both within the service and outside of it. Furthermore, it appeared that these dossiers – perhaps owing to the manner of storage and the opportunities for consultation – were accessed noticeably less frequently than the 'normal' dossiers. The question is whether this was intentional. The Standing Committee I is of the opinion that it is State Security itself that must weigh the pros and cons in this matter. However, it must clearly communicate its decision, both internally and externally. Furthermore, the service must be consistent to the extent that if it elects to protect certain paper dossiers, the same must be done with regard to the information stored in the electronic system.

Taking into account the capacity of a person, it can therefore be justified to allow certain information to continue to be protected internally. This does not change the fact that the current presence of politicians and prominent persons in the now digitised reports of an intelligence service remains an extremely delicate

issue. The Standing Committee I could establish that State Security generally adopted a rather cautious attitude in this regard, which was possibly prompted by the complications in the past. However, the Committee was of the opinion that the capacity of a prominent person or politician must not be an obstacle to an adequate follow-up and a corresponding availability of the relevant reports in the light of the performance of the legal assignments of an intelligence service. This activity must take place 'irrespective of the person'.

This, however, implies that State Security must define clear criteria in this regard.[30]

II.2.3.3. Protection of the constitutionally enshrined right to inspection via classification

The investigation revealed that State Security classifies the dossiers of (former) Members of Parliament and (former) Ministers as 'SECRET – Act of 11.12.1998'. The Standing Committee I would like to point out that this method of working is in se justifiable. This is because Article 3 of the Classification Act allows the classification of information if the '*inappropriate use*' thereof can harm certain interests. An inappropriate use of (personal) data of incumbent politicians could constitute a misuse of that data for the purposes of blackmail with a view to forcing a certain standpoint/voting behaviour/attitude/statement. This could indeed jeopardise '*the operation of the decision-making bodies of the State*'. This last element is one of the interests the legislator intended to safeguard via the classification technique. But, of course, the question remains whether information from e.g. open sources also deserves such protection.

The classification technique offers protection not just with respect to external elements. Internally as well, classification means that the information cannot be freely accessed by all staff members: classified data can only be consulted if one can demonstrate a *need to know* (which means that possessing a security clearance of the required level is not sufficient).

But this issue becomes problematic when the classification diverts from its actual purpose. For example, the Standing Committee I has learnt that the classification technique was used in the mid 1990s to limit the right to inspection. When a number of politicians wanted to inspect their dossier on the basis of the Open Government Act, State Security management took an unusual initiative: it classified all the dossiers. This right to inspection was inscribed in Article 32 of the Constitution and developed by the Open Government Act of 11 April 1994. As mentioned above, the Council of State had already judged that the refusal to allow inspection of government documents must be justified *in concreto*. The classification technique may not be used to circumvent this constitutionally enshrined right or to make it impracticable.

---

30 Also see Chapter VIII.1.2, Activity Report 2008 in this regard.

II.2.3.4. Creation of dossiers on political opinion, affiliations or activities

The Standing Committee I draws attention to the important judgement of the European Court of Human Rights in the case of *case of Segerstedt-Wiberg and Others v. Sweden* of 6 June 2006. In this judgment, the Court questions the acquisition and storage of data related to political opinion, affiliations and activities deemed unjustified for the purposes of Article 8 of the ECHR.

The fact that such information, even though it concerns publicly known facts, is being collected or stored is a serious violation of privacy. This violation can only be justified – according to the European Court of Human Rights – if it is proportionate from the point of view of national security. In assessing this proportionality, the ECHR attached great importance to whether or not a political party was violent by nature. The assessment of such a violent nature may not be inferred solely based on the political programme; it must also translate itself into the actions of the party leaders and the positions they take.

II.2.3.5. Destruction of old dossiers and enforcement of the law

Article 21 of the Intelligence Services Act states that personal data processed by intelligence services may only be stored '*for a period which may not be longer than that necessary for the purposes for which it is stored, with the exception of data of a historic nature as recognised by the State Archives*' and that this data may only be '*destroyed after a definite period after the last processing of this data*' (free translation). The storage period and the procedure for destruction must be determined by Royal Decree, based on advice from the Privacy Commission.

Until now, no such decree has been passed. The Standing Committee I urges that this must be done, not only to enforce a legal obligation but also since the storage of old data by the intelligence services may imply a violation of Article 8 of the ECHR as evident from the earlier-mentioned judgement of the European Court.[31]

The storage of obsolete dossiers is an old problem. As early as in 1998 (and therefore just before the enactment of the Intelligence Services Act), the Standing Committee I focused attention on this issue.[32] At that time, it was stated that the actual destruction of the dossiers would take place within two years. This has still not happened. However, for some time now State Security has taken measures to take the old dossiers 'out of circulation', without actually destroying

---

31 '*However, as to the information released to the second applicant (i.e. his participation in a political meeting in Warsaw in 1967), the Court, bearing in mind the nature and age of the information, does not find that its continued storage is supported by reasons which are relevant and sufficient as regards the protection of national security. Therefore, the Court finds that the continued storage of the information released to the second and fifth applicants entailed a disproportionate interference with their right to respect for private life.*'

32 STANDING COMMITTEE I, *Rapport d'activités 1999*, 14 ff.

them. They are stored separately to be destroyed or to be sent to the State Archives. In concrete terms, this means that this data is no longer accessible to staff members. The service thus complies with the spirit of the law.

There is a different regulation regarding the dossiers on security investigations. Article 25 of the Classification Act states that '*personal data obtained or received within the framework of this Act must be destroyed as soon as the person in question can no longer be subjected to a security investigation*' (free translation).[33] No implementation decree is required for this. The Standing Committee I therefore finds it surprising that old security dossiers of politicians are still to be found among the reserved dossiers.

II.2.3.6. Passing personal data to foreign intelligence services

Passing personal data about Belgian nationals and *a fortiori* about persons who have been elected in a democratic manner, to foreign intelligence services is not at all self-evident. It is *almost* impossible for the Belgian service to control the use of this data, despite the regular invocation of the 'third party rule'.

The Standing Committee I has repeatedly urged the formulation of a legal regulation on this matter.[34] Article 20 of the Intelligence Services Act is absolutely not sufficient in this respect, all the more since it appears that the Ministerial Committee for Intelligence and Security has not yet produced any guideline governing the cooperation with foreign services.

II.3. INTERIM REPORTS IN THE BELLIRAJ CASE

In February 2008, the Moroccan authorities announced the arrest of 32 persons allegedly involved in an organisation which intended to infiltrate the political parties and gain control of the country's institutions. Moreover, the clandestine network of this organisation was reported to have planned assassination attempts on Moroccan Ministers and high officials.

Among the detainees were five persons who had a connection with Belgium. Two of them had the Belgian nationality. Furthermore, one of these Belgians, namely Abdelkader Belliraj, was said to be the leader of the network. He was born in 1957 in Morocco and had moved to Belgium in the beginning of the

---

33 The first sentence of Article 25, first paragraph, which creates an exception with regard to the destruction of personal data obtained within the framework of a security investigation ('*Except when the reasons for collecting this data still exist and its continued storage therefore remains advisable*' – *free translation*), should be regarded as null and void because the same sentence, but then for the security verifications (Art. 25, third paragraph, first sentence), was nullified by the Constitutional Court by judgement no. 151/2006 of 18 October 2006 (BOJ 26 October 2006).

34 See for the last time STANDING COMMITTEE I, *Rapport d'activités 2007*, 75-76.

1970s. In 2000, he became a naturalized Belgian. Belliraj appeared to have maintained contacts with several international terrorist organisations, including Al Qaeda, the Salafist Group for Preaching and Combat (GSPC), the Moroccan Islamic Combatant Group (GICM) and the Lebanese Hezbollah. In 2001, he was also said to have travelled to Afghanistan to meet the Taliban chiefs and heads of Al Qaeda.

In the weeks following the arrest, the revelations in the press followed in rapid succession. It was thus alleged that significant amounts of arms and ammunition, originating from Belgium, had been seized. The network was also said to have been responsible for the robbery in 2000 at the Brinks headquarters in Luxembourg. Belliraj himself was allegedly responsible for six unsolved murders in Belgium between 1986 and 1989.[35] Concerning these murders, the person in question is deemed to have made detailed confessions to the Moroccan court.

When, in the beginning of March, the Belgian press also reported that Belliraj was allegedly a paid informant of State Security, the Minister of Justice and subsequently his colleague from Defence requested the Standing Committee I to initiate an investigation into '*the manner in which the Belgian intelligence services had monitored the persons who were recently arrested in Morocco and who were apparently suspected there of forming a terrorist group*' (free translation). Soon after this, the Monitoring Committee of the Senate requested the Committee to extend its investigation to two more points: according to certain press articles, the Belliraj case was reported to have given rise to tensions between the intelligence services and the police services and secondly, the Standing Committee I needed to investigate whether State Security and the GISS had correctly applied the Classification Act of 11 December 1998 on the information at their disposal *in casu*. In September 2008, additional questions followed from the Monitoring Committee (they wished to know what intelligence had supposedly been given by the Moroccan services to State Security regarding the possible involvement of Belliraj in extremist and/or terrorist activities) and from the Minister of Justice (he wanted details regarding the cooperation between State Security and the CUTA).

The Standing Committee I was of the opinion that the investigation should not have restricted itself to the alleged involvement in a terrorist network. Certainly not considering the reports in the media: Belliraj was reported to have been a State Security informant, which was unfortunate considering his serious criminal past; he appeared to have been naturalized as a Belgian citizen without much ado, smuggled huge amounts of arms from Belgium … These aspects were included by the Committee in its investigation.

---

[35] The ongoing criminal proceedings in Morocco against the person in question, are not yet complete. A judicial inquiry has also been initiated in Belgium. The Standing Committee I is not aware of the content of these dossiers.

As a consequence, the Committee was faced with a very extensive investigation straddling several decades as State Security's interest in Belliraj dated back to the 1980s.

The Standing Committee I has already invested a great deal of effort in this dossier. Numerous documents were requested, inventoried and examined and this was followed up by a considerable number of interviews of members of the intelligence services. Pursuant to Article 48, § 2 of the Review Act, some of these interviews were conducted under oath.

It was not possible for the Standing Committee I to complete this investigation in 2008. However, three detailed interim reports have already been drawn up and sent to the competent authorities. The present chapter gives a summary of the main (and inevitably, temporary) findings of the three reports.

But it is first important to point out two significant elements. Firstly, a lot of information related to this case was classified based on the provisions of the Classification Act of 11 December 1998. The Committee is naturally not authorised to disclose this information. Furthermore, the investigation activities of the Committee were focused primarily on State Security. The intelligence position of the GISS was limited, in the sense that it only knew two of the five detainees who had a connection with Belgium.

The manner in which State Security monitored the detainees – and mainly Belliraj – is discussed below based on nine specific questions.

II.3.1. DID STATE SECURITY KNOW THE DETAINEES?

Belliraj was known to State Security since the beginning of the 1980s as an extremist Islamist and a pro-Iran opponent of the Moroccan King. He had been placed under surveillance several times during that period. This was with the intention of gaining an insight into the contacts he maintained with the radical Islamist world. Even after this period, he was actively monitored by State Security.

In addition, two other detainees were known to State Security because of their close contacts with extremist groups with Shi'ite or salafist leanings. One of the two was also known for banditry.

II.3.2. DID STATE SECURITY HAVE INFORMATION ABOUT POSSIBLE RELATIONSHIPS BETWEEN DETAINEES AND FOREIGN INTELLIGENCE SERVICES?

Until now, the Standing Committee I has not been able to establish whether State Security had information which could help conclude that Belliraj or the other

detainees had cooperated with one or more foreign intelligence services active in Belgium.

II.3.3. WAS STATE SECURITY AWARE OF ANY INVOLVEMENT OF THE DETAINEES IN PUNISHABLE OFFENCES IN BELGIUM AND/OR ABROAD?

In the press, Belliraj was linked to arms trafficking, terrorist activities, six unsolved murders in Belgium, a robbery in Luxembourg, involvement in a clandestine network aiming to overthrow the Moroccan regime …

Nevertheless, all State Security staff questioned by the Standing Committee I stated that they did not have any information, indication or suspicions in that sense. Belliraj had a clean criminal record. He did not seem to have the profile of a leader of a network of the level that had apparently been dismantled in Morocco. According to the same statements, there were never any indications of any involvement in the six unsolved murders. The State Security staff who were questioned also appeared to be surprised by the possible arms trafficking charges.

The Standing Committee I could only be amazed by some parts of these concurrent statements. Especially since the Committee was aware of elements indicating that Belliraj was (possibly) involved in a number of criminal offences. For instance, documents had been found that showed that he had actually been sentenced for theft and for assault and battery charges. But more importantly, in the dossiers originating from State Security itself, Belliraj had been repeatedly linked, from the 1980s and beginning of the 1990s, with trafficking in arms and explosives, with a possible involvement in a group responsible for an attack against a foreign head of state, with a pro-Iran movement of which the leaders were wanted by the police in Morocco, with the creation of false documents and with maintaining contacts with a (non-Islamist) terrorist group … One report even mentioned the fact that Belliraj was looking for arms and explosives to carry out an attack in Belgium as a result of the arrest of GIA (Groupe Islamique Armé) leaders. Though it must be immediately noted that the person in question was never sentenced for terrorism-related offences and no judicial inquiry had been carried out against him, the statements of the State Security staff still remain surprising in the light of their own documentation.

However, the Committee did not find any elements in the State Security documents indicating any involvement in the murders of 1986 and 1989 and in the robbery in Luxembourg.[36] Also, there was no mention in any report of the

[36] But State Security was aware of the fact that one of the other detainees, with whom Belliraj was in contact, was involved in the hold-up at BRINKS in Luxembourg.

fact that Belliraj appeared to have been involved in the (alleged) terrorist cell. Neither could the Standing Committee I establish that State Security had apparently received such information from its Moroccan colleagues.

With regard to this last aspect, certain sources suggested, however, that the Moroccan foreign intelligence service had informed State Security of the imminent arrest a few months before the case broke out. Apparently, they had made it clear that they considered Belliraj to be the leader of a dangerous terrorist organisation and they had also asked concrete questions in this regard. But it appeared that State Security had never responded to these questions. The Standing Committee I could establish that this information was not correct. Questions were probably asked by the Moroccan intelligence service, but these were very general in nature. At no point of time was it possible to establish a link to Belliraj.

II.3.4. WAS BELLIRAJ A STATE SECURITY INFORMANT?

The Standing Committee I was, of course, unable to get past the question as to whether Belliraj was recruited by State Security as an informant and if so, how he had been handled. The Committee investigated the matter and reported on this to the Minister of Justice, the competent authority in this case. The Committee has neither the power nor the authority to offer an affirmative or negative answer to other persons or agencies regarding the question as to whether the concerned person was an informant.

It is important to underline that the Committee takes this position independent of this case as this is the only way to effectively guarantee source protection. In fact, the intelligence services customarily apply the same rule in such matters: the answer provided is neither negative nor affirmative. This is essential for the operation of the intelligence services. When asked whether a particular person is an informant or not, if these services always answer negatively when the person in question is not an informant, and always refuse to answer if he is a source – which is legally required (Art. 18 of the Intelligence Services Act) –, it quickly becomes clear who is cooperating with the service and who is not. Also, a part of the intelligence position is revealed by saying whether someone is supplying information or not. Besides it is equally important for an intelligence service to conceal what people do not know, than what people do know.

Source protection is, therefore, both the Achilles' heel as well as the cornerstone of the operation of an intelligence service. Certainly for the Belgian intelligence services, where HUMINT is and remains the absolute core business. Disclosure of names or methods of working with sources obviously jeopardises the future operation of the service. After all, who will still supply information –

certainly in areas such as terrorism and extremism – if he does not have a full guarantee of anonymity?

Direct or indirect disclosure of sources will not only create a negative effect at a national level, but also in the relationships with foreign services. Because a rigorous respect for confidentiality with regard to human sources is a fundamental acquis within the entire international intelligence community.

The Standing Committee would also like to point out that source protection is not specific to the world of intelligence alone. The protection of the sources of journalists e.g. is also legally enshrined. Just as with intelligence services, it is also essential for their current and future operation that sources can count on their identity remaining undisclosed. Based on the same concern, the Parliamentary Investigations Act also specifies that statements made during private sessions must be kept secret at all times.

II.3.5. DOES STATE SECURITY HAVE PROCEDURES, REGULATIONS AND GUIDELINES WITH REGARD TO WORKING WITH INFORMANTS?[37]

At the request of the Monitoring Committee, the Committee investigated whether State Security has procedures, regulations and guidelines with regard to the use of informant.

For most staff members of the information sections of the field services of State Security, the recruitment, running and assessment of human sources is a daily activity which is closely monitored by the direct manager(s).

There are a number of written guidelines in this respect (e.g. regarding the decision for accepting a person as a 'centrally registered informant' and the elements which are to be investigated, regarding the assessment and compensation …) although these are spread over various documents. In addition, certain aspects of working with informants are only included in the course material for trainees or are only part of practices specific to the service. The Standing Committee I found this surprising, considering the importance of the use of informants for the service. However, the rules have been subjected to a thorough assessment since 2007, with a view to ensuring an adequate training for new inspectors. A HUMINT office has also been set up in the same period.

---

[37] Also see II.5. regarding working with informants. The Standing Committee I has focused its attention on informant operations on various occasions in the past; the first time, through an extensive thematic investigation (Investigation of the informants of State Security and of the GISS (*Rapport d'activités 1997*, 139-168)) and later through more ad hoc investigations in which certain aspects were examined in more detail: *Rapport d'activités 1999*, 95-96; *Rapport complémentaire d'activités 1999*, 72-75; *Rapport d'activités 2004*, 24-35; *Rapport d'activités 2000*, 163-170 and 192; *Rapport d'activités 2003*, 9-10; *Rapport d'activités 2003*, 207-208 and 230-232 and *Rapport d'activités 2004*, 111.

Its task is to implement State Security policy on this matter in practice, contribute to the organisation of staff training and cooperate with regard to the assessment and protection of sources.

II.3.6. DID STATE SECURITY UNLAWFULLY INTERVENE IN THE NATURALIZATION PROCESS OF BELLIRAJ?

Another question was whether State Security had, in any way whatsoever, facilitated the naturalization of Belliraj as a Belgian citizen.

It is important to note that Belliraj had submitted an initial application at the end of the 1980s. After a long procedure, his application was rejected in 1998 by the House of Representatives. The most notable aspect was the distinctly negative advice of State Security. The service had knowledge of various elements linking Belliraj to criminal and extremist activities (see II.3).

When the so-called 'Fast Track Naturalization Act' came into effect in 2000, Belliraj submitted a new application. This time, however, he was granted the Belgian nationality. But the Standing Committee I came to the notable conclusion that State Security had formulated two different advisory opinions in this dossier: the first one drawn up by the Deputy Head of the concerned department on 6 June 2000 and the second on 13 June 2000, this time signed by the Head of the concerned department. The first advisory opinion was as follows: '*I have the honour to inform you that Belliraj is known to our services owing to his activities within the Algerian and Moroccan Islamist radical movements*' (free translation). In the second advisory opinion, this became: '*I have the honour to inform you that Belliraj was known to our services during the 1980s owing to his activities within the pro-Iran Moroccan milieu. Since then however, he has not come to our attention either in this context or due to any other political activity*' (free translation). Only this second advisory opinion was found in the naturalization dossier at the competent prosecutor's office. Since there were no indications to the contrary, the Belgian nationality was granted.

The Standing Committee I has conducted an intensive investigation into how and why these two advisory opinions were formulated. According to the members of State Security questioned under oath, no actions were carried out at any time with a view to facilitating the acquisition of the Belgian nationality.

In the current status of the investigation, the Standing Committee I can only conclude and regret that State Security was not in a position to give a satisfactory explanation about these two advisory opinions. This naturally provides fertile ground for speculation and guesswork.

II.3.7. HOW DID THE COOPERATION WITH THE CUTA PROCEED?

The Minister of Justice asked for clarifications regarding the earlier report of the Standing Committee I which revealed that State Security had apparently not shared all the intelligence it had with regard to Belliraj, with the CUTA. Yet Article 6 of the Threat Assessment Act obliges State Security to pass on all intelligence which is relevant within the framework of the execution of the assignments of the CUTA (in particular, the drawing up of ad hoc or strategic threat assessments with regard to terrorism or extremism).

It is true that State Security has not communicated any information to the CUTA, even though they knew Belliraj and two of the other detainees. The Standing Committee I is therefore of the opinion that State Security has not fulfilled its legal obligation. As a result, the CUTA was not in a position to assess a possible threat against persons (Art. 2, 1°, RD CUTA). Since the reports in the press that certain persons were allegedly informants of State Security also mentioned their place of residence, this meant that their safety and that of their next of kin could be in danger. This possible danger is not necessarily related to the fact of whether or not these persons are also actually informants.

But the Director-General of State Security contested that the information available to his service could be regarded as 'relevant' under the meaning of Article 6 of the Threat Assessment Act. Moreover, he pointed to a possible conflict between two legal provisions, one of which implies an obligation and the other a ban on the communication of certain information. In view of these elements, specific to this case, the Committee was of the opinion that though Article 6 of the Threat Assessment Act had indeed not been respected, no criminal or disciplinary violations could be established on the part of any member of State Security.

II.3.8. HAS THE BELLIRAJ CASE GIVEN RISE TO TENSIONS BETWEEN THE INTELLIGENCE SERVICES AND THE POLICE SERVICES?

At the request of the Monitoring Committee, the Standing Committee I tried to investigate whether the Belliraj case had given rise to tensions between the intelligence services and the police services. Some press sources even referred to a 'war between anti-terror services' and it sometimes seemed that this war was being fought out in the media with allegations flying back and forth from mostly 'anonymous sources'.

Though it is not easy to formulate a clear and unambiguous answer to this question (tensions may arise between persons in the field and/or sections of both

services and/or at management level; the Belliraj case may be the only cause for possible tensions or the last drop that makes the cup run over; there may be tensions with regard to a certain area and an excellent cooperation in another area; the remarks in the press may be intended to arouse tensions …), the Standing Committee I has closely examined the news reports in this regard and questioned the State Security management on this matter.

Though the Director-General of State Security refuted these reports and referred to good relations in the field, the fact remained that one could read of many 'revelations', 'insinuations' and 'accusations' in the press. In a reaction to this, the Director-General lodged two complaints. A civil complaint lodged against unknown parties for violation of the principle of professional secrecy and of the classification principle; a second complaint lodged with the Standing Committee P which targeted a particular section of a police service.

In view of these complaints, the Committee judged it suitable to wait for the results of these investigations before resuming its investigation in this area. But the Committee did formulate a number of remarks. Firstly, it focused attention on the fact that there was a certain tension noticeable between both services since the Federal Police started devoting a lot of time and effort in developing a proactive approach to the fight against terrorism. This tension has become even more perceptible as a result of the events surrounding the declaration of the terror alarm in the end-of-year period of 2007.[38] Also, the fact that the intelligence services could avail of special intelligence methods (SIM) in the future, while the police services would not be able to apply any special administrative methods (SAM), could have paved the way for this friction. The Standing Committee I noted that there is question of rivalry in the fight against terrorism and radicalism. It appears that a solution can only be found if there is a clear division of tasks and if the exchange of information proceeds smoothly. That is why it is vital that both services enter into a cooperation agreement. The competition must make way for cooperation. The College for Intelligence and Security could play a crucial role in this.

II.3.9. WAS THE CLASSIFICATION OF THE INFORMATION JUSTIFIED?

The Monitoring Committee of the Senate has requested the Standing Committee I to extend its investigation to the question of whether the classification introduced in the documents of the intelligence services was justified pursuant to the Act of 11 December 1998 on classification and security clearances, certificates and advice.

38 See Chapter II.1, *Activity Report 2008*.

One must immediately point out the fact that the safety of informants of intelligence services is not part of the interests protected by Article 3 of the above-mentioned Act. The fulfilment of the assignments of the intelligence services is also not part of those interests.

Nevertheless, Article 18 of the Intelligence Services Act of 30 November 1998 states the following: '*In fulfilling its assignments, the intelligence and security services may enlist the help of human sources. In that case, these services must safeguard the safety of the information related to the human sources and the intelligence that they share*' (free translation). The Act therefore requires the intelligence services to safeguard '*the safety of the information related to the human sources*' and not the safety of the persons as such.

But in its *Activity Report 2004*, the Standing Committee I had stated that the obligation referred to in Article 18 can only be respected by classifying the identity of informants.[39]

In practice, the intelligence services safeguard the safety of both the intelligence and the informants themselves by assigning a high level of classification to the information they receive from their human sources.

In casu, the Standing Committee I was of the opinion that the classification of the investigated documents was necessary and justified, in view of the legislation applicable to the intelligence services. No case of misuse was found in this context.

II.4. THE ROLE OF THE INTELLIGENCE SERVICES WITHIN THE FRAMEWORK OF THE FIGHT AGAINST THE PROLIFERATION OF NON-CONVENTIONAL AND VERY ADVANCED WEAPONS

The proliferation of chemical, biological, radiological and nuclear (CBRN) weapons is one of the most significant threats for the coming decades. That is already apparent from a report for the United Nations identifying the threats and challenges which the international community will be confronted with.[40] This also emphasises how difficult it is to develop a coherent, strategic response to this threat. The fight against proliferation – or '*the intention to contain the nuclear, chemical and bacteriological arsenal of the various nations by preventing its expansion or global spread, or the dismantling of existing weaponry*'[41] (free

39 STANDING COMMITTEE I, *Rapport d'activités 2004*, 115.

40 Www.un.org/secureworld ('A more secure world: Our shared responsibility').

41 'Non-proliferation' as defined by a State Security analyst (O. DETEZ, 'Le travail du renseignement et la non-prolifération', in M. COOLS, et al (eds.), *De Staatsveiligheid. Essays over 175 jaar Veiligheid van de Staat,* Brussels, Politeia, 2005, 303).

translation) – must be regarded as a key element of the national and European security policy. State Security and the military intelligence service also have an important role to play in this context. With this investigation, the Standing Committee I has tried to examine the present or future contribution of the Belgian intelligence services to this fight. The following investigation is primarily based on the analysis of documents and statements of members of the intelligence services.[42]

II.4.1. STATE SECURITY AND THE FIGHT AGAINST PROLIFERATION

II.4.1.1. Legal powers

The tasks of State Security are extremely varied and that is particularly true within the framework of the fight against proliferation.

First and foremost, there is the intelligence assignment regarding specific threats against the continued existence of democratic and constitutional order (Art. 7, 1° of the Intelligence Services Act). The task entrusted to State Security consists in tracing and analysing information regarding each threat, including possible or actual proliferation (Art. 8 of the Intelligence Services Act). Article 8, 1°, d) of the Intelligence Services Act defines proliferation as follows: '*trafficking in or transactions with respect to materials, products, goods or know-how which can contribute to the production or the development of non-conventional and very advanced weapon systems. In this context, this refers to the development of nuclear, chemical and biological weapons programmes, the transmission systems associated therewith, as well as the persons, structures and countries involved thereby*' (free translation).

A second legal task, which contributes indirectly to the fight against proliferation, is described in Article 7, 2° of the Intelligence Services Act: State Security carries out the security investigations entrusted to it pursuant to the guidelines of the Ministerial Committee.

Finally, State Security must '*carry out all other assignments entrusted to it pursuant to the law*' (Art. 7, 4° of the Intelligence Services Act – free translation). Within that framework, one may refer to the supporting role assigned to State Security in the Advisory Committee for the Non-proliferation of Nuclear Weapons (CANVEK/CANPAN) or even to its advisory function with respect to the Minister of Justice within the framework of the licence allocation procedure

[42] In this investigation, the Standing Committee I also enlisted the help of an external expert; Professor Quetin Michel, associated with the University of Liège. His article '*Réflexions sur le rôle des services de renseignements dans le domaine de la lutte contre la prolifération des armes de destruction massive*' can be consulted on the website of the Standing Committee I (www.comiteri.be).

for the import, export and transit of and the fight against illegal trafficking in arms, ammunition and material, including the technology associated therewith, intended especially for military use or for the maintenance of law and order (R.D. of 16 May 2003).

II.4.1.2. Interpretation of the role of State Security in the area of the fight against proliferation

The collection and processing of information on the various CBRN programmes worldwide should allow the intelligence services to form as realistic a picture as possible of the scope of these programmes and the potential threat posed by them. Taking into consideration the limited resources at the disposal of State Security (see II.4.1.3), the service recognises that it is not capable of monitoring this issue in its entirety.

To summarise, State Security defines its tasks as follows:

- collection and processing of relevant information on each aspect of the proliferation. An overall idea of the proliferation plans worldwide should make it possible to find out about the equipment and *know-how* which countries identified by State Security as 'proliferation countries', are trying to obtain;
- monitoring of 'proliferation activities' in Belgium by developing methods for tracing the clandestine export of 'proliferation material' from ports and airports and by paying special attention to certain foreign students and researchers depending on their interest in a subject matter related to proliferation;
- exercising control – along with the competent authorities in the various phases of the process – on the export of sensitive goods and goods which could be used for civil as well as military purposes (*dual use*). This involves making sure that Belgian companies are not participating in proliferation via transfer of technologies or materials which could contribute to the development of programmes for weapons of mass destruction. Of course, State Security will neither 'materially' control nor intercept the export by itself;
- inform and raise awareness among the competent authorities as well as in the business and industrial world and among specialised laboratories. The information made available can be both basic information concerning developments in the area of proliferation as well as specific information which can contribute to the prevention of undesirable transactions.

II.4.1.3. Organisation of the available resources

In December 2003, State Security was of the opinion that it did not have sufficient human resources to monitor the proliferation issue. The then Director-General

stated that only a considerable increase in staff would make it possible to extend the initiatives or to take up new initiatives in the area of the prevention and control of CBRN weapons.

The issue of available resources (and particularly, their scarcity) was also discussed in the open sources: '*Unfortunately, we must conclude that the material and human resources of State Security, in comparison with a large majority of western intelligence services, have not been strengthened in order to cope with the increase in and urgency of the work needed to be carried out in the fight against proliferation.*' And furthermore: '*Although following the attacks of 11 September 2001, new resources were allocated to the fight against terrorism, the non-proliferation dimension was not taken into consideration and was consequently not strengthened*'[43] (free translations).

The present situation gives a more balanced picture. Thanks to recruitments, it was possible to gradually supplement the staff of the assessment services. At the same time, with the reorganisation of the assessment services, a 'Security' pillar was created with a view to the protection of the economic security and the political, national and international integrity of the Belgian constitutional state. Besides dealing with organised crime, sects and SEP, this pillar is also involved in the fight against proliferation. But the 'Intelligence' pillar also devotes attention to terrorist groups and the use of non-conventional weapons. Terrorist threats, regardless of their nature (CBRN or otherwise) are treated within this pillar depending on their geopolitical origin.

A coordinator was appointed to guarantee the interaction between the two pillars.

As regards the field services, a department of the central section in Brussels is specifically entrusted with gathering intelligence in the area of proliferation. The provincial posts have the task of gathering intelligence with regard to the proliferation within their regions.

State Security does not have any agents abroad; they can only rely on the exchange of information with foreign services or, secondarily, on human sources who can provide useful information on the proliferation issue.

II.4.1.4. Partners of State Security in the fight against proliferation

The intelligence network of State Security in the field of non-proliferation assumes that there is an ongoing interaction with various regional, federal and international players. But apart from one agreement with the GISS, at present there is no cooperation agreement on this matter with regional and federal authorities. Nevertheless, State Security does maintain informal contacts with various services which are (or may be) involved in the proliferation problem. The most important partners are mentioned below.

---

43 O. DETEZ, *o.c.*, 312.

II.4.1.4.1. Partners at the level of the regional authorities

In 2003, the authority and the accompanying responsibility for the granting of licences for the import, export and transit of arms, ammunition and materials (and technology associated therewith) specifically intended for military use or for the maintenance of law and order, as well as of products and technologies for dual use, were transferred to the three regions.[44] State Security (indirectly) provides the regions with information which can play a role in deciding whether or not to grant these licences.

It was not without some concern that State Security focused its attention on the risks inherent to this regionalisation. On the one hand, this transfer of authority runs counter to the Europeanization principle and even the globalisation with regard to this subject matter, but also to the Belgian foreign policy on non-proliferation. On the other hand, there was the fear that since three regional authorities are now authorised for one and the same subject matter, widely varying criteria would be applied in the assessment leading to the granting or refusal of licences.

II.4.1.4.2. Partners at the federal level

In order to handle the proliferation issue in a thorough manner, State Security is correct in thinking that it must maintain contacts with various federal authorities.

The cooperation agreements with the FPS Economy (Directorate-General for Inspection and Arbitration[45]) and the FPS Finance (Administration of Customs and Excise) announced by State Security, were still being developed at the end of 2008. The purpose of these agreements is to improve the exchange of information with these services. In addition, State Security stated that they maintain contacts with the FPS Public Health.

However, State Security does have a cooperation agreement with the General Intelligence and Security Service. Cooperation platforms were created as an offshoot of this agreement. One of these is dedicated to proliferation, which implies that both services regularly exchange information, particularly with regard to CBRN proliferation (II.4.2.6.2).

For assessing the terror threat, regardless of its nature, State Security refers to the CUTA with whom it cooperates and to whom it supplies all the relevant intelligence at its disposal.

---

44 Special Act of 12 August 2003 amending the Special Act of 8 August 1980 for reform of institutions (*BOJ* 20 August 2003).

45 The engineers and scientific experts of the economic inspection may be called in with regard to sensitive materials and equipment.

Furthermore, State Security has a liaison officer at the Governmental Coordination and Crisis Centre (GCCR). The GCCR has earlier drawn up a plan for emergency situations with regard to CBRN which require to be coordinated or managed at a national level. The GCCR includes various cells and working groups in which State Security is represented.

Despite the absence of any cooperation agreement, State Security works together with the Administration of Customs and Excise, whose role is to prevent the illegal export of goods for dual use. For that purpose, the Administration for Customs and Excise maintains a database in which all refusals of export licences are recorded. State Security can consult this database for all cases of export of goods which can contribute to the proliferation of weapons of mass destruction.

Along with a representative of the Administration of Customs and Excise, the Director-General of State Security also participates in the activities of the National Authority for Maritime Security.[46] In addition, State Security has a permanent representative in the local Committees for Maritime Security, which are set up in all Belgian ports subject to the *International Ship and Port Facility Security Code* (*ISPS*). With this, Belgium supports American security initiatives for countering the proliferation of weapons of mass destruction via maritime transport.

Furthermore, there is the cooperation at the federal level within the Advisory Committee for the Non-Proliferation of Nuclear Weapons (CANVEK/CANPAN). To prevent nuclear materials, nuclear technology or goods for dual use from being used for the development or manufacture of nuclear weapons, an export licence for such goods may only be granted subject to a prior approval from the competent minister(s). They take their decision based on the advice of the CANVEK/CANPAN. State Security is represented within this Committee. State Security, in its turn, enlists the help of the Committee to request intelligence on companies which are not compliant with the legal export obligations. The service has, however, pointed out certain difficulties occurring within the CANVEK/CANPAN. As a result of the heterogeneous composition of this Committee, there are divergent opinions regarding the approach to the dossiers and it is more difficult to reach a consensus. Furthermore, the intelligence services were not allowed to divulge any classified information at the meetings. This situation was recently remedied: from now on all members of CANVEK/CANPAN must have the required security clearance.[47]

Finally, one can also refer to the Federal Agency for Nuclear Control (FANC). As an independent body, the FANC monitors compliance with the laws and regulations for protecting the population, employees and the environment

46 R.D. of 21 April 2007 on maritime security (*BOJ* 27 April 2007).

47 R.D. of 9 December 2008 amending the Royal Decree of 12 May 1989 governing the transfer of nuclear materials, nuclear equipment, technological nuclear information and derivatives thereof to non-nuclear states (*BOJ* 18 December 2008).

against the risk of ionising radiation and formulates proposals for improvements in this regard.[48] This agency investigates all information with regard to potential illegal use of nuclear technical materials. Such investigations assume that close contacts are being maintained with the police, the prosecutor's office, the judicial services and the points of contact (POC) in the various countries.[49] State Security and the FANC do not maintain any relationships other than those essential for carrying out the security verifications prior to issuing security certificates.

II.4.1.4.3. Partners at the international level

At an international level, State Security maintains bilateral and multilateral relationships.

For this purpose, State Security has a liaison officer at the FPS Foreign Affairs. The document defining his assignment provides for the exchange of information in matters falling under the legal scope of competence of State Security. Strangely enough however, there is no mention of the proliferation of weapons of mass destruction. However, cooperation with regard to the protection of the country's scientific and economic potential *'via the exchange of information regarding the contacts between companies, Belgian researchers and 'sensitive countries' in the areas of technology, science, IT, medicine, chemistry, physics …'* and the dissemination of information about arms trafficking in general, have been provided for.

In Belgium, the meetings of the non-proliferation group of the Council of Ministers of the European Union[50] are prepared by the FPS Foreign Affairs. The meetings organised within the framework of the Non-Proliferation Treaty or the international export control regimes are prepared via a specific mechanism of inter-departmental consultations to which all concerned administrations are invited.[51] Together with delegates from the FPS Foreign Affairs, State Security also sends representatives to some meetings held within the framework of the international commitments of Belgium. State Security participates in meetings of the *Missile Technology Control Regime* (MTCR), the Australia Group, the *Nuclear Suppliers Group* (NSG), the *Proliferation Security Initiative* (PSI), the Wassenaar Arrangement or the International Atomic Energy Agency (IAEA).

It is worth mentioning that State Security has a liaison officer at the EU *Joint Situation Centre* (SitCen). The task of SitCen is to monitor and assess international events round-the-clock with specific attention for sensitive areas, terrorism and

48 See: www.fanc.fgov.be.

49 FEDERAL AGENCY FOR NUCLEAR CONTROL, *Jaarverslag aan de wetgevende kamers*, 2003 and 2004.

50 *Contingency Operations (CONOP)* group, a working group within the framework of the Council of Ministers of the European Union for the non-proliferation of nuclear weapons.

51 *Q&A*, House of Representatives, 2006-2007, 19 March 2007, no. 160, 31114, Q. no. 460.

the proliferation of weapons of mass destruction. For this purpose, SitCen receives information from the national intelligence services.

Of course, State Security also exchanges information with foreign intelligence services about CBRN proliferation and the associated terrorist risks.

II.4.2. THE MILITARY INTELLIGENCE SERVICE AND THE FIGHT AGAINST PROLIFERATION

In its *Activity Report 1997* – and therefore before the enactment of the Intelligence Services Act – the Standing Committee I stated that the fight against the proliferation of CBRN weapons should also fall under the scope of competence of the GISS.[52] The Committee urged this service to optimise its intelligence work in this area by means of cooperation agreements and advised the Minister of Defence to increase the number of GISS staff for this purpose.

II.4.2.1. Legal powers

While the powers of State Security within the framework of the fight against proliferation were described clearly and in detail, the legislator was not so clear regarding the assignments of the military intelligence service.

The fight against proliferation is not explicitly mentioned as an assignment of this service. However, this does not mean that the General Intelligence and Security Service cannot perform any assignments in connection with this matter. Therefore, Article 11, § 1 of the Intelligence Services Act entrusts the GISS with the task of '*collecting, analysing and processing intelligence related to any activity which threatens or could threaten the inviolability of national territories, the military defence plans, the fulfilment of the assignments of the armed forces, or the safety of Belgian nationals abroad or any other fundamental interest of the country, as defined by the King on the motion of the Ministerial Committee and of immediately informing the competent ministers thereof as well as providing advice to the government, at its request, in defining its foreign defence policy*' (free translation).

The legislator has defined the concerned activities in greater detail in the second paragraph (Art. 11, § 2 of the Intelligence Services Act): *'any expression of the intent to use military means to capture, occupy or attack the entire territory or a part of it as well as the airspace above that territory or the territorial waters, or to jeopardise the protection or the continued existence of the population, the national heritage or the economic potential of the country (…)*' (free translation). It goes without saying that 'military means' also implies CBRN weapons. In contrast with State Security, the emphasis is not so much on trafficking or

52 STANDING COMMITTEE I, *Rapport d'activités 1997*, 185-186.

transactions of materials, products, goods or know-how which can contribute to the production or the development of non-conventional or very advanced weapon systems, but rather on the possible 'use' of these weapons.

II.4.2.2. Interpretation of the role of the GISS in the area of the fight against proliferation

Since 2001, the fight against CBRN proliferation (and CBRN terrorism) in accordance with the provisions of the Intelligence Steering Plan and the Security Intelligence Steering Plan have been priorities of the GISS. The main objective of the GISS consists in drawing up a threat assessment and the risks originating from countries described by the GISS as '*pays 'préoccupants' ou candidats à la prolifération*' ('disquieting' or proliferation-prone countries) and from CBRN terrorism.

For this purpose, the GISS acquires its information via open sources as well as via HUMINT, exchange of information, both nationally (e.g. with State Security) as well as internationally (with friendly services) or even via images from observation satellites (various treaties on disarmament, arms control and the ban on nuclear tests provide for the use of national or multinational 'technical resources' as control methods[53]).

Just as in other matters, 'products' emerging from the exploitation of proliferation-related intelligence are provided to various authorities, usually in one of the forms mentioned below:

- analyses of global studies;
- answers to requests for information from national governments, foreign or domestic partner services, the high command of the Belgian armed forces deployed abroad …;
- *briefings* to authorities and to the high command of the armed forces;
- communiqués and specific reports, daily and/or weekly in case of perceived threats or high risks or if a notable event has occurred …;
- assessment of risks and threats in case of an alarming incident with regard to the territories where the Belgian armed forces are deployed and foreign territories where Belgian nationals are present.

II.4.2.3. Organisation of the available resources

Just as the Director-General of State Security, the Head of the GISS also declares that his service does not have sufficient manpower to deal with all aspects of the

[53] It was mainly satellites, such as the military observation satellite Helios II, that ensured more transparency in the monitoring of disarmament agreements. Depending on their type, observation satellites make it possible to provide both basic information (on factories, nuclear infrastructure, rocket launch bases) as well as situation-specific information (such as the localisation of nuclear, biological and chemical activities).

problem. It is obvious that the Standing Committee I cannot go into details in this regard. However, it can give an idea about the organisation of the available resources.

The issue of the proliferation of weapons of mass destruction is primarily monitored by the *Intelligence* department.[54] This department gathers and analyses intelligence on external threats against national territories, the safety of the armed forces abroad and the safety of Belgian nationals and Belgian interests abroad. *In casu*, the service monitors and analyses the capabilities, armament programmes, installations, transfers of technologies as well as the purchasing sources of certain countries, regions or groups which constitute a potential threat. As a result, the *Intelligence* department devotes constant attention to the political and military events taking place in those areas and to the economic, doctrinal, social and cultural factors which can influence the proliferation of weapons of mass destruction.

Some aspects related to this issue can be of interest to the *Counterintelligence* department. This department is more specifically involved with potential threats posed to the Belgian armed forces by terrorism, subversion and espionage. According to the GISS, the department has the task of identifying and countering the threats originating from foreign intelligence services, organisations or individuals involved in activities of espionage, sabotage, subversion or terrorism against military installations in Belgium. As a result, this department holds the view that it is not authorised to deal with proliferation as such, except to the extent that there is a connection between the proliferation and its areas of competence as mentioned above.

II.4.2.4. Preventive measures proposed by the GISS

The GISS is of the opinion that the NATO countries have long prepared themselves to cope with nuclear, biological or chemical attacks within the framework of a confrontation between conventional armed forces. But they are much less prepared to tackle similar threats made by terrorist groups.

Therefore the GISS has recommended the development of specific measures and improvement of existing initiatives which can help prevent such attacks. This involves:

- strengthening multilateral instruments and treaties on disarmament and non-proliferation in order to prevent terrorist groups from gaining access to weapons of mass destruction and their technologies;
- making an inventory of radiological sources and radioactive substances used for civil purposes in Belgium and abroad;

---

[54] The *Intelligence* department includes an assessment department which devotes its attention to cross-border phenomena and is itself divided into three departments: (a) proliferation of weapons of mass destruction and their carriers; (b) trafficking in arms and natural resources; and (c) international Islamist terrorism.

- improved coordination of the activities carried out by the various services concerned for obtaining intelligence; these activities must include the monitoring of the sources of funding for terrorist groups and for certain trafficking transactions, of organisations for organised crime and of the prohibited trade in sensitive products;
- improving the cooperation between the services of friendly countries and their partners;
- strengthening the regulation and controls with regard to the production, acquisition and processing of certain hazardous substances in the industry and the laboratories;
- introducing and reinforcing vigilance exercised with regard to the issuance of security clearances for industries and laboratories which produce and use CBRN materials for civil purposes even though, according to the GISS, this measure appears to be difficult to apply in practice;
- optimising the manner in which radioactive materials of military origin are moved or transported;
- developing systems for quick detection, identification and protection in case of disasters;
- drawing up emergency plans, including the creation of intervention units;
- informing and raising awareness among the population.

According to the GISS, a broad overview of the cross-border phenomena is absolutely necessary in order to better evaluate and assess the threat. To take more efficient and effective action, a medium and long term approach is essential.

II.4.2.5. Partners of the GISS in the fight against proliferation

II.4.2.5.1. Partners at the level of the regional authorities

In the area of proliferation, the GISS has not entered into any cooperation agreements with regional authorities. The only contacts maintained by the GISS with these regional authorities are those initiated by its representative during the meetings of the CANVEK/CANPAN and during the coordination meetings organised by the FPS Foreign Affairs with a view to participation in the plenary sessions of the export control regimes.

II.4.2.5.2. Partners at the federal level

The protocol agreement between the two intelligence services (II.4.1.4.2) provides for the creation of several permanent cooperation platforms. One of these is devoted to proliferation. These platforms are the preferred forums for the exchange of information between the two services. In principle, State Security

and the GISS meet twice a year regarding the proliferation issue. Various topics are discussed during these meetings: the use of unmanned aircraft for the dispersion of chemical or radioactive agents, the possible discovery of radioactive substances in Congo, the status of programmes and capabilities with regard to CBRN weapons in high-risk countries, the involvement of certain companies or entities in sensitive export activities … Each service investigates these subjects within the framework of its own areas of competence. According to statements gathered by the Standing Committee I from the two services, there is a question of complementarity and information is actually exchanged.

The CUTA is also an important partner of the GISS with regard to the assessment of the general terrorist threat, including the threat of the proliferation of weapons of mass destruction. The GISS provides all its assessments to the CUTA, which the latter then compares with its own assessments. In case of divergent analyses, the respective standpoints are compared, discussed and, if necessary, modified. Both the GISS and the CUTA are of the opinion that the cooperation between both services is well-developed.

Representatives of the GISS are also members of the CANVEK/CANPAN. They issue their advice based on intelligence regarding the activities of the destination countries, the end users, guidelines of the export control regimes, characteristics and possible applications of the concerned products or materials as well as the risks of conversion to a military programme.

Furthermore, the GISS participates in various initiatives of the Ministry of Defence and/or of other (governmental) services with a view to setting up committees for the assessment of the existing resources and requirements for the defence against CBRN weapons. This involves *in casu* working groups or committees for the assessment or coordination of measures which must be taken as a result of certain events (e.g. attacks of 11 September 2001, letters with anthrax powder …). In this context, the GISS plays a supporting role and it mainly assesses the risks and threats. This service has, for instance, contributed to the development of a concept of resistance to CBRN weapons.

The GISS does not maintain any direct contacts with the FANC. Nevertheless, the GISS is in favour of coordination between the FANC, the National Security Authority (ANS/NVO) and the Board for Intelligence and Security within the context of this issue.

II.4.2.5.3. Partners at the international level

There is a cooperation, in the form of (bilateral) exchange of information with services of EU countries, the NATO as well as within the framework of international export control regimes.

The GISS does not have any representative at the EU *Joint Situation Centre* (SitCen). However, this does not prevent the GISS from answering questions

asked by the SitCen. The GISS also receives the quarterly SitCen reports. These mainly contain analyses summarising the information received by the SitCen from the various national services.

Subjects such as the assessments regarding the proliferation of weapons of mass destruction and their carriers, recent technologies as well as CBRN terrorism are also brought up at the NATO conferences within the working groups (*Intelligence Working Groups*).

These matters are also discussed within the framework of the multilateral meetings of the countries (including countries which are not members of NATO or the European Union) which have entered into various export control regimes (Group Australia, *Nuclear Suppliers Group*, MTCR).

Finally, the GISS was also present in 2003 at the coordination meeting of the representatives of various federal ministries involved with the possible participation of Belgium in the *Proliferation Security Initiative* (PSI). Despite the fact that no concrete request for information has been received since then regarding cases of transfer or interception of sensitive material in connection with the proliferation of weapons of mass destruction, the GISS is kept informed of the progress of interception exercises organised within the framework of the PSI. The GISS itself does not take part in these.

II.4.3. CONCLUSIONS

The fight against the proliferation of non-conventional or very advanced weapons is an important point of attention for our country. Belgium has supported a large number of initiatives and incorporated the international agreements in this regard within its legislative and regulatory framework.

It is obvious that a clear and coherent action cannot be taken without the supporting role of the intelligence services. A general idea of the issue is essential in order to better define and assess the threat, while a medium and long term approach is necessary in order to take action more effectively and efficiently. In the fight against proliferation, an entire series of assignments was therefore assigned to the intelligence services, even though the legislator did not explicitly define the assignments of the GISS.

The degree of risk in connection with the various actual and potential CBRN threats varies considerably. It is also evident that links must be established between the fight against proliferation and the fight against terrorism.

The exchange of information and the formulation of assessments must contribute to the implementation of a coherent and correctly outlined strategy so as to respect the multilateral treaties and agreements on disarmament and non-proliferation. However, the intelligence services cannot take the place of the institutions created by (international) regulations and whose (sole) purpose is to monitor non-proliferation.

Intelligence services mainly pay attention to unreported, clandestine or peripheral activities of armament programmes for weapons of mass destruction.

But the information position of the intelligence services in this matter is not only important for countering proliferation. Intelligence services must also control, validate, put in perspective or negate the flow of vague, incorrect, exaggerated or biased information because this information is sometimes intended to influence political, strategic and military decisions in a subjective manner and to guide these decisions in a certain direction. This is a form of 'interference' and therefore one of the threats which State Security must explicitly monitor (Art. 8, 1°, g) of the Intelligence Services Act). Such interference can in fact jeopardise a country's decision-making autonomy. This can only be prevented if the intelligence capacity is kept as autonomous as possible, without losing sight of international cooperation.

However, the Standing Committee I points out that detecting transactions with regard to proliferation appears to be difficult – both for the intelligence services as well as for their partners – due to several reasons:

- the potential civil and/or military use (dual use) of many materials and technologies;
- the large number of transactions and export activities to 'proliferation countries';
- the lack of reliability and transparency of the information provided by the companies involved in the export of proliferation materials;
- the complexity of the international system for the coding of goods by customs services and the ease with which this system can be bypassed.

Moreover, the conclusion that regulations for certain export operations were violated is not, in itself, irrefutable evidence or a clear indication that there is a link with proliferation. Therefore, it should be possible to establish an actual 'link' with companies, organisations, persons, addresses, programmes and/or *sites* whose activities are known to be connected with proliferation.

But the Standing Committee I is forced to conclude that there is a tendency in Belgium of underestimating the contribution of the intelligence services in this matter, despite the clear intention of pursuing an effective policy so as to respect international agreements.

Earlier the analysis service of State Security had more resources at its disposal to cope with the increased number and urgency of the tasks to be carried out. However, the consequences of this increase in resources are not yet clearly noticeable within the framework of the fight against proliferation. The human resources that State Security and the GISS (can) presently deploy in this matter, are too limited. This lack of resources can possibly provide an explanation for the lack of proactiveness found by the Standing Committee I with regard to, for example, the prevention of certain export operations involving sensitive products or products for dual use to a so-called 'proliferation country'.

Both services do, however, have a detailed (theoretical) plan regarding the manner in which they want to tackle this issue. In addition, the Standing Committee I wants to emphasise the high quality of the analysis reports examined by it. These show that the intelligence services have a thorough understanding of the scientific and technical information as well as of the geostrategic interests. These analyses, drawn up with a critical mind, were aimed at independently arriving at a realistic picture and a correct assessment of the threat.

II.5. MONITORING THE ACTIVITIES OF NEO-NAZIS AND THE RECRUITMENT AND MANAGEMENT OF INFORMANTS WITHIN THIS FRAMEWORK

II.5.1. RECRUITMENT OF AN INFORMANT

Within the framework of collecting information on extreme-right movements, a local section of State Security approached a person who appeared to be well-placed in the neo-Nazi milieu. It seemed that not only was he quite ready to cooperate, but that he already had experience as a long-term informant of the GISS.

As 'occasional informant' (OI), he brought in relevant information very regularly. State Security therefore quickly decided to recruit him as a 'centrally registered informant' (CRI).[55] But during the security investigation[56] preceding such a registration, something went wrong. The local section of the GISS consulted by State Security gave a not-so-obvious explanation of the reason for ending the cooperation with the person in question. The real reason for his dismissal did not come up: the informant had become increasingly unreliable, supplied fictitious information and occasioned increasingly higher expenses. Besides, State Security had not informed the GISS that they were planning to recruit the person in question. Neither had they contacted the central GISS level.

The person in question was registered as CRI for a trial period. He received a fee and an allowance for his expenses. The informant had very regular contacts

---

55 The 'centrally registered informant' is an informant who, after a security investigation and by the decision of the Director-General, is registered under a code number (initially for a trial period) and of whom it is expected that he or she functions as a human source on a regular basis, often against payment.

56 Such an investigation must be clearly distinguished from the security investigation conducted within the framework of the Act of 11 December 1998 on classification and security clearances, certificates and advice. There is no legal basis for the security investigation to which informants are subjected. The intelligence services tend to conduct this investigation according to their own requirement and culture.

with his runner and initially supplied a great deal of sound and plausible information. He could also regularly provide answers to questions posed by State Security. After a short time, however, the cooperation became more difficult. At the same time, he demanded more money and could provide no proof of his alleged movements. The informant appeared to be difficult to control and made references to a new, extreme-right, violent splinter organisation that was rapidly growing within Europe. These spectacular 'revelations' could not, however, be confirmed by foreign correspondents of State Security. It also appeared that the information supplied did not correspond in any way with the information received by State Security via other channels. Furthermore, it was proved that his statements about his movements were false. When confronted with this, he came up with a story, after which State Security concluded that both he and the information he supplied were untrustworthy. Thereupon, he was – justifiably – dropped as informant.

II.5.2. MONITORING OF NEO-NAZIS BY THE INTELLIGENCE SERVICES

For a considerable time now, neo-Fascist or neo-Nazi movements and individuals with similar sympathies are being monitored by State Security and the GISS. Presently, State Security is doing this within the general framework of 'extremism' (Art. 8, 1°, c of the Intelligence Services Act). Both services focus primarily on the same groups, with the understanding that the GISS is specifically interested in servicemen reported to be members of such movements. The subject is mentioned as such in the annual steering plan of the GISS. Extreme-right groups also figure in the list of subjects to be monitored by State Security.

Considering the rather limited resources deployed, this subject matter does not really seem to be a priority for either of these two services. This was also admitted by them in so many words.

In terms of reporting, the GISS makes mention of three to four reports per month while State Security has produced an average of more than a hundred reports per year over a period of four years.

As regards the provision of information to other authorities, the GISS restricted[57] itself to supplying information to the Minister of Defence. However, intelligence was also exchanged punctually with the police services. State Security referred to about 40 memos in connection with (neo-)fascist organisations or persons, which had been sent to other authorities within a period of one year. Furthermore, within that same period of four years, State Security exchanged more than 200 messages with foreign correspondents.

[57] This conclusion is with reference to the pre-CUTA period.

With regard to the mutual exchange of information between the two Belgian intelligence services, the GISS referred to '*bilateral contacts within the general framework of the extreme-right movement, but not specifically aimed at neo-Nazi movements*' (free translation). State Security, on its part, specified that this involved "*half-yearly consultations regarding current evolutions and tendencies within the extreme-right milieu in Belgium*' (free translation) with the understanding that information is also exchanged, verbally or in writing, regarding actual dossiers as and when the situation requires this.

Both services stated that most of their information on neo-Nazi movements comes from informants who supply information either for financial or ideological reasons. Precisely because informants are so important for the monitoring of these phenomena, the necessary attention must be paid to their reliability and to that of the information they share. At the GISS, this control is carried out by testing the supplied information based on existing intelligence, via debriefings, regular screenings and even via observations. State Security carries out an extensive background check and works with a trial period during which the reliability of the supplied intelligence is assessed. But did this preventive system work in the present case?

II.5.3. CHECKING THE RELIABILITY OF THE INFORMANT IN QUESTION

The dubious informant had also been subjected to an extensive screening. But the Standing Committee I questioned the fact that State Security had not contacted the central services of the GISS and the lack of scepticism in the face of a not very convincing explanation about the way in which the cooperation between the informant and the GISS had been terminated. But the Committee believed that this could be clarified by the justifiably high expectations from the informant, in view of his position within the milieu, his background and the initially supplied information. After all, such informants are scarce.

The Standing Committee I is aware that no control system is waterproof. On the other hand, it was of the opinion that, had there been a better communication between State Security and the GISS, it would have been immediately apparent that the informant could not be trusted. Of course, this also assumed that State Security would have clearly informed the GISS about the reason why it required information on the person in question. At that time, if the GISS had faithfully interpreted the obligation of providing '*the most effective mutual cooperation as possible*' (Art. 20 of the Intelligence Services Act – free translation), a more objective picture of the person in question would have emerged. Obviously, such openness means divulging the identity of a (current, potential or former) informant to a sister service. The Standing Committee I is of the opinion that *in casu* this would not be contradictory with the obligation of safeguarding the

security of the information relating to human sources (Art. 18 of the Intelligence Services Act). The 'sparse communication' on the part of both intelligence services turned out to be completely counterproductive.

However, the Standing Committee I was convinced of the fact that State Security was very alert in its monitoring of the person after he was recruited, which led to a swift termination of the cooperation.

II.6. PROTECTION OF THE SCIENTIFIC AND ECONOMICAL POTENTIAL (SEP) AND THE BELGIAN AEROSPACE INDUSTRY

The attention of the Standing Committee I was drawn by the sale of a Belgian company, active in the aerospace industry, to a foreign group partially controlled by a non-European consortium.

The founder and primary shareholder of the company in question himself took the initiative for this sale to a foreign group in order to give his company a European profile and thus ensure better access to important European aerospace programmes.

The acquiring foreign group was created as a result of the attempts of a European government to achieve a partial privatisation of its arms production. There was a lot of criticism regarding this privatisation operation by those who believed that a sector that is so significant for a country should not be handed over to the private sector. The government in question remained the primary shareholder of the acquiring group, but after some time a non-European investment consortium acquired a participation in the capital of the group. This participation was approved by the European Commission.

Since the common factor between the companies owned by the consortium is that their largest customers are governments and public authorities, reports soon appeared in certain media about a possible conflict of interests and interference in the political decision-making process.

The non-European consortium also develops its activities in Europe via participations in companies active in the arms and aircraft groups participating in a European project.

The Parliament has often laid emphasis on the strategic, civil and military importance of the aerospace industry. This is not only important at a national level, but also and more particularly, in a European context. Since, as far as its aerospace programme is concerned, Europe strives for autonomy with respect to competing powers. The strategic significance of this sector needs to be placed above the commercial interest of the companies in question.

The Belgian Senate has repeatedly argued in favour of an active involvement of the Belgian authorities in protecting this sector of activity.[58]

In view of the investigative and developmental capacity of the concerned company in an area that can be of importance for national security and which, moreover, was and is regarded as a priority by State Security for safeguarding the scientific and economic potential (SEP), the Standing Committee I wished to know whether the company in question had drawn the attention of either State Security or the GISS.

The Standing Committee I also made enquiries regarding the resources presently deployed by intelligence services for safeguarding the SEP and about the current priorities in this field.

II.6.1. STATE SECURITY

II.6.1.1. Priorities for protecting the SEP

For the main principles of its approach to safeguarding the SEP, State Security refers to the definition and action plan for the SEP as approved in 2007 by the Ministerial Committee for Intelligence and Security (MCI&S).

In that action plan, four priorities come to the fore. A first priority is to tap external (relevant) expertise. A second priority is to counter economic and scientific espionage and interference. This includes economic and scientific espionage by foreign intelligence services in Belgium or by private intelligence firms as well as the protection of specific knowledge and information companies.[59] Monitoring the infiltration of criminal capital flows in the regular economy is the third priority. In particular, the evolution of organised crime in Eastern Europe is very significant in this respect. The fourth and last priority is to raise awareness among involved parties in a targeted manner, i.e. by focusing on concrete threat information.

II.6.1.2. Resources deployed for protecting the SEP

A section of the field services is entrusted with the protection of the SEP, the proliferation issue and security investigations with a view to the issuance of

---

58 Report on behalf of the Finance and Economic Affairs Committee and the 'Aerospace' Working Group, *Print.*, Senate, 2002-2003, 1332/1, and Report on behalf of the Federal Advisory Committee on European Affairs, together with the Finance and Economic Affairs Committee and the 'Aerospace' Working Group of the Senate and the Committee for Trade and Business and the Advisory Committee for Scientific and Technological Issues of the House of Representatives, *Print.*, Senate, 2002-2003, 1521/1.

59 These are companies which, owing to the nature of their activities, have sensitive or valuable information on other companies or private individuals, such as SWIFT and Euroclear.

security clearances to companies. The remaining field services may also carry out investigations within the framework of safeguarding the SEP when companies are threatened, specifically by criminal organisations or harmful sectarian organisations.

The provincial posts of State Security have a general scope of competence. This means that they must handle all the tasks entrusted to this service. In each of these provincial posts, at least one inspector is entrusted with (among other tasks) the protection of the SEP.

The Standing Committee I believes that State Security does not have sufficient staff resources to perform this task efficiently, especially in view of the multitude of tasks and facets related to this assignment. The Standing Committee I is also of the opinion that the number of analysts deployed within the framework of safeguarding the SEP, is inadequate.

II.6.1.3. Monitoring of the company in question

Regarding the safeguarding of the SEP, State Security has pointed out that the sector in which the company in question is developing its activities, is one of its priorities. More specifically, it considers the field of aerospace programmes from the perspective of the fight against the proliferation of weapons of mass destruction.

State Security's interest in the company was and is primarily prompted by its scope of competence regarding the non-proliferation issue, and not so much because of the fact that the company has been acquired by a foreign group.

In a report about an earlier transaction between the company and a foreign power, the technical reasons were examined in detail and it was concluded that there was no risk of a inexpedient transfer of technology.

Other reports show that the interest of State Security in the concerned company stretched beyond the non-proliferation issue. The last examined report concerns the sale of the Belgian company to the European group and underlines the economic significance of this take-over because of the opening up of new markets. This short report, drafted on the initiative of State Security, was primarily composed based on open sources.

It appears that after this, State Security did not draw up any further reports or analyses about the company in question. Of the mentioned reports, not a single one was sent to any authority or agency besides State Security.

For State Security, the simple reason resides in the fact that there was nothing to report.

The report concluded that there was no danger. As a result, State Security seemed unnecessary to sent a memo to the authorities. Only if there is a prior request for information or technical assistance, will State Security send a memo if it should appear that there is no threat after all. That is an important premise for State Security; no memo is sent if there is no threat.

II.6.1.4. Standpoint of State Security

With reference to the Intelligence Services Act as well as the definition and Action Plan 2007 of the SEP, State Security believes that foreign take-overs of Belgian companies is not one of its priorities.

State Security is, therefore, of the opinion that it is not its task to trace and communicate information other than that related to the threats as defined in Article 8 of the earlier-mentioned Act, namely espionage, interference, terrorism, extremism, proliferation, harmful sectarian organisations and criminal organisations. In the absence of a different definition of its assignment with regard to the protection of the SEP, State Security does not consider itself legally competent to carry out other types of investigations and assessments.

With regard to the take-over of a Belgian company by a foreign group, State Security has never viewed this transfer from any angle other than that of a commercial transaction which was carried out legally on the initiative of the company itself and which was favourable for its economic development. Since no possible risk of interference or espionage had been taken into account in relation to this transaction, State Security did not send any communication to the authorities. The monitoring of take-overs of Belgian companies by foreign groups is not a priority for State Security, especially if these transactions are prompted by economic reasons and carried out by the concerned private players.

State Security believes that it is not its task to monitor normal economic evolutions, even though these could be unfavourable for the SEP.

Nevertheless, State Security deems it appropriate that a legal regulation be formulated for the strategic sectors (including critical infrastructure) which would define conditions for foreign investments and commercial activities in the strategic sectors and the role of the intelligence services, if any.

II.6.1.5. Standpoint of the Standing Committee I

The limited interest of State Security in the take-over of the Belgian company by the foreign group may prima facie appear to be justified. If considered more closely, however, the standpoint of State Security lacks nuance.

It would therefore be a sign of short-sightedness to allow oneself to be *a priori* blinded by the legal and economically justified nature of the transaction, which at first sight does not cause one to suspect any hostility. State Security is rather quick to overlook the not unlikely idea that this apparent conformity may be a potential cover for underlying transactions or agendas which can certainly be considered as threats regarding which it has tasks to fulfil within the framework of the SEP. *In casu*, the Standing Committee I feels that State Security has too quickly, if not immediately, decided that there is no such danger, even when this was preceded by little or no prior investigation. The only initiatives taken are the

reflections on the economic desirability and even the necessity of the transaction, but then merely from the standpoint of the company.

But that is where it stops, despite the conclusion that the take-over – at least according to certain open sources – is not entirely undisputed. The Standing Committee I therefore believes that there was definitely sufficient reason to justify, and even demand, a more in-depth interest in this take-over.

On the other hand, no account has been taken – or assessments been carried out – with the conflicts in interest which may arise from the take-over of the control of the company by a foreign group in which non-European military-industrial interests are strongly represented, nor with the possible consequences of these conflicts in interest on the attempts of certain European aerospace projects to gain autonomy.

Surely, this is the primary role of the intelligence services?

Just as the Finance and Economic Affairs Committee of the Senate[60], the Standing Committee I is of the opinion that space is primarily a strategic sector. Therefore, one must indeed look beyond the purely commercial interest. European autonomy in these sectors is of strategic importance for the future of Europe. However, during the hearings of the Committee, it was found that the European industry is becoming increasingly dependent on basic components supplied from the United States and Japan. This is an evolution which must be monitored.

In any case, the Standing Committee I still believes that the take-over of the Belgian company by the foreign consortium should have received the attention of State Security. Not only within the framework of the assignments currently assigned to it, as specified in Article 7, 1°of the Intelligence Services Act, but also in terms of a broader attention for certain tendencies which can hinder the autonomy of our strategic sectors.

II.6.2. THE GISS

The Standing Committee I could establish that the GISS never carried out a proper investigation into the company in question and neither did it make a more detailed examination of the activities of this company.

The only monitoring carried out by the GISS with regard to the company in question consisted of simply collecting documents from open sources, keeping in mind the sensitive nature of the activities developed by some branches of this company.

---

60 Report on behalf of the Finance and Economic Affairs Committee and the 'Aerospace' Working Group, *Print.*, Senate, 2002-2003, 1332/1.

II.6.2.1. Standpoint of the GISS

The GISS is only authorised to carry out an investigation into a Belgian company if the latter has submitted a request for a security clearance for itself or for staff members in order to be able to participate in a call for tender issued by the Defence Department.
The GISS justifies its position by referring to the principles of the partnership entered into five years ago between the GISS and State Security with regard to the protection of the economic and scientific potential. The GISS is solely competent (in terms of analytical monitoring, briefings for raising awareness, investigations and other operational activities) in cases where the company or the institution in question is authorised by Defence.

In all other cases, only State Security is authorised to take action unless it explicitly requests our service to act.

The Standing Committee I was also informed by the GISS that the latter could not get involved with the protection of the SEP since it lacked the required analysts. This would have a direct influence on the effort and the quality of the work in this matter.

II.6.2.2. Standpoint of the Standing Committee I

With regard to the GISS, the Standing Committee I concluded that the Act defining the legal assignments of this service does not indeed allow this service to carry out preventive investigations into economic transactions such as take-overs or absorptions of Belgian companies by foreign groups, even when these companies might be directly involved in a Belgian or European military programme.

But the Standing Committee I believes that the potential military importance of a company established on national territory merits the preventive attention of the GISS if the company is question is transferred to foreign hands.

II.7. THE MILITARY INTELLIGENCE SERVICE, CONGO AND THE ELECTION CAMPAIGN

In May 2006, the attention of the Standing Committee I was drawn by the alarming tone of some press articles which referred to increasing tension in the Congolese capital shortly before the presidential election of 30 July 2006. According to a journalist, the situation even brought back echoes of '*le climate délétère qui régnait au Rwanda en mars 1994, à la veille du génocide*' (the poisoned climate that gripped Rwanda in March 1994, just before the genocide). The reference to these dramatic events could not fail to rouse the concern of the

Committee, considering that in the same period there was a possibility of a Belgian military contingent participating in the EUFOR mission in the Democratic Republic of the Congo (DRC).

The Standing Committee I therefore initiated an investigation into the manner in which the GISS had monitored the events in the DRC and its analysis of the general situation in this country prior to the elections and particularly, of the security situation in Kinshasa. The aim was to verify whether the military intelligence service had information which could either confirm, negate or put into perspective the tense situation as it had been described in the press.[61] The report therefore dealt with the monitoring of the situation during the first half of 2006.

II.7.1. THE POLITICAL AND MILTARY CONTEXT OF THE BELGIAN PARTICIPATION IN THE EUFOR MISSION IN THE DRC

II.7.1.1. The situation as described by the Belgian press

In May 2006, the press reported a growing climate of tension in the Congolese capital, further intensified by the media warfare involving the presidential candidates just a few months before the elections. According to this report, malicious remarks were the order of the day in the press and even Belgium was not spared.
The attention of the Belgian press in the security situation in the DRC during the first half of 2006 also concerned numerous other problems such as military skirmishes in the east of the country, the plundering of the country's natural resources by foreign companies, illegal transport of arms, the presence of child soldiers in the armed militias …

II.7.1.2. MONUC and EUFOR missions in the DRC

The UN Mission in the Democratic Republic of the Congo (MONUC) was set up on 30 November 1999 by Resolution 1291[62] of the Security Council of the United Nations, in pursuance of the Lusaka Agreements for organising the transition to democracy in the DRC. The purpose of these agreements was to bring an end to

---

61 The Standing Committee I had carried out a similar investigation in the past, when it attempted to establish the way in which the intelligence services had monitored the events in Rwanda (1994). See in this regard: STANDING COMMITTEE I, *Rapport d'activités 1996*, 120-136, 'Report of the investigation regarding the efficiency and cooperation of the intelligence services in connection with the events in Rwanda'.

62 Resolution 1291 (2000) adopted by the Security Council at its 4104th session, 24 February 2000. This was followed by Resolution 1711 (2006) adopted by the Security Council at its 5541st session, 29 September 2006. In view of the continuing disturbances in the east of DRC, the assignment of the MONUC was extended several times.

the civil war raging in the country for several years. The assignment consisted of four phases: the first phase was aimed at the implementation of the Lusaka Agreements for ceasefire; the second phase involved the monitoring of any violation of the agreements via the appropriate channels; the third phase was with regard to the DDRRR process (Disarmament, Demobilisation, Repatriation, Resettlement and Reintegration of the members of the militia) and finally, the fourth phase involved the organisation of reliable elections in the DRC. In the course of 2006, the international community put in a great deal of effort in helping the DRC government organise successful and safe elections. The international community was concerned that violence would possibly break out before, during and after the elections which the armed forces of the DRC would not be able to control.

On 27 April 2006, the Council of the European Union decided to send a military force, 'EUFOR RD Congo', to the DRC.[63] With this, the European Union responded to the call of the UN Security Council[64] to cooperate in safeguarding the Congolese elections. EUFOR RDC received the assignment of assisting the 17,600 UN peacekeepers of the MONUC and to help them counter a possible escalation of the violence during the election period. The European Union declared itself ready to allow the MONUC to make the maximum possible use of intelligence gathered by the European peacekeeping forces, in accordance with conditions to be specified in further detail.[65]

II.7.1.3. Belgian military presence in the DRC and its contribution to the EUFOR RDC missions

Africa occupies a special place in Belgian foreign policy and this is particularly applicable for the DRC and the countries in the area of the Great Lakes. This Africa policy is primarily focused on creating partnerships for peace and discouraging conflict movements. The Ministry of Defence is also obliged to be prepared to carry out evacuation operations for citizens, if necessary. This means that there are evacuation plans for Belgian and European citizens living in the DRC. Pursuant to the recommendations of the Rwanda Commission, the participation of Belgium in peacekeeping operations was rather limited.[66]

---

63 Council joint action 2006/319/CFSP of 27 April 2006, *Official Journal,* L 116, 29 April 2006. The EUFOR RDC operation was officially launched on 12 June 2006 and was allowed for a period which would expire four months after the date of the first round of elections. The assignment came to an end on 30 November 2006.

64 Resolution 1671 (2006) adopted by the Security Council at its 5421st session, 25 April 2006.

65 Letter of 28 March 2006, addressed to the Secretary-General of the United Nations, sent by the Minister of Foreign Affairs of Austria on behalf of the Council of the European Union.

66 In December 1997, the Rwanda Commission formulated its advice of not allowing any more Belgian soldiers to participate in the UN peacekeeping missions in the former Belgian colonies. Despite this, from June to September 2003, Belgium participated in the Artemis operation which was the first military peacekeeping operation carried out by the European

In February 2006, the then Minister of Foreign Affairs stated that he had reservations about the Belgian participation in an intervention force in Congo and thereby declared his support for the conclusions of the Rwanda Commission. However, the then Minister of Defence referred to the Artemis Operation and considered sending out 'medical or intelligence personnel' temporarily.[67] Subsequently, on 21 March 2006, the press announced that '*Belgium would send forty troops, including specialists in the area of intelligence and unmanned aircraft, to reinforce the European forces (EUFOR RDC) entrusted with the task of safeguarding the elections in the DRC*' (free translation). After discussions, Belgium eventually did participate in the EUFOR RDC mission by sending a detachment of fifty troops as well as a medical team and operating personnel for four unmanned reconnaissance aircraft (teleoperated UAVs or unmanned aircraft).[68] These had to be completely operational from 29 July 2006 and were assigned the task of flying over Kinshasa in order to detect any suspicious events. This was an assignment related to intelligence gathering and cartography.

It appeared from certain articles appearing in the Belgian press halfway through 2006 that the Congolese opposition was hostile to this development, which was presented as '*a planned bloodbath for all Congolese people resisting the new colonisation of their country*' (free translation).

At the end of the EUFOR RDC mission, the Belgian contingent withdrew in December 2006.

II.7.2. ACTIVITIES OF THE GISS

The situation in the DRC was monitored by the *Intelligence* department of the GISS.

This department provided the Standing Committee I with a very large number of documents which showed that it had been closely involved in the monitoring of the military, political and social events in the DRC during the period prior to the elections. Most of these documents were classified as 'CONFIDENTIAL' or 'SECRET'. The Standing Committee I focused primarily on the assessments of the security situation in Kinshasa, where the Belgian contingent of EUFOR RDC had carried out its assignment during the period preceding the elections.

Union within the framework of the European Security and Defence Policy (ESDP). In 2003, a partnership agreement was also concluded which was primarily with regard to the integration of the Congolese army (FARDC), for which Belgian military personnel organised trainings and aerial transport.

67 *Deliberations*, House of Representatives, 2005-2006, 15 March 2006, CRIV 51 COM 893, Defence Committee.

68 The UAVs had already been shipped to Congo from Zeebrugge on 19 May 2006. This was made public only on 28 May 2006.

The information gathering and analysis activities of the *Intelligence* department are determined on the basis of the annual steering plan of the GISS. Since, it is this document that determines the priorities of the various departments, depending on the foreign missions of the Belgian armed forces. Given that the Belgian foreign policy in 2006 devoted a lot of attention to the DRC, this country was given high priority by the GISS. Based on these priorities, the analysts also draw up a number of periodic or specific bulletins as well as other exclusively military reports.

With regard to the actual elections, the political developments as well as the evolution of the situation were the subject of continuous attention and very detailed monitoring. Several analysis documents were devoted to the DRC and the imminent elections as well as to the security risks in the period before and after the elections.

The evolution of the security situation in the DRC was of central importance in most of the analyses made by the GISS in 2006.[69] Moreover, the GISS also paid attention to the progress of various aspects of the election campaign. The military intelligence service described the logistical difficulties in organising elections in a country where the infrastructure is not always suitable and there are political trends which could give rise to incidents during the campaign.

For the GISS, the presence and involvement of the international community appeared to offer the only guarantee for stability.[70]

From April 2006, the reports refer to the climate of tension and nervousness in which the election campaign was being conducted. Without sounding alarming, the reports described situations which, depending on the period and from the security point of view, could be regarded as anything between more or less satisfactory to disturbing. But the GISS still advised caution and emphasised that a calm situation could worsen very quickly. The demonstrations and meetings were accurately described and were the subject of analyses which offered a better insight into the latent interests at stake and the security threats arising from these.

---

69 As early as in December 2005, the GISS had written a study about the '*transition*' and the election process in the DRC. This document described the risk factors in the area of politics as well as security.

70 In March 2006, the then Minister of Defence had decided that, despite the postponement of the elections (which were initially supposed to take place in 2005), the situation in the DRC was satisfactory for organising elections (*Deliberations*, House of Representatives, 2005-2006, 15 March 2006, CRIV 51 COM 893, Defence Committee).

II.7.3 ASSESSMENT OF THE REPORTS OF THE *INTELLIGENCE* DEPARTMENT

The Standing Committee I found that the reports of the military intelligence service showed evidence of a thorough knowledge of both the political and security situation in the country as well as of the situation in the field.

The Standing Committee I was of the opinion that the reports had been designed with care, with importance given to visual elements both with regard to the presentation of the texts as well as the maps, photos … Numerous illustrations (satellite images, maps, diagrams) aided the understanding of the texts and spared the reader long and difficult descriptions. The content of the reports was sober, detailed and precise, and was usually accompanied by comments. The tone of the consulted reports was neutral and objective. The words used avoided any tendency towards sensationalism.

The question is whether the press and the military reports were on the same wavelength. The dramatic tone of some press articles, which compared the situation in the DRC with that in Rwanda before the genocide of 1994, drew the attention of the Standing Committee I and was the direct cause of this investigation. The Standing Committee I found that all the events and facts discussed in the press were mentioned in the GISS reports. As opposed to some press articles which reported isolated facts, the military reports ensured that these facts were monitored over time. The military reports consulted by the Standing Committee I described the progress of the election campaign in a less dramatic tone than the press. They neither concealed nor minimised the tensions which were inherent in the election process. Though the GISS referred to the topic of the '*congolité*'[71] which has fuelled the debate between the main presidential candidates, no calls to racial or ethnic hatred or to xenophobic behaviours, except perhaps to a marginal extent, were mentioned. The GISS also noted a growing feeling of 'opposition to western interference'. But this feeling, which was further reinforced with the development of EUFOR, was not one that would jeopardise the course of this mission. During the period under investigation (March to July 2006), the threat assessment was never raised to the highest level. The repatriation of the Belgian and European citizens living in the DRC was never considered.

II.7.4. CONCLUSIONS

The main assignment of the GISS consists in gathering and processing intelligence related to any activity whatsoever which constitutes or could constitute a threat to the execution of the assignments of the armed forces or to

[71] The sense of being connected with an ethnic group of Congolese origin.

the safety of Belgian nationals abroad (Art. 11 of the Intelligence Services Act). In this investigation, the Standing Committee I could establish that the GISS also generated socio-political intelligence and analyses that offered an overall insight into the context within which this assignment had to be carried out. These analyses were accurate and detailed. The Standing Committee I found that the various Belgian authorities involved were addressees of information from the GISS. The analyses made by the GISS of the security situation in the DRC during the period preceding the elections, were consistent with the facts: the progress of the EUFOR RDC mission and that of the elections of 30 July 2006 was fairly satisfactory. In this sense, the GISS appears to have drawn the necessary lessons from the dramatic experience in 1994 in Rwanda.

But such a high-quality analysis is not possible without having access to sufficient numbers of qualified staff. In this connection, the Standing Committee I found that the number of analysts working with the GISS has sharply declined since then. This service will not be able to maintain the continuity and the quality of its analyses if the number of staff in its analysis department is not restored to the 2006 level.

II.8. COMPLAINT AGAINST A HEAD OF DEPARTMENT OF THE CUTA IN CONNECTION WITH THE HANDLING OF AN INCIDENT WITH A MEMBER OF STAFF

Mid 2008, a staff member of the CUTA had a fall. This fall appeared to have been (un)intentionally caused by a colleague.

When a Head of Department of the CUTA was notified of the incident, he gathered information from as many people as possible to arrive at a well-informed assessment of whether the CUTA needed to start legal proceedings against the colleague of the staff member.

This colleague, however, had the impression that the Head of Department had immediately initiated a disciplinary or administrative procedure against him, while he was left in the dark regarding the actual nature of this complaint. According to him, this impaired his fundamental rights and his chances of preparing his defence.

After an in-depth investigation (questioning of the most important parties involved, examination of documents and analysis of the entire incident), the Standing Committee I and the Standing Committee P jointly reached the conclusion that there was insufficient evidence or objections to substantiate the complaint of the colleague of the staff member.

II.9. THE ALLEGED INTERVENTION BY A MEMBER OF STATE SECURITY IN THE COMMERCIAL ACTIVITIES OF A COMPLAINANT

In 2003, a complaint was lodged by a private individual against a State Security inspector. The complainant was active in the real estate market. He was involved with finding sites for large projects and taking care of the licence applications. He had been active in this area for some time, along with a partner who was residing in Belgium illegally. More than often however, negotiations with regard to certain acquisitions, which involved millions of euros, appeared to come to nothing. Furthermore, mid-2002 a warrant for arrest was issued against the complainant and his business partner on suspicion of money laundering practices. The complainant was of the opinion that he and his business partner had aroused the unsavoury personal interest of an inspector of the State Security service. It was alleged that this inspector – taking advantage of his position – had left no stone unturned to thwart or seriously hamper all their projects by regularly describing the duo as being unreliable and advising that they be avoided. The complainant therefore believed that his reputation as an honest businessman had been seriously damaged.

Shortly after submitting his complaint, the concerned person also lodged a civil complaint with the investigating magistrate. He accused the inspector of misuse of authority (Art. 254 of the Penal Code) and libel (Art. 443 of the Penal Code). To avoid obstructing the judicial inquiry, the Standing Committee I suspended its investigations. Both the pre-trial chamber as well as the Indictment Division decided to discontinue the criminal proceedings against the inspector.

Mid-2008, the Standing Committee I gained access to the criminal dossier. From this it appeared that all persons, with whom the complainant claimed to have been discredited, had been questioned during the judicial inquiry. Yet nine out of the ten persons [72] – mostly owners of prime real estate – did not confirm the complainant's accusations. They stated that they had been contacted by the inspector in question, who was apparently looking for information about the business partner of the complainant. However, on these occasions the inspector had apparently informed them that it was always advisable to exercise care in such transactions. But none of the witnesses referred to insinuations intended to put the complainant in a bad light. Neither did the interview with the inspector appear to be the determining factor for calling off further negotiations with the complainant and/or his business partner.

---

[72] Only one person presented a different version. According to him, the inspector was not neutral and had even advised against doing any further business with the duo. Moreover, this person, who was clearly the only person with this story, did not at first sight appear to face any personal financial risk if the deal was called off.

In addition, the investigation of the Standing Committee I revealed that the gathering of information on account of the complainant and his business partner was one of the legal matters assigned to the inspector, namely organised crime. Moreover, the intelligence gathering activity was the subject of a strict reporting to the Head of Department as well as to the competent judicial federal police.[73] Finally, the inspector was described by his Head of Department as an experienced staff member with a flawless reputation and a sense of diplomacy. Legitimising oneself with respect to interviewees – which should be *standard policy* with State Security – may, in no way, be considered a form of intimidation or misuse of authority.

Therefore, the Standing Committee I did not find any evidence which might indicate that the inspector had not acted in the proper manner.

II.10. THE ALLEGED INTERVENTION BY STATE SECURITY IN PUBLIC INSTITUTIONS

A complainant suspected State Security of an ill-considered intervention in one or more public institutions from which he expected to receive an assignment. This intervention allegedly caused him serious damage.

However, the investigation of the Standing Committee I has revealed that State Security has not in any way made an ill-considered intervention with respect to the complainant in any institution whatsoever.

II.11. INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2008 AND INVESTIGATIONS INITIATED IN 2008

This section contains a summary and a brief description of the investigations in which important investigative steps were taken in the course of the operating year 2008, but which were not completed.[74] Likewise, all investigations initiated

---

73 It must, however, be noted, as an aside, that the business partner was sentenced by the Correctional Court to a prison term of four years for money laundering (among other charges) and millions of euros were seized. The complainant was acquitted. Therefore, the interest of State Security appeared *a posteriori* to have been more than legitimate.

74 In addition to these investigations, there are two other investigations pending with the Standing Committee I, which were initiated earlier but for which no investigative actions were taken in 2008. These concern an investigation into the cooperation of State Security in a house search – in which a response is awaited from the Standing Committee P – and an investigation into the contribution of the intelligence services in the judicial inquiry into a network of Jihadists recruiting for Iraq. This investigation could not be dealt with because of other priorities.

in 2008 are mentioned, even if no investigative steps could be taken as yet in this regard.

II.11.1. A PERFORMANCE AUDIT OF STATE SECURITY

The Coalition Agreement[75] of March 2008 stated that '*our country will step up the fight against international terrorism. It guarantees the proper operation of the Coordination Unit for Threat Assessment (CUTA) and a dissemination of the information to the judicial authorities to monitor, together with the Parliament, the proper exchange of information between the various services. The review activities must be structurally organised. This means that the legislation on particular investigative methods must be urgently amended and a legal framework must be adopted for the particular methods for receiving and exchanging information from the intelligence and security services, with respect for fundamental rights and freedoms. Because the proper operation of the intelligence services is essential for all this, the government will examine, based on an audit, whether the operation can be improved and if so, how this must be done*' (free translation).

This intention – i.e. examining based on an audit whether and how the operation of the intelligence services can be improved – was confirmed and reiterated in the general policy document of the Minister of Justice[76], evidently only with respect to State Security which falls under his scope of competence.

This task was assigned to the Standing Committee I. The assignment commenced in September 2008 and included carrying out a *performance audit* with the objective of '*investigating and assessing 'how' the activities of State Security are carried out, based on the criteria of efficiency and effectiveness*'[77] (free translation). It is not the first time that State Security was subjected to an audit. Such an audit had been carried out earlier by the Standing Committee I (Audit 2002-2003), and State Security had carried out a self-assessment prior to the Master Plan and the launch of the improvement projects within State Security (CAF 2003-2004). In line with earlier conclusions of the Standing Committee I, State Security implemented an overall IT project (Project Vesta). This project commenced with an audit carried out by an external consultant. In this project, the Standing Committee I has already completed the first phase of an investigation of the information flows within State Security.[78]

The current *performance audit* includes four central themes.

---

75 *Print.*, House of Representatives, 2007-2008, 20/2, 42-43.

76 *Print.*, House of Representatives, 2007-2008, 995/3, 27-28.

77 *Ditto.*

78 Also see 'II.3. The information processes of State Security' and 'II.10.4. Information management at State Security' from previous Activity Report (STANDING COMMITTEE I, *Activity Report 2006*, *Activity Report 2007*, 101).

Firstly, the leadership aspect is given special attention. The following questions are considered: How is the organisation managed, especially in terms of its policy objectives? Does the management take into consideration the specific competence levels of its staff? What is being done, from the perspective of competence management, to continually optimise staff management? How does the institution apply a strategic staff policy in order to strive towards the realization of organisational goals?

The next theme is information management. The following aspects are dealt with: How are the principles of availability, accessibility and permanency of information and staff guaranteed? What can be said about the speed and flexibility of the information and of the staff? For example, how is the work schedule structured to provide quick, efficient and continuous services?

Thirdly, this performance audit examines the work processes: Is the flow and processing of the information managed in an efficient manner? Are these work processes mapped and optimised on the basis of a clear vision? What concrete recommendations could help to achieve this, if required?

Finally, a number of quality and customer satisfaction aspects are discussed: Are there systems in place to measure the satisfaction of customers and staff with regard to the input and output of information? Are the Belgian customers of State Security (e.g. political, police and judicial authorities) satisfied? Which elements could be provided to monitor this better? For example, how is a consistent application of the declaration obligation, stipulated in Article 29 of the Code of Criminal Procedure, actually being monitored and controlled? Is State Security itself satisfied over the information received by its domestic and foreign customers?

The audit activities in 2008 were primarily aimed at drawing up an audit plan and developing a thorough methodological base. The next step was the collection and analysis of information based on the examination of documents, various enquiries via interviews or questionnaires and on-site controls. Within this framework, enquiry tools were developed (questionnaires, interview plans …), quantitative and qualitative information was collected and verified for its accuracy and completeness, data was analysed and the data gathered was checked against existing standards.

It is expected that the Standing Committee I will have communicated its findings to its principals halfway through 2009.

II.11.2. INFORMATION MANAGEMENT AT THE MILITARY INTELLIGENCE SERVICE

At the end of November 2005, an investigation was initiated into the way in which the military intelligence service manages and uses the information it obtains. In this connection, the existing instructions were one of the subjects of

investigation, and clarifications were sought regarding the way in which the GISS stores, manages and uses the personal information it obtains.

In 2008, the Standing Committee I suspended the investigation. The reason for this was the announced integration of the *Intelligence* and *Counterintelligence* pillars. Since, the initial reason for starting this investigation was that, in an actual case, there had been a lack of information flow between these two pillars of the military intelligence service. In order to tackle this issue, plans have been made for modifying the structure of the service. From this point of view, it is obvious that there is little sense in finalising this investigation now. The Standing Committee I will reconsider the issue of information management within the GISS after the implementation of the proposed reforms.

II.11.3. COMPLAINT OF A PRIVATE INDIVIDUAL ABOUT THE WAY IN WHICH STATE SECURITY HAS ALLEGEDLY OBTAINED, PROCESSED AND DISSEMINATED INTELLIGENCE ABOUT THE PERSON IN QUESTION

In the course of 2006, the Standing Committee I received a complaint from a citizen who alleged that he had been seriously prejudiced by the activities of State Security. The person in question believed himself to have been a victim of manipulation and fabricated information for several years now, all of which had resulted in destroying his reputation. The Standing Committee I has – based on its double objective (examination of legitimacy and efficiency) – made considerable efforts in searching for relevant information and documents. Indeed, it was far from easy to gain access to these documents, which over time were scattered across various administrative and judicial services and which were also to be found among private individuals and agencies.

This investigation was completed mid-2009 and will be discussed in the next Activity Report.

II.11.4. ESPIONAGE IN THE EUROPEAN JUSTUS LIPSIUS BUILDING

On 19 March 2003, the European Council revealed that, at the end of February 2003, its security services found apparatus in the Justus Lipsius building of the Council of the European Union in Brussels which made it possible to eavesdrop on various delegations, including those of Spain, Germany, France, Italy, the United Kingdom and Austria.

However, the Council was unable to find out who was responsible for the installation of the electronic apparatus connected to certain telephone lines. In

line with a series of countermeasures and a prior internal investigation, the Council approved the decision '*authorising the Deputy Secretary-General of the Council to lodge a complaint on its behalf against person or persons unknown with the Chief Public Prosecutor at the Brussels Court of Appeal with regard to the discovery of phone tapping devices in the Justus Lipsius building in Brussels. The complaint will be based on the relevant provisions of the Belgian Penal Code, in particular Article 314bis*' (free translation).

At the end of May 2006, it was decided to initiate an investigation '*into the manner in which the Belgian intelligence services (State Security and the GISS) intervened in response to a phone tapping case in the offices of the delegation of the European Council in Brussels*' (free translation). In view of the fact that State Security had been indicated as an expert for the relevant judicial inquiry, it felt that it could not respond to the questions of the Standing Committee I.

It was only in the autumn of 2008 that the Standing Committee I was given the right to inspect the judicial dossier. But it was not allowed to make any copies. Nevertheless, on the basis of the findings of the consultation, further investigative actions were taken. The report of this investigation will, of course, be partly dependent on the evolution of the judicial dossier: as long as this is pending, the investigation secrecy must be respected.

II.11.5. HARMFUL SECTARIAN ORGANISATIONS

State Security must pay attention to phenomena such as '*any individual or collective activity, developed at home or from abroad, which is related to espionage, interference, terrorism, extremism, proliferation, harmful sectarian organisations, criminal organisations (…)*' (free translation). Each of these is individually defined in Article 8 of the Intelligence Services Act. For example, the concept of 'harmful sectarian organisations' is defined as '*any group having or claiming to have a philosophical or religious purpose and whose organisation or practice involves harmful illegal activities, causes harm to individuals or society, or impairs human dignity*' (free translation).

In the beginning of January 2007, the Standing Committee I decided to initiate an investigation '*into the manner in which State Security carries out its legal assignment with regard to harmful sectarian organisations, as stipulated in Articles 7 and 8 of the Intelligence Services Act*' (free translation).

This investigation is intended to find an answer to the questions as to which organisations are monitored by State Security and how are they monitored. The criteria used by the intelligence service to determine whether to consider a sectarian movement as dangerous, and the analyses sent by State Security to the authorities and their purpose will also be examined. Finally, the Standing Committee I wants to gain an insight into the personal and material resources made available by State Security for this assignment.

In 2008, the investigative activities focused on State Security. The central departments 'Sects' of the foreign services and the analysis service as well as the local antennas of State Security, the so-called 'provincial posts', were also visited in this context.[79] The final report is normally expected in 2009.

II.11.6. THE MILITARY INTELLIGENCE SERVICE AND THE PERFORMANCE OF A SECURITY INVESTIGATION

In the beginning of May 2007, the Investigation Service I received a written complaint from a private individual, who expressed his dissatisfaction with the course of a security investigation by the military intelligence service. After a brief preliminary investigation, the Standing Committee I decided to initiate an investigation '*into the manner in which the GISS has initiated a security investigation*' (free translation).

In this context, the Investigation Service I took various additional investigative steps in 2008. The investigation will be concluded in 2009.

II.11.7. PROTECTION OF COMMUNICATION SYSTEMS AGAINST POSSIBLE FOREIGN INTERCEPTIONS

The issue of protecting information and telecommunication systems managed via new IT technologies, has regularly come up for discussion in the Federal Parliament. The security of these systems is essential in the evolution towards an information society. This is because the current interception possibilities form a possible threat not only for the security, military interests and economy of a country, but also for the fundamental rights and freedoms of citizens.

Indeed, there is a noticeable trend of foreign powers strengthening their phone tapping and interception capabilities. One only has to think of the American *Protect America Act* of 2007. But recently, cases have also emerged of alleged illegal phone tapping practices or improper intrusions into IT systems of companies or governments. For example, the Italian military intelligence service (the then SISMI) is supposed to have illegally intercepted electronic correspondence between the *Magistrats Européens pour la Démocratie et les Libertés (MEDEL)*, which also includes a number of Belgian magistrates. Attacks on computer systems of various (foreign) government institutions were also regularly reported.

Furthermore, the Monitoring Committee of the Senate expressed the desire to be kept informed by the Standing Committee I regarding the manner in which the intelligence services monitor these events and trends. It also wished to receive

[79] Also see Chapter III.2. regarding these provincial posts, STANDING COMMITTEE I, *Rapport d'activités 2008*, 82-83.

an *update* of the Echelon Report presented by the Standing Committee I in 2000.[80]

All these elements resulted in the Standing Committee I deciding at the end of December 2007 to initiate an investigation into '*the manner in which the Belgian intelligence services consider it necessary to protect the communication systems against foreign interception*' (free translation).

This investigation was started in 2008 and numerous investigative actions were undertaken. The Committee did not focus so much on the actual facts leading to the initiation of the investigation, but rather on the general issue of securing communication systems against possible foreign interceptions.

II.11.8. PROTECTION OF CLASSIFIED INFORMATION ON NON-SECURE SITES

In the middle of December 2007, the Standing Committee I decided to initiate an investigation into '*the manner in which the GISS protects classified information and/or personal data on non-secure sites*' (free translation) as a result of some incidents in which such data had been lost. In 2008, information was collected regarding this problem.

II.11.9. COMPLAINT IN RESPONSE TO THE NON-RECOGNITION OF A MOSQUE

In 2008, the Appeal Body for security clearances, certificates and advice was requested by a complainant to start an investigation because it appeared that a dossier for the recognition of a mosque had not been handled correctly. However, the Appeal Body was not competent for this matter and referred the complainant to the Standing Committee I which, in its turn, initiated an investigation into the role and advice of State Security on this recognition procedure. For this, State Security was questioned regarding the methods used. This investigation was completed in spring 2009.

II.11.10. THE BELLIRAJ CASE

At the end of February 2008, the Standing Committee I was assigned a task by the Minister of Justice and the Minister of Defence to initiate an investigation

80 See STANDING COMMITTEE I, *Rapport d'activités 2000*, 'Synthesis report of the investigation into the manner in which the Belgian intelligence services respond to the possible existence of an American system, named Echelon, for the interception of telecommunications in Belgium', 29-60.

into '*the manner in which the Belgian intelligence services had monitored the persons who were recently arrested in Morocco and who were apparently suspected there of forming a terrorist group*' (free translation). The Standing Committee I invested a considerable amount of time and resources in this investigation and delivered three interim reports in 2008.[81] The investigation was continued in 2009.

II.11.11. INFORMATION POSITION OF THE INTELLIGENCE SERVICES WITH REGARD TO A MEMBER OF A MOROCCAN TERRORIST NETWORK

In the middle of May 2008, the press agency *Maghreb Arabe Presse* (MAP) reported that the Moroccan police had arrested eleven terror suspects in Nador and Fez. It appeared that one of them was a Moroccan residing in Belgium. The network had allegedly planned attacks in Belgium and Morocco. They were reported to have links with the *Al Qaida pour le Maghreb Islamique* (AQMI) group.

Thereupon, the Standing Committee I decided to initiate an investigation into '*the manner in which the Belgian intelligence services had possibly monitored X, who was arrested in Morocco for planning terrorist attacks in Morocco and Belgium*' (free translation).

II.11.12. GATHERING AND PROCESSING INFORMATION ON PERSONS NOTICED IN THE NEIGHBOURHOOD OF MILITARY INSTALLATIONS

In the summer of 2008, another complaint by a private individual resulted in the initiation of an investigation into the reasons for and the manner in which the intelligence services have gathered and processed information on persons who had been noticed in the neighbourhood of military installations. The investigation will be completed in 2009.

II.11.13. COMPLAINT OF A PRIVATE INDIVIDUAL AGAINST AN OFFICER OF THE MILITARY INTELLIGENCE SERVICE

In July 2008, the Standing Committee I received a complaint from a private individual against a public prosecutor, the Federal Police, a governor and an

[81] For an overview of the results of the interim reports, see Chapter II.3, *Activity Report 2008*.

officer of the military intelligence service. The Committee stated that it was not competent with regard to the first three parties, but initiated an investigation '*into the complaint of a private individual against an officer of the GISS*'. The officer in question had allegedly carried out actions which had prevented the complainant from developing his commercial activities.

CHAPTER VIII
RECOMMENDATIONS

Based on the investigations concluded in 2008, the Standing Committee I has formulated the following recommendations. These relate in particular to the protection of the rights which the Constitution and the law confer on individuals (VIII.1), to the coordination and efficiency of the intelligence services, the CUTA and the supporting services (VIII.2) and finally, to the optimisation of the review capabilities of the Standing Committee I (VIII.3).

VIII.1. RECOMMENDATIONS WITH REGARD TO THE PROTECTION OF THOSE RIGHTS WHICH THE CONSTITUTION AND THE LAW CONFER ON INDIVIDUALS

VIII.1.1. LEGISLATION FOR SENDING PERSONAL DATA ABROAD

Further to the findings of the investigation into the so-called 'reserved dossiers'[82], the Standing Committee I reiterates its recommendation[83] for the need to develop a clear regulation for passing on personal data to foreign (intelligence) services. Inspiration for this can be found in the Dutch, German and Norwegian legislation.

For instance, the Dutch Act on Intelligence and Security Services (2002) explicitly defines the authority to share data with intelligence and security services of other countries and with international security and intelligence agencies. This also explicitly defines the third party rule and the conditions thereto. Moreover, there are special provisions for the external dissemination of less recent data or information whose accuracy cannot be determined. It is also worth mentioning that records must be maintained of the transfer of information.

In Germany, a similar regulation was developed in the *Bundesverfassungsschutzgesetz* (2002). For example, the *Bundesamt für Verfassungsschutz* (BfV)

82 See Chapter II.2.3.6, *Activity Report 2008*.
83 STANDING COMMITTEE I, *Activity Report 2006*, 60.

states that personal data may be provided to foreign, international and supranational authorities and agencies if this is required for the performance of their tasks or for the protection of essential security interests of the receiving authority or agency. The dissemination of data is stopped if this is in the interests of the German federal republic or the concerned persons. Records must be maintained of all information provided. The receiving authority or agency is informed that the data may only be used for the purpose for which it is provided. Finally, it is explicitly stated that the BfV may request information about the intended use of the data.

In Norway as well, a similar regulation can be found in the so-called Internal guidelines for the *handling of information*. Freely translated, *Section 4–1* stipulates the following: '*Information may be disclosed to cooperating foreign police authorities and security or intelligence services in order to avert or prevent criminal acts or if this is required for verifying information. However, such disclosures may take place only after an assessment of the proportionality between the purpose of the disclosure and its consequences for the individual*'. The Standing Committee I wishes to specifically emphasise that the Norwegian review body effectively verifies whether the applicable rules in this matter are being respected. For this, the monitored service is obliged to record any transfer of data to foreign authorities and the review body conducts random checks each year.[84]

VIII.1.2. GUIDELINES FOR HANDLING DATA REGARDING CERTAIN CATEGORIES OF PERSONS

Also in response to the investigation into the so-called 'reserved dossiers'[85], the Standing Committee I recommends that State Security must decide for each dossier whether it must be stored, destroyed or transferred to the State Archives. Naturally, the first option is only possible if the data is still meaningful in the light of the current legal assignments and possibilities of the service. However, before making a decision regarding these dossiers, their contents need to be checked for reliability and relevancy.

More generally speaking, the Standing Committee I wants State Security to develop clear and unambiguous guidelines with regard to the collection, processing, consultation (including the internal screening, if any), storage and archiving of data regarding certain categories of persons who have or had special responsibilities.[86]

---

84 THE NORWEGIAN PARLIAMENTARY INTELLIGENCE OVERSIGHT COMMITTEE (EOS Committee), *Annual report 2007, s.l.*, 17-18.

85 See Chapters II.2.3.1 and II.2.3.2, *Activity Report 2008*.

86 One must therefore determine whether former and present mandatories need to be treated in the same way.

For the development of these guidelines and the actual monitoring of (former) political representatives, State Security must take into consideration the guidelines outlined in the judgement of the European Court for Human Rights in the case *Segerstedt-Wiberg and Others v. Sweden*.

VIII.1.3. IMPLEMENTATION DECREE ON THE DESTRUCTION OR ARCHIVING OF DOSSIERS

Within the framework of the investigation into the 'reserved dossiers', the Standing Committee I insists that urgent action needs to be taken with regard to the Royal Decree implementing Article 21 of the Intelligence Services Act, which states that personal data may be destroyed or archived.

VIII.1.4. POSSIBILITY OF EXTERNAL RECTIFICATION OF THE CLASSIFICATION BY INTELLIGENCE SERVICES

The Standing Committee I has recommended earlier that a system should be designed in which the classification made by our intelligence services can be rectified if it does not comply with the legal provisions.[87]

The Committee made the recommendation based on the need to submit meaningful reports to the Monitoring Committee. If a classification appears to be unjustified, this does not prevent the data from being inspected by the Committee, but it does hinder the editing of a conclusive report for the benefit of the Monitoring Committee. Under the current legislation, one can only make an informal *appeal* to the sense of responsibility of the agency that classified the information.

But the Committee also arrives at this recommendation based on a concern for the rights of the citizen. Since, the system by which the possibilities of the Classification Act were used in 2000 to obstruct the right to inspect administrative documents[88] reinforces the conviction of the Standing Committee I that an external rectification of the classification by intelligence services must be possible.

87 STANDING COMMITTEE I, *Activity Report 2006*, 65.
88 See Chapter II.2.3.3, *Activity Report 2008*.

VIII.1.5. A LEGAL REGULATION FOR SCREENING (POTENTIAL) INFORMANTS

The fact that it is necessary to *screen* informants, both prior to their recruitment as well as during their 'activities', is obvious.[89] In order to assess the relevance and reliability of the information to be supplied or already supplied, the intelligence services must have as accurate an image as possible of the concerned person. Nevertheless, these actions are indisputably a violation of privacy under the meaning of Article 8 of the ECHR and Article 22 of the Constitution. A legal basis defining the boundaries of such controls should therefore be provided. This regulation should be part of a broader legal regulation for informant operations as recommended by the Standing Committee I in its advice on the SIM Bill.[90]

VIII.2. RECOMMENDATIONS CONCERNING THE COORDINATION AND EFFICIENCY OF THE INTELLIGENCE SERVICES, THE CUTA AND THE SUPPORTING SERVICES

III.2.1. SCOPE OF THE EMBARGO PROCEDURE FOR THE ANALYSIS WORK OF THE CUTA

As was evident from the investigation into the terror alarm[91], the application of the embargo procedure specified in Articles 11 and 12 of the Threat Assessment Act results in the Director of the CUTA becoming solely responsible for the assessment of a threat. To do this, neither can he enlist the help of analysts specially recruited for this purpose nor – based on a literal reading of the law[92] – can he appeal to the Deputy Director for help. This obviously implies a risk of inefficiency, because the analysis work must be done by one person who is not necessarily specialised in this field. This argument becomes even more compelling in the light of the fact that any data supplied 'under embargo' will usually concern matters of the highest importance.

89 See Chapter II.5, *Activity Report 2008*.
90 STANDING COMMITTEE I, *Rapport d'activités 2006*, 75.
91 See Chapter II.1.3.4, *Activity Report 2008*.
92 According to the Director-General of State Security, the text of the Act must be interpreted literally and the Director is intended as *intuitu personae* and not his Deputy. However, the Director and his Deputy rightly believe that such a reading of the Act creates serious problems in practice. Assuming that the embargo procedure continues for a long time or that there are several ongoing embargos, then it is simply impossible to expect that these will be managed exclusively and personally by the Director, because this would mean that he must be permanently available.

That is why the Standing Committee I is an advocate of a system in which *all* relevant intelligence is always communicated to the CUTA and the Director decides which staff members (all of whom have a 'TOP SECRET' security clearance and are bound by their individual duty of professional secrecy) will be involved in the analysis. After the actual analysis activities, the Director and the Federal Prosecutor or the head of the concerned supporting service jointly decide what information is included in the assessment document and in what wording, and the authorities to which this assessment is communicated. If necessary, all authorities receive the same information. This system ensures the complete protection of sensitive data, without losing the added value offered by the CUTA.

Furthermore, the Standing Committee I believes that if one continues to uphold the interpretation that the information supplied under embargo may not be communicated to the Deputy Director, then it also becomes essential to amend the law such that the Deputy Director becomes a fully-fledged replacement for the Director. At any rate, this also seems to have been the intention of the legislator.

VIII.2.2. PROCEDURE IN CASE OF A DIFFERENCE IN OPINION REGARDING THE USE AND DISSEMINATION OF INFORMATION SUPPLIED UNDER ENBARGO

The Threat Assessment Act of 10 July 2006 does not offer any solution for the situation in which, on the one hand, the Federal Prosecutor or the head of the service supplying the information, and on the other hand, the Director of the CUTA cannot reach an agreement about whether certain intelligence may or may not be included in the assessment or regarding the authorities to whom the assessment must be sent. During the preparatory activities, it was proposed that in case of a difference of opinion, '*the conflict of interests will be referred to the competent ministers, who will then take the final decision*'.[93] Although there was no question of such a difference of opinion during the investigation into the terror threat around the turn of year, it would still be advisable to include this regulation, in so many words, in the Act to prevent any future problems.

VIII.2.3. CONTROL OF THE APPLICATION OF THE EMBARGO PROCEDURE

It is recommended that the decisions taken pursuant to Article 11 or 12 of the Threat Assessment Act, regarding whether or not to include certain intelligence

93 *Print.*, House of Representatives, 2005-2006, 2032/1, 24.

in a threat assessment and for determining who is to be informed of this, be formalised in a written document. Since this involves joint decisions taken by the Director of the CUTA and the Federal Prosecutor or the head of the supporting service that supplies the information, these fall under the review competence of the Standing Committee P and the Standing Committee I. A written document encourages greater accountability, while enabling the Committee to supervise the legitimacy of these decisions at all times.

VIII.2.4. A SECURE COMMUNICATION NETWORK

The Standing Committee once again[94] emphasises its earlier recommendation that it is absolutely and urgently necessary to develop a secure communication network between the CUTA, the supporting services and the threat assessment addressees. This necessity was again made apparent further to the investigation into the terror alarm around the turn of the year.[95]

VIII.2.5. IDENTIFYING UNRELIABLE INFORMANTS

The recruitment by an intelligence service of an informant expelled by a sister service runs the risk of being a wastage of time and resources.[96] Therefore, the two intelligence services should consider implementing a system that allows them to inform one another of the identity of informants with whom the cooperation was stopped on the initiative of one of the services. The principle and terms of such an agreement could be formalised in a protocol agreement.

VIII.2.6. ROLE OF THE INTELLIGENCE SERVICES IN CERTAIN FOREIGN INVESTMENTS

The Standing Committee I believes – as does State Security[97] – that it is desirable to establish a legal regulation for the control and review of foreign investments and commercial activities in sectors regarded as important for Belgium from a strategic and military point of view. For this it would be advisable to define, following the French example, the possible role of the intelligence services.

The Standing Committee I also believes that the potential military importance of a company established in Belgium merits the preventive attention of the GISS if the company in question is transferred to foreign hands.

---

94 See STANDING COMMITTEE I, *Activity Report 2007*, 114.
95 See Chapter II.1.3.11, *Activity Report 2008*.
96 See Chapter II.5, *Activity Report 2008*.
97 See Chapter II.6.1.4, *Activity Report 2008*.

VIII.2.7. A LEGAL DEFINITION OF THE ASSIGNMENT OF THE GISS WITHIN THE FRAMEWORK OF THE FIGHT AGAINST PROLIFERATION

The Standing Committee I recommends that – following the example of the description of the assignments of State Security – the assignment of the military intelligence service within the framework of the fight against proliferation should also be clearly and explicitly included in the Intelligence Services Act. In addition, the Committee advises the Ministerial Committee for Intelligence and Security to define in detail, pursuant to this same Act, how the GISS must perform this assignment.

VIII.2.8. COOPERATION BETWEEN STATE SECURITY AND OTHER AUTHORITIES IN THE FIGHT AGAINST PROLIFERATION

The Standing Committee I agrees with State Security that the latter must also be one of the authorities which is officially authorised with respect to the export of goods.[98] State Security had planned to conclude cooperation agreements with the FPS Economic Affairs, with Customs and with the Regions with a view to achieving a better exchange of information. As yet, no agreement has been signed. The Standing Committee I recommends that such cooperation agreements be concluded with the other partners and urges that provisions resulting from such agreements be effectively complied with.

VIII.2.9. SECURITY INVESTIGATIONS OR VERIFICATIONS OF PERSONNEL OF CERTAIN COMPANIES OR INSTITUTIONS

Unless it concerns a classified investigation programme, at present not a single security investigation is being carried out with regard to the personnel of companies or institutions which deal with chemical, radiological or biological substances which can be used for the development of CBRN weapons.[99] The Standing Committee I is of the opinion that it would be opportune to subject these persons to a security investigation or verification.

---

98 See Chapter II.4.1.4, *Activity Report 2008*.
99 See Chapter II.4.2.4, *Activity Report 2008*.

VIII.2.10. SUFFICIENT RESOURCES IN THE FIGHT AGAINST PROLIFERATION

The Standing Committee I recommends to provide State Security and the GISS with sufficient human and material resources so that they can cope with the assignments in the fight against the proliferation of non-conventional or advanced weapon systems. The Standing Committee I expects the services to devote the required attention to this phenomenon and to deploy the necessary resources for this purpose.

VIII.2.11. ADEQUATE ANALYTICAL CAPABILITY

Both with regard to the investigation into the role of the intelligence services within the framework of the fight against proliferation[100] as well as the investigation into the manner in which the GISS has monitored the election campaign in Congo[101], the Standing Committee I was able to conclude that the analyses conducted by the GISS were of the highest quality. However, in order to maintain this level of quality, the service must have access to an adequate number of qualified staff in the analysis department. Otherwise, an essential link in the so-called 'information cycle' is weakened.

VIII.3. RECOMMENDATIONS CONCERNING THE EFFECTIVENESS OF THE REVIEW

VIII.3.1. REVIEW OR EXMINATION OF THE CASES IN WHICH THE INVESTIGATION SECRECY IS INVOKED

When the staff of the CUTA or the police or intelligence services invoke the investigation secrecy to avoid communicating certain intelligence, the Standing Committee P and the Standing Committee I do not have any way of reviewing or examining the legitimacy and expediency of this claim.[102] But the Committees believe that there may be cases where one cannot justify the undisputed acceptance of the invoked investigation secrecy. In concrete terms, one can think of situations in which one suspects or has the impression that the investigation secrecy is used outside its intended purpose (namely, guaranteeing the privacy of suspects and/or preventing that the criminal proceedings are jeopardised) or in

100 See Chapter II.4, *Activity Report 2008*.
101 See Chapter II.7, *Activity Report 2008*.
102 See Chapter II.1.3.1, *Activity Report 2008*.

which a delayed disclosure – only at the end of the investigation – of the relevant information would make the parliamentary review completely impossible.

In this context, the Standing Committee I refers to the already existing *overruling* system referred to in Articles 24, § 2, third paragraph, and 48, § 2, third paragraph of the Review Act, where the Chairperson(s) of the Committee(s) assesses (assess) the possibility of disclosing a secret invoked for the protection of the physical integrity of a person.

It was emphasised that breaking the investigation secrecy with respect to the Committees does not imply that the criminal proceedings may or will be jeopardised. This is because the members of the Committees are also privy to this secret. As long as the investigation secrecy is in effect, the Committees are obliged to take this into account in their reports to the parliamentary Monitoring Committee and to the public at large.

If this line of thought is not considered, then the possibility of invoking the investigation secrecy should at least be restricted to the judicial authority. Even though this would mean that the earlier mentioned reporting issue still remains, this would at least prevent every member of a police or intelligence service or the CUTA from being able to invoke this secrecy principle.

VIII.3.2. DIRECTIVES OF THE MINISTERIAL COMMITTEE FOR INTELLIGENCE AND SECURITY

Within the framework of the investigation into the 'protection of the scientific and economic potential and the Belgian aerospace industry'[103], the Standing Committee I was again confronted with the fact that it could not avail of the necessary information to be able to carry out its task completely. This is because the Committee was never informed of the action plan for safeguarding the SEP issued by the Ministerial Committee for Intelligence and Security. In this context, the Standing Committee I refers to the pending parliamentary initiative for defining a clear regulation in this matter and to the investigation of the Prime Minister further to the official request of the Committee.[104]

103 See Chapter II.6, *Activity Report 2008*.
104 See Chapter I.2, *Rapport d'activités 2008*, 4.

ACTIVITY REPORT 2009

TABLE OF CONTENTS OF THE COMPLETE ACTIVITY REPORT 2009

PREFACE

The Coalition Agreement of March 2008 stated that "*our country will step up the fight against international terrorism. (…) This means that (…) a legal framework must be adopted for the special methods for receiving and exchanging information from the intelligence and security services, with respect for fundamental rights and freedoms. Because the proper operation of the intelligence services is essential in this regard, the government will examine, based on an audit, whether the operation can be improved and if so, how this must be done*" (free translation).

The Standing Committee I was very closely involved with these objectives from the Coalition Agreement. It was entrusted with carrying out the audit and formulating various advisory opinions on the draft texts which ultimately resulted in the Act of 4 February 2010 governing the methods for collecting information by the intelligence and security services (Special Intelligence Methods Act). These two assignments have therefore determined, to a considerable extent, the course of the operating year 2009.

Especially the first assignment – which had already been started in the autumn of 2008 – implied a large investment of people and resources in 2009. This performance audit was aimed at investigating and assessing 'how' State Security carries out its activities based on the criteria of efficiency and effectiveness. Here the Standing Committee I was confronted with an intelligence service that found itself at a turning point: the 'Strategic Plan 2008–2012' had been implemented and new statutes introduced, the information management process had been redesigned and contemporary management principles were steadily making their entry. These initiatives can only be applauded. The Standing Committee I is convinced that an organisation and management compliant with the management standards of an efficient and effective government service would not only benefit State Security, but the General Intelligence and Security Service and the Coordination Unit for Threat Assessment as well. The final report was sent in mid-2009 to the two principals (the Minister of Justice and the Senate Committee entrusted with monitoring the Standing Committee I).

In 2009 the Standing Committee I also intensively studied the special intelligence methods. In its recommendations, the Committee had been insisting, for several years now, on the urgent necessity of granting additional powers to the intelligence services by creating a clear legal basis with a specific focus on the protection of the rights and freedoms of citizens. In the build-up to such a

legislative framework, the Standing Committee I could perform its statutory advisory role to the fullest extent. Since, Article 33 of the Review Act states that "*the Standing Committee I may advise on a Bill, Royal Decree, Circular Letter, or any other document expressing the lines of policy adopted by the competent ministers, at the request of the House of Representatives, the Senate, or the competent minister*" (free translation). As early as in 2006, the then Ministers of Justice and Defence requested the Standing Committee I for advice on the draft Act governing the methods for the collection of information by intelligence and security services. In fact, the advice of the Standing Committee I was sought in this regard up to three times in 2009: by the Chairman of the Justice Committee of the Senate in January 2009, by the Minister of Justice in September 2009 and finally by the Chairman of the Justice Committee of the House of Representatives in November. Just as in its advice of 2006, the Standing Committee I once again drew its inspiration from the preamble of Recommendation 1713 (2005) of the Parliamentary Assembly of the Council of Europe: "*The need for security often leads governments to adopt exceptional measures. These must be truly exceptional as no state has the right to disregard the principle of the rule of law, even in extreme situations. At all events, there must be statutory guarantees preventing any misuse of exceptional measures.*" The Standing Committee I is pleased to find that its detailed advice has weighed in the decision-making process, even though not all its suggestions have been taken into consideration.

This conclusion, combined with the fact that the legislative and executive powers have also paid heed to innumerable other recommendations, mean that the Standing Committee I can look back with satisfaction on a successful operating year.

Guy Rapaille,
Chairman of the Standing Intelligence Agencies
Review Committee

1 June 2010

CHAPTER II
INVESTIGATIONS

In 2009 the Standing Committee I received fifteen complaints from private individuals. Four of those resulted in the initiation of three investigations (two of the complaints led to one common investigation). Ten complaints were not acted upon because either they appeared to be – following the verification of a number of details – manifestly unfounded (Art. 34 of the Review Act) or because the Committee was not competent for the matter in question. In the latter case, the complainants were referred to the competent authority where possible.

In addition to the three investigations on the basis of complaints, the Standing Committee I also initiated six other investigations: four on its own initiative and two at the request of the chairman of the Senate. Three of these investigations – regarding an aspect of the operation of the Coordination Unit for Threat Assessment (CUTA) – were initiated and carried out jointly with the Standing Committee P in accordance with the Review Act of 18 July 1991.

Nine investigations were also completed in 2009. In addition, investigative steps were taken in several other cases. This chapter will first discuss the completed investigations (II.1 to II.9). Then follows a summary and brief description of the investigations in which important investigative steps were taken in the course of the operating year 2009 but which could not be completed as yet, as well as of the investigations initiated in 2009 (II.10).

II.1. A PERFORMANCE AUDIT OF STATE SECURITY

II.1.1. THE ASSIGNMENT

The Coalition Agreement[105] of March 2008 stated that "*our country will step up the fight against international terrorism. It guarantees the proper operation of the Coordination Unit for Threat Assessment (CUTA) and a dissemination of the information to the judicial authorities to monitor, together with the Parliament, the proper exchange of information between the various services. The review activities must be structurally organised. This means that the legislation on special investigative methods must be urgently amended and a legal framework must be*

105 *Print,* House of Representatives, 2007–2008, 20/2, 42–43.

adopted for the special methods for receiving and exchanging information from the intelligence and security services, with respect for fundamental rights and freedoms. Because the proper operation of the intelligence services is essential in this regard, the government will examine, based on an audit, whether the operation can be improved and if so, how this must be done" (free translation).

The latter intention – i.e. examining, based on an audit, whether and how the operation of the intelligence services can be improved – was confirmed and reiterated in the general memorandum of the Minister of Justice[106], manifestly only with respect to State Security, which falls under his scope of competence.

Following the meeting at the end of May 2008 of the Senate committee entrusted with monitoring the Standing Intelligence Agencies Review Committee, the Minister of Justice decided to request the Standing Committee I to carry out the audit. The Senate committee supported this assignment and thus became the co-principal. In September 2008, the Committee started the performance audit with the aim of "*investigating and assessing 'how' State Security carries out its activities based on the criteria of efficiency and effectiveness*".[107]

II.1.2. THE FOUR KEY THEMES

The Minister of Justice then formulated a number of very precise questions, which were subsequently grouped into four themes by the Standing Committee I.

Firstly, the leadership aspect was given special attention. The following questions were considered: How is State Security managed, especially in terms of its policy objectives? Does the management take into consideration the specific competence levels of its staff? What is being done, from the perspective of competence management, to continually optimise staff management? How does the institution apply a strategic staff policy in order to pursue the realisation of organisational goals?

Subsequently, the information management process of State Security was discussed and the following aspects were dealt with: How are the principles of availability, accessibility and permanence of information and staff guaranteed? What can be said about the speed and flexibility of the information and the staff? For example, how is the work schedule structured to provide quick, efficient and continuous services?

Thirdly, the work processes were examined: Is the information flow and processing managed efficiently? Are these work processes outlined and optimised on the basis of a clear vision?

---

106 *Print,* House of Representatives, 2007–2008, 995/3, 27–28.

107 *Ditto.*

Finally, a number of quality satisfaction aspects were discussed: Are there systems in place to measure the satisfaction of customers and staff with regard to the input and output of information? Are the Belgian customers of State Security (e.g. political, police and judicial authorities) satisfied? Which elements could be provided to monitor this better? Is State Security itself satisfied with the information received by its domestic and foreign customers?

II.1.3. THE METHODOLOGY APPLIED

II.1.3.1. Framework of standards

The audit was based – as is customary for a performance audit – on standards[108] for the effective and efficient functioning of an organisation, *in casu* State Security as a public service. The focus was on management level (i.e. the organisation in the narrow sense) rather than on policy level (the policy framework within which State Security operates). As far as 'management' is concerned, the Standing Committee I expected State Security to take the correct measures so as to be reasonably sure of realising its objectives. With regard to 'performance', it could be expected that there is a level of quality consciousness at State Security and that the stakeholders – both internally within State Security as well as outside of it – are satisfied with the quality of the services provided. The Standing Committee I chose to investigate whether the general conditions for management and control of the organisation were met, as well as to verify the extent of satisfaction with the services provided.

In order to reach a judgement ('good', 'poor'…) by comparing a fact ('what is') with a standard ('what should be'), one usually makes use of 'frameworks'. However, a specific framework with a theoretical basis of how a (Belgian) intelligence service must be managed in order to guarantee efficiency, effectiveness and quality of operations, does not exist (yet). That is why, when starting the investigation, the Standing Committee I decided to use the

---

[108] Standards can be classified into various groups:
- Standards related to operation (of the government): these standards are further subdivided into standards with regard to *management* (what takes place inside an organisation: primary, supporting and management activities) and *policy* (regulations, budget, policy objectives…). For *management*, the focus is on public managers, for *policy* the focus is on politicians;
- Standards related to government policy results: these standards are further subdivided into standards related to performance (*output*) and effects (*outcome* or achievement of objectives);
- Standards related to the responsibility of ministers to Parliament.

See in this regard: V. PUT, *Met welke bril kijken auditors naar de werkelijkheid?,* Die Keure, Bruges, 2006, 14.

CAF model[109] as a framework. The model had already been used by State Security in 2003 in order to identify and remedy bottlenecks in the operation of the field services. The CAF model allowed the Committee to identify factors to be included in the investigation and to draw up questionnaires for interviewing the personnel. Another framework also included as a frame of reference in the course of the investigation, is the '*Leidraad Interne Controle en Organisatiebeheersing*' (Guideline for Internal Control and Organisational Control) used within the Flemish government. The guideline appeared to be useful for collecting information and drawing conclusions since here the emphasis lies on 'management control'. In this guideline, the organisational preconditions are worked out in more detail than in the CAF model. The guideline also combines the themes of the COSO and ERM model[110] and the principles of sound public governance. These frameworks provide the theoretical basis for an efficient, effective, high-quality and ethical management (control).

In addition, the existing situation was also assessed according to various Belgian legal standards related to the management, assignments, powers, performance… of State Security.

The Committee decided to follow an approach based on a business and human perspective. This means that State Security was not only considered a rational, goal-oriented organisation (with a focus on planning and control, organisational structure, procedures…), but that the human dimension was also taken into account (culture, communication, involvement of personnel…). At the same time, the approach was both substantive and systematic in nature. In other words, the Committee considered not only the performance and whether there was satisfaction with the services provided, but also whether there were any systematic failures which could possibly lead to dysfunctions.

II.1.3.2. Methodology

The performance audit was prepared and carried out with maximum compliance with the *Standards and guidelines for performance auditing based on INTOSAI's Auditing Standards and practical experience*.[111] The audit consisted of the following steps:

---

109 The *Common Assessment Framework (CAF)* is a quality management tool specifically developed for organisations in the public sector, which is provided to public administrations in the European Union as an aid to understanding and using quality management techniques. The main purpose of the CAF is to provide public institutions with a simple, user-friendly structure for self-assessment.

110 The *Committee of Sponsoring Organizations of the Treadway Commission (COSO)* is a management model aimed at providing organisations with a uniform and common frame of reference for internal control and assisting the management in improving the internal control system. *Enterprise Risk Management* (ERM or COSO II) is an extension of the COSO internal control framework.

111 See www.intosai.org.

- development of tools for collecting information (questionnaires, interview plans…);
- actual collection of information and verification of the correctness and completeness of the same;
- analysis of information, whether quantitative or qualitative;
- comparison of the gathered facts with the standards in order to arrive at an assessment;
- drawing up of a draft report and sending this to the auditee;[112]
- modification of the draft report based on the substantiated remarks of the auditee;
- formulation of recommendations.

It was decided to use a combination (methodical triangulation) of various investigative methods, with a focus on formally structured written questionnaires. The collection and analysis of information was done on the basis of exhaustive desk research, a systematic inquiry – both written (with a questionnaire) and verbal (face-to-face interviews, focus groups, interviews with external stakeholders…) – and onsite verification. The results of the written questionnaire – in which almost all managerial and non-managerial staff of State Security were interviewed – were described as being representative in accordance with the prevalent methodology (response rate of managerial staff 84%, response rate of non-managerial staff 47%).

The inquiry was concluded at the end of April 2009. All the stated information dates from before this date, which means that any changes introduced or documented in the intervening period, i.e. between this date and the time of publication or release of the audit report, could not always be taken into consideration.[113]

The Standing Committee I has invested a particularly large amount of time and human resources in this investigation. An extensive investigation team was set up, in which members of the Committee, its Investigation Service and the administrative executives worked together closely. During this period, various staff members were almost exclusively entrusted with the task of carrying out the audit.

---

112 State Security seized this opportunity to report a number of external factors (limited autonomy, recruitment problems, shortage of personnel) which might have an effect on the results of this audit. The aforementioned external factors were, however, outside the scope of this audit.

113 An audit is a feedback mechanism and is concerned with the past, it occurs *ex-post*: auditing is inherently retrospective. Therefore, the assessment of the proposed policy (estimating the potential effectiveness, feasibility etc. of the policy that has not yet come into existence) is not an audit (V. PUT, *o.c.*, 2006, 26).

II.1.4. PERFORMANCE AUDIT

As mentioned above, four key themes were addressed: leadership, information management, work processes and finally, satisfaction with quality. The main investigation results are outlined below.[114]

II.1.4.1. Leadership

Firstly, the Committee tried to identify the manner of leadership at State Security. The definition of leadership was adopted from the CAF model 2006: "*Leadership is the way in which leaders contribute to the development and achievement of the mission and vision of the organisation. It shows how they develop values for long-term success and implement those via targeted actions and behaviours. It indicates how leaders are personally involved in the development, implementation and evaluation of the management system and shows how organisations are continuously focused on change and innovation. Managers take on leadership positions depending on their level of responsibility.*"

In the context of the 'leadership' theme, particular attention was paid to various forms of management (strategic, risk, cultural and communication management) as well as to the organisational structure. At the request of the Minister of Justice, the Committee also tried to provide an answer to questions such as "*Does the management take into account the specific skill levels of its employees?*", "*How does the management try, from a competency management perspective, to continually optimise the leadership of its staff?*", or even "*How is the strategic personnel policy implemented in order to achieve the organisational objectives?*".

II.1.4.1.1. Strategic management

The audit showed that State Security applied the principles of strategic management[115] without sufficiently embedding them in its management processes. This could be seen in the strategy formulation, strategy implementation as well as the strategy evaluation phases.

It was concluded that *strategy formulation* did not take place on time and in a sufficiently structured manner. The following elements supported this conclusion:

---

114 In July 2009, the principals received a non-classified report (Part I, 40 p.) and a 'Confidential (Act 11/12/1998)' classified report (Part II, 189 p.).

115 Strategic management is the process by which the company's top management ensures the long-term adjustment of the company to its environment by means of (1) a suitable strategic analysis, (2) an appropriate strategy formulation, (3) the appropriate implementation of the strategy and finally (4) a continuous evaluation of its operation.

- the management defined its mission, vision and long-term and short-term objectives in the classified 'Strategic Plan 2008–2012';
- it was only in May 2009, at the time of the formulation of the operational plan, that the stakeholders within the organisation were informed of the concrete plans, intentions, objectives and goals which the management of State Security wanted to achieve in the short term (January-December 2009). This delay was caused by the late drafting and approval of the 'Strategic Plan 2008–2012', which had been planned for the beginning of 2008 but was only finalised in October 2008;
- State Security failed to draw up the action plan for 2008. For 2009, no formal action plan – within the meaning of Article 3 of the Royal Decree of 5 December 2006 on the general management and Support Cell of State Security (Royal Decree on State Security) – was submitted. State Security did, however, have the most important elements for developing such an action plan (i.e. strategic objectives, a staffing plan, an estimate of the budgetary requirements, general rules for the functioning of the organisation and the proper functioning of the services), which meant that the service complied with the spirit of this provision. Only the evaluation of the Support Cell was missing for the time being;
- during the formulation of the strategy, the management did not take the implementation requirements sufficiently into account. Some objectives did not always satisfy one or more SMART criteria;[116]
- the management of State Security felt that the formulation of inspiring and ambitious objectives was not a futile exercise, even if the service did not have the resources available to realise the objectives set;[117]
- as regards the factors necessary for the effective realisation of the planned objectives, the management of State Security was mainly concerned about the availability of the necessary budgets and less about the availability of support for these objectives within the organisation;
- the management committee complied with the regulatory requirements regarding the frequency of its meetings and asked the Support Cell for advice on every specific issue related to the matters referred to in Article 3 of the Royal Decree on State Security which involved their competencies. The management committee appealed to the expertise of the members of the Support Cell for drawing up the strategic and operational plans. The members of the Support Cell could consult all relevant documents, had access to the

116 Specific (the objective must be unambiguous), Measurable (the measurable, observable conditions or form under/in which the objective is achieved), Acceptable (will the target group and/or management accept this objective?), Realistic (the objective must be feasible) and Time-bound (by when must the objective be achieved).

117 The Standing Committee I did not share this view. See also M. HEIDE, K. GRONHAUG, and S. JOHANNESSEN, "Exploring barriers to the successful implementation of a formulated strategy", *Scandinavian Journal of Management*, 2000, 18 (2): 217–231.

databases of the organisation and could rely on the expertise of other staff members. In addition, they were given the necessary assistance with respect to administration, equipment and staffing;
- shortly after their appointment in May 2007, the members of the Support Cell were assigned the task of drawing up a strategic plan. The Standing Committee I could establish that the management had assigned the members of the Support Cell a broader role in the process of strategy formulation than the task assigned to them by the Royal Decree on State Security. They were each entrusted with the actual drafting of a (partial) draft of the strategic plan, whereas their contribution, according to Article 6 of the above-mentioned Royal Decree, is to give collegial advice. The Royal Decree explicitly states that the strategic plan must be prepared by the management committee;
- the Support Cell was inadequate guided by the management. The actual cooperative processes between the Support Cell and the management were not defined and proceeded in an informal and unstructured manner. The Standing Committee I remarked that the experts, despite their professional experience, had little or no actual experience with the functioning of an intelligence service. This, however, was not applicable to the (then) management expert – the primary partner of the management in this matter – since this expert, based on his competency, had been working together closely with State Security for a number of years;
- the Standing Committee I felt that the delay in realising the 'Strategic Plan 2008–2012' was due to the chosen method;
- neither the methodological basis of the strategic plan nor the preliminary analysis were sufficiently structured or centrally documented;
- as regards the involvement of the personnel in realising the strategic plan, the Standing Committee I found that only half the respondents among the managers admitted to having been consulted in this regard.

As regards the strategy implementation, it was concluded that this had not occurred in a timely fashion. For example, in April 2009 the 2009 operational objectives were yet to be translated into the various organisational units. Also, no objectives had yet been defined for the Director of Operations and the Director of Analysis. Neither had the objectives for the Department Commissioners responsible for a special unit been aligned to the strategic plan. There was only one general communication initiative to inform the internal stakeholders about the strategic plan and the strategic and operational objectives of the organisation. Despite the remarks of the CAF 2003, the traditional channel of communication, i.e. internal mail, was still being used for this. There was no process of awareness-raising and the strategic plan was not made available in the two national languages. This limited communication on the strategic plan did

not promote awareness of the objectives among the personnel. At the time of the interviews with the managerial staff, it appeared that one out of five were insufficiently aware or even completely unaware of the operational objectives.

The audit also revealed that the *strategy evaluation* process had not yet been developed. There was no general measurement and monitoring system that enabled State Security to efficiently monitor all the objectives in the 'Strategic Plan 2008–2012'. However, the management committee supported the principle of a measurement and monitoring system and had decided to implement a Balanced ScoreCard (BSC)[118] in 2009. The preparations hereto were underway. For monitoring the objectives of the strategic plan, the management mainly relied on the information provided by the managers and the middle management. The reporting happened informally, either at the weekly meeting at the management committee level or in the daily contacts between the managers and their staff.

II.1.4.1.2. Risk management

The Standing Committee I could establish that various methods were being applied within State Security for identifying, evaluating and managing risks. But the risk identification process was too fragmented, with too narrow an interpretation of the term 'risk'. It could also be established that the responsibility for risk management was spread over a number of positions within the organisation. Moreover, it appeared that though identified risks were assessed and reported in order to take the necessary risk management measures, sometimes the follow-up and the implementation of remedial decisions were lacking. According to State Security, this was due to a lack of time and human resources.

II.1.4.1.3. Cultural management

State Security did not have a sharp enough focus on the dissemination of values and norms in the organisation. The initiatives taken by management were not sufficiently in-depth to guarantee a general positive work climate. During the audit phase, it could also be established that:
- there has been a charter for personnel for several years;
- the effective implementation of the code of ethics was forthcoming;
- there were no guidelines for the attitude and behaviour of leaders, managers and employees with regard to teamwork and leadership;
- there was no evidence as yet of a general positive work climate within the organisation. From the contacts between the Standing Committee I and

[118] Balanced ScoreCard is a system for measuring the performance of the organisation (or organisational units) and for verifying the extent to which the defined objectives were achieved.

various staff members, it appeared that some staff members felt that vision, leadership, communication (including feedback) and personnel management are absent or at least severely inadequate, which is translated into a lack of confidence in the management committee. The management committee claimed that two initiatives taken in June 2008 with a view to improving coordination[119] would indirectly promote a positive work climate. Since these initiatives had culminated in measures only in April 2009, it was too early to judge whether they had created the desired effects on the work climate. However, the Standing Committee I was of the opinion that the initiatives were too insubstantial to act as a significant incentive. Similar conclusions were noted during the interviews with the focus groups. No evidence was found of initiatives to defuse the specific relational issues between the management of the assessment services and the employees. In the context of the 'Strategic Plan 2008–2012', the management announced that it would develop a special statute for members of internal services, similar to that of the field services. This would – according to the management – lead to an improved work climate.

II.1.4.1.4. Organisational structure

The audit revealed that the organisational structure and the approach to projects could be further improved. State Security management had made efforts to optimise the coordination mechanisms, but its handling of the compartmentalisation between the internal services and the field services was still inadequate. The Standing Committee I also established the following:

- an organisation chart of the entire organisation and the various sub-entities – except temporary (although sometimes practically permanent) work forms – existed and was to be communicated more actively to all staff members via a business application;
- the organisational structure was revised at regular intervals with a view to its optimisation;
- however, the management did not sufficiently sound out its personnel regarding whether it was necessary to actually modify the organisational structure;
- the levels, positions, responsibilities and powers were defined;
- however, no job descriptions had been drawn up as yet for the Department Commissioners responsible for a special unit;
- the inquiry among personnel showed that they were sometimes insufficiently aware of their tasks, powers and responsibilities;

[119] On the one hand, the initiative for improving the coordination between the internal and field services; on the other hand, the coordination between the field services and the provincial posts.

- the tasks actually performed by the managers were – as it appeared from the sample – consistent with the tasks listed in the job descriptions;
- steps had been taken towards improving the coordination mechanisms, but in view of the existing structure, in which the assessment services and the field services operate in a compartmentalised manner, the Standing Committee I had to conclude that the required coordination mechanisms were still not adequately implemented. The Committee was of the opinion that the two initiatives for improvement[120] urgently needed to be developed further;
- various projects had been set up within State Security, but not always according to a well-founded project management methodology.

II.1.4.1.5. Communication management

The communication management process was also closely examined. This showed that the management of communication flows within State Security could be improved. Useful initiatives had been taken (State Security had outlined its vision on internal communication in the 'Strategic Plan 2008–2012', a communication cell was set up, a person had been made responsible for communication and his tasks and responsibilities were clearly described, the operational objectives with regard to external communication had been defined…), but a number of areas for improvement were also noted. For example, there was no formal communication plan. Also, according to a large section of personnel, the communication of the supervisors with the personnel – regarding change initiatives within State Security – was still inadequate. For the communication with the internal stakeholders, apart from face-to-face communication, State Security almost always used a business application. To improve and develop this system, a second business application was being developed for internal communication. As regards external communication, the channels and tools had been defined but the results were not very visible yet.

II.1.4.1.6. HRM objectives and tools

It was found that State Security had outlined its main challenges with regard to human resource management (HRM) in its strategic and operational plan. The inquiry carried out in the context of the audit – completed one month after the internal distribution of the 'Strategic Plan 2008–2012' – revealed that the managerial staff at State Security still considered themselves to be inadequately informed regarding the organisation's strategy for developing the skills of personnel in the long or short term.

120 *Ditto.*

As regards the HRM tools, it could be inferred from the audit that State Security had drawn up staffing plans, but the managers responsible for personnel management said they did not get involved with the monitoring, evaluation and adjustment of the HRM objectives. The staffing plan was, however, being annually adjusted according to staff turnover and operational needs.

II.1.4.1.7. Competency management

State Security had defined the necessary competencies through job profiles and job descriptions for all positions in the field services and for some positions in the assessment services. With regard to the personnel of the general services, the necessary competencies specific to State Security had not yet been defined.

II.1.4.1.8. Personnel training

The performance audit also focused on personnel training. It appeared that no training plan had been developed as yet with the aim of maximising the alignment between the existing and desired competencies. However, a clear vision for competency development had been outlined for the field services, as a result of the current legislation. It was also established that:

- in time, the ambitious training and development system for the field services can certainly deliver an added value. Nevertheless, the 'training and development' service will only be able to carry out its numerous tasks if it has sufficient staffing. The management was clearly aware of this, as is evident in the 'Strategic Plan 2008–2012', which provides for a reinforcement/expansion of the 'training and development' service. The service had set training priorities for the field services, but these were not managed in a systematic manner;
- for the internal services, there was a more systematic approach to the training courses. For the training of analysts, the legislation and regulations for federal officials are applicable. This legislation is, in itself, inadequate and interferes with the intention of providing the analysts a specific training adapted to the needs of State Security in the area of analysis. The evolution towards a harmonised statute for the various services of State Security would also make it easier to develop a general training policy for all these services;
- however, for the administrative personnel of the general services of State Security, the legislation applicable to the federal officials seemed sufficient to allow for the necessary, specially adapted trainings.

II.1.4.1.9. Development of managerial capabilities

Since 1999, management staff in the field services have been required to attend training courses to further develop their managerial capabilities. This matter has been regulated since the new statute came into effect.

For the internal services (analysts and general services), no information was available regarding the training courses attended by managers for developing their leadership qualities. Nevertheless, it appeared that the managers received regular feedback about their style of leadership. At the time of the audit, there was an evaluation system for the field services; the system had been recently modified.

Due to the absence of development circles applicable to State Security, no evaluations have yet been made for the assessment services on the basis of the new evaluation system.

II.1.4.1.10. Ensuring continuity in management positions

Finally, the problem of ensuring continuity in management positions was also examined. It was found that a *tool* had been developed for the transfer of knowledge between exiting staff members and their successors to the position, but this appeared to be limited to a job description. Overall consideration to the optimal organisation of the retention and transfer of knowledge is still lacking.

Normally, the level promotions are done through internal (promotion) exams. However, for the continuity of certain senior positions, the management has taken measures to temporarily grant these positions to certain employees without exams. Naturally, the subsequent publication and granting of the position do not place the candidates on an equal footing, since now the temporary employee already has experience in the position.

With regard to the temporary filling of senior positions, a considerable section of personnel found the selection criteria to be unclear and non-transparent. Therefore, attention was given to continuity, but sometimes at the expense of ensuring the objectification of the available competencies.

II.1.4.2. Information management

Information management within State Security was also addressed in the audit, in response to the following questions from the Minister of Justice: "*Availability, accessibility and permanence of information and employees is of key importance in the State Security organisation. How are these principles guaranteed? The speed and flexibility of information and employees is also of key importance within the organisation. For example, how is the work schedule structured to provide quick, efficient and continuous services?*"

II.1.4.2.1. Information

From impressions of staff, it appeared that the majority were satisfied with the accessibility and relevance of the information provided. However, a relatively small number were dissatisfied with the degree of user-friendliness of the information system and the timely availability of the information.

II.1.4.2.2. ICT resources for supporting the information flow

The audit also revealed that State Security had made a thorough analysis of the existing ICT organisation and systems in 2007, on the basis of which a long-term plan had been drawn up. The ICT objectives had then been converted into a short-term plan with specific, clear and measurable objectives and indicators.

In 2008, funds were made available for recruiting three staff members whose task was to develop the ICT service and to prepare recruitments and budgets. In the light of this task, the Standing Committee I was surprised by the recruitment choice: instead of an ICT director, an IT specialist and an administrative assistant for the ICT Cell as provided in the 2008 budget, an IT specialist and two administrative assistants were recruited. Moreover, at the end of the audit, the additional recruitment provided for in the ICT plan had still not taken place.

A majority of the respondents were of the opinion that there were a sufficient number of control points (control of the reliability, accuracy, classification and the need to know) in the information flow.

The Standing Committee I was of the opinion that, since the new ICT system had not yet been fully implemented, no proper assessment could be made about the quality of modifications in the information management process.

II.1.4.2.3. Availability and accessibility of personnel

As regards the flexibility and permanent availability of the employees of State Security, one should not ignore the relatively small size of the organisation.

In addition, the difference in statute between the members of the internal services and the field services also appeared to be important. The same statutory provisions – namely the principle of working hours being limited to normal office hours – are applicable to both the internal services of State Security as to the other administrative services of the Ministry of Justice. The management tried to remedy this situation, not unsuccessfully, by appealing to the professionalism of officials contacted during an incident. Here, too, recognising the specificity of the assessment services and therefore separating them from the general regime of public office, could provide opportunities for a guaranteed service around the clock. The field services, on the other hand, for which a more flexible statute is applicable, frequently work outside the office hours. After office hours, services are provided via an on-call service. Historically, this concept is

based on a surveillance task to which an alarm and call function has been added. The more ambitious concept of an 'operational centre' that might guarantee, for internal purposes as well as with respect to the policy level and external customers, an active monitoring (24/24) of the specific work area, could not be achieved as yet although efforts had been made to realise this for a long time.

II.1.4.3. Work processes

"*Is the flow and processing of the information managed in an efficient manner? Have these work processes been outlined and optimised based on a vision of how these work processes should be set up?"* The Committee also tried to find an answer to these questions. It was soon clear that steps had been taken towards applying the principles of process management, but the management of the processes[121, 122] was not yet perfect. Furthermore, it could be established that:

- the work processes of State Security were not adequately outlined. This task had, however, been allocated to a member of staff. In this context, the organisation also regularly referred to the ICT project, which was undergoing difficulties at the time of the inquiry. This project is part of the main projects originating from the 'Strategic Plan 2008–2012'. The inquiry among personnel showed that the work processes were not yet sufficiently formalised in documents, that the existing documentation inadequately defined how the activities needed to be conducted and that personnel felt insufficiently involved in the development and implementation of the work processes;
- State Security could define a process owner[123] for only one of the work processes;
- a majority of the personnel said to be aware of who was responsible for the outcome of the activities and who contributed towards achieving the result;
- a systematic evaluation of the work processes – in their entirety – was impossible for the time being because they were not yet sufficiently documented. According to the Head of the so-called Process Implementation Team (PIT), the middle management continuously evaluated the contents of the activities and the process results. The inquiry showed that the targeted results (quality criteria or standards) and performance indicators were still insufficiently defined and the measurements to verify whether the intended

---

121 A process (sometimes also called a business process or work process) is defined in the '*Leidraad Interne Controle/Organisatiebeheersing*' of the Flemish government as '*… a series of successive activities which convert resources (input) into results (output and outcome) whereby an added value is created" (free translation).* See: Agentschap Interne Audit van de Vlaamse Administratie, *Leidraad Interne Controle/Organisatiebeheersing*, 2008, 21.

122 State Security regards intelligence, security investigations and protection as its core processes. Its supporting processes are communication and sharing of information, personnel management, financial and procurement management, ICT and legal management.

123 The 'process owner' is the person responsible for the results (*output* and *outcome*) of a work process.

quality was being achieved were still inadequate. It could also be inferred from the inquiry that the modification of the work processes did not always happen on the basis of the measured efficiency, effectiveness and/or results and that this improvement did not always take place in consultation with the staff members participating in the work process.

II.1.4.4. Satisfaction with quality

In the last part of the performance audit, the Committee tried to get an idea of the level of satisfaction with the quality of the input and output of the information flows. It was also examined whether State Security was working on improving quality; in other words, whether it continuously strives for improvement. In view of the questions of the Minister of Justice (cf. II.1.2) – which almost exclusively focus on customer and employee satisfaction – a 'consumer-oriented perspective' was chosen, relating quality to the effects of the product or the service for the user (citizen/customer).[124]

II.1.4.4.1. Quality policy

The audit revealed that the management and staff of State Security were aware of the importance of implementing a quality policy, but a structured and orderly approach was lacking at present. It was also established that:

- integrating this policy within the cascade of objectives was underway. Strategic objectives had been formulated, which were aimed at increasing the quality of service. There was definitely a quality awareness within the organisation, but a structured and orderly approach would be appropriate here. In this respect, the abolition of the previously existing quality agency was regrettable. The inquiry among the managers revealed that the quality policy was not yet properly embedded at all levels. However, in the 'logistics' pillar, a methodical implementation of the quality efforts had already taken place;
- there was no quality manual or other document available in which the quality system was outlined;
- since 2003, no formal self-evaluation had been carried out for the entire State Security organisation, such as e.g. by means of a CAF.

A specific point of attention for the Minister of Justice was the question whether there was any actual monitoring and control for a consistent application of the declaration obligation stipulated in Article 29 of the Code of Criminal Procedure.

---

[124] G. BOUCKAERT and N. THIJS, *Kwaliteit in de overheid – Een handboek voor kwaliteits-management in de publieke sector op basis van een internationaal comparatieve studie,* Ghent, Academia Press, 2003, 9.

Barring the directives from the confidential circular letters COL 9/2005 and COL 12/2005 and the adherence to the legal obligations of the service for source protection and classification, there appeared to be no formal guidelines within State Security regarding the monitoring and control of the application of Article 29 of the Code of Criminal Procedure. According to the AG, monitoring and control of the application occurred via the systematic review for validation purposes by the line management and the transfer takes place after verification by the Director of Analysis. State Security provided no recent figures with regard to the application of Article 29 of the Code of Criminal Procedure. The Standing Committee I was also never informed by the judicial authorities of any non-compliance with this legal obligation.

II.1.4.4.2. Relations with external stakeholders

State Security had defined operational objectives in its strategic and operational plan aimed at improving its customer relationships. For this, it was essential that State Security first and foremost sounded out its customers[125] regarding their respective expectations with respect to the products to be delivered and their quality factors. However, the statements of the interviewed decision-makers showed that there was confusion regarding the useful product that State Security could be expected to deliver.

II.1.4.4.3. Satisfaction with quality

The relationship and cooperation with State Security was generally described by most players – each for its own more or less specific domain – as being relatively positive. Nevertheless, there were some comments regarding the exchange, quality and punctuality of the information, the cooperation, the making of formal agreements and communication. There were no comments regarding the relevance of the intelligence provided.

II.1.5. CONCLUSIONS

It was not the first time that State Security was the subject of an audit. Such an audit had been carried out earlier by the Standing Committee I (Audit 2002–2003), and State Security had carried out a self-assessment prior to the Master Plan and the launch of the improvement projects within State Security (CAF

[125] In the context of the *performance audit*, the following players were selected from the various customers: the GISS, the Federal Police, the National Security Authority, the Federal Prosecutor's Office, the Governmental Crisis Centre, the Immigration Service, the strategic units Justice, Foreign Affairs and Home Affairs and the CUTA.

2003–2004). In line with earlier conclusions of the Standing Committee I, State Security had implemented an overall IT project. This project commenced with an audit carried out by an external consultant. In this project, the Standing Committee I had already completed the first phase of an investigation of the information flows within State Security.[126]

The picture outlined in this performance audit is the result of a snapshot in time (October 2008 – April 2009). As already mentioned, the task in this audit was focused on management level (the organisation in the narrow sense) rather than on policy level (the policy framework within which State Security operates). Therefore, an assessment of the proposed policy (estimating the potential effectiveness, feasibility etc.) was not on the agenda.

It is clear that, at the time of the audit, the Standing Committee I was faced with an organisation at a turning point: the 'Strategic Plan 2008–2012' had been implemented and new statutes introduced, the information management process had been redesigned and contemporary management principles were steadily making their entry…

Nonetheless, for the Standing Committee I, the findings of its audit indicated that State Security was being managed in an ambiguous manner. On the one hand, the management made use of business management applications such as 'planning & control'. On the other hand, it could not be determined whether the management did this merely because of the obligations imposed on it by the Royal Decree on State Security, or whether it was motivated by the belief that such tools are valuable. Since, the management continued to insist on the operational and informal nature of the service. The audit subsequently showed that, for the management, the formalisation was not a *conditio sine qua non* for achieving a 'good' decision-making process. The service also seemed to often operate based on a behavioural decision-making process existing within a cooperation of participants, each with their own objectives. As soon as the management committee found a solution that met the aspirations of the parties involved, that path was chosen. The risk of this type of decision-making process is that it follows a rather whimsical course, with a risk of gaps, sudden deviations, repetitions and contradictions.[127] A rational decision-making process, on the other hand, leads to a consistent and straightforward course, in which everything is linked to one another in cascade form (e.g. all sub-goals linked to goals).

If the Standing Committee I was critical of State Security in this audit, it wants to emphasise its confidence in the desire and capability present within State Security to carry out its tasks efficiently and effectively. The Standing

---

126 Also see 'II.3. The information processes of State Security' and 'II.10.4. Information management at State Security' from the 2007 Activity Report (STANDING COMMITTEE I, *Activity Report 2007*, 101). Of course, these conclusions were also taken into account in this performance audit.

127 N. VALLET, *Management van organisaties. Een caleidoscopische blik*, Acco, Leuven, 2006, 183.

Committee I postulates that national security requires a strong and reliable intelligence and security service. That is also why the Committee is convinced that an organisation and a management that meets the management standards of an efficient and effective public service would benefit State Security.[128]

II.2. THE MANNER IN WHICH STATE SECURITY HAS OBTAINED, PROCESSED AND DISSEMINATED INTELLIGENCE ABOUT BARON DE BONVOISIN

II.2.I. INTRODUCTION

With the complaint of Baron Benoît de Bonvoisin[129] in connection with "*the actions of some State Security officials, which have seriously prejudiced him since 1981, as well as against Koen Dassen, the current Director-General, who continues to refuse to refute the false accusations made against him by State Security*"[130] (free translation), the Standing Committee I became involved in protracted disputes[131] between the complainant and State Security. The person in question alleged to be (or have been) seriously prejudiced by the activities of some members of State Security. He believed to have been a victim of manipulation and fabricated information for many years, which had resulted in damaging his reputation. Baron Benoît de Bonvoisin became known to the general public in the spring of 1981 when the newspaper *De Morgen*[132] revealed the contents of a confidential memorandum from the then Minister of Justice (the so-called CEPIC Memorandum) addressed to the Senators of the Wijninckx Committee (*infra*). In

---

128 For the recommendations formulated in the context of the audit, see Chapter VIII. Recommendations.

129 In contrast with the rule followed by the Standing Committee I, the names of the complainant (Benoît de Bonvoisin) and of the then Administrator-Director-General of Public Safety (Albert Raes) are explicitly mentioned, in view of the wide publicity given in the media to the disputes between these persons. Other persons are not mentioned by name.

130 "*The actions of some State Security officials, which have seriously prejudiced him since 1981, as well as against Mr. Koen Dassen, the current Director-General, who continues to refuse to refute the false accusations made against him by State Security*' (free translation).

131 Benoît de Bonvoisin had instituted multiple civil proceedings, the Court of Appeal of Bergen had acquitted him on 12 May 2000 in the 'PDG-Cidep' case and during the course of the investigation, legal proceedings were instituted against the complainant before the Criminal Court of Brussels in the context of a dossier concerning forged KGB documents, in which Albert Raes was involved as a civil party. At the end of 2009, the Court gave its judgement in this case, in which it decided to separate the dossier with respect to Baron Benoît de Bonvoisin and adjourned the case *sine die* as far as he was concerned.

132 W. DE BOCK, '*Nota van de Staatsveiligheid: top van CEPIC financierde Jongerenfront*', *De Morgen*, 19 May 1981.

the memorandum, which was based on elements provided by State Security, de Bonvoisin was described as 'a financier of the extreme right in Belgium'.

The Standing Committee I initiated its investigation in the beginning of February 2006.[133] However, several (former) agents of State Security, as well as the previous and current Director-General have stated that the Standing Committee I was not authorised to carry out an investigation into 'old and therefore lapsed facts or into facts which took place before the establishment of the Standing Committee I'. But the Standing Committee I was of the opinion that the term 'limitation' does not apply in the context of its review tasks. Since its task is not criminal or even judicial in nature, but has a different objective (i.e. to ensure a permanent parliamentary review, safeguard the rights and freedoms and contribute to the proper functioning of the intelligence services). Nor does the Review Act contain any provision limiting the competence of the Standing Committee I to facts dating from after this Act had come into effect. The aforementioned fundamental objections were therefore not an obstacle to carrying out the investigative actions considered necessary by the Standing Committee I.

However, the Committee decided to restrict its investigation to the period from the late '70s to the early '80s. On the one hand, because the documents available for consultation were related exclusively to this period and, on the other hand, because the information which had allegedly prejudiced the complainant was *de facto* nothing more than a repetition of information dating from that period.

II.2.2. METHODOLOGY

The Standing Committee I systematically[134] examined all reports and documents of State Security as well as those found in the judicial dossiers. This allowed the Committee to identify any developments and changes in their content or repetitions and sometimes also contradictions between the reports of various departments within State Security. Besides examining the documents, the Standing Committee I also questioned a number of (former) members of State Security who were involved in monitoring this case at that time.

---

133 Initially, the Committee had decided to focus its investigation not only on State Security, as requested by the complainant, but also on the military intelligence service. However, it seemed that the GISS did not have any file on Benoît de Bonvoisin, even though in 1980 the person in question maintained close relations with an officer of the army who was associated with extreme right-wing activities, and though he travelled regularly to Zaire. The Committee decided not to continue its investigation with regard to the military intelligence service.

134 A chronological distinction was made between four periods: (a) the period before 1980; (b) the Ekkehard Weil case (early 1980); (c) the period around the Wijninckx Parliamentary Inquiry Committee (1980 – June 1981) and (d) the period after the Wijninckx Committee.

II.2.2.1. Collection and analysis of the existing documentation

The Standing Committee I made considerable efforts in searching for relevant information and documents and concluded that this case, despite its age, was still a very sensitive issue. Also, it was far from easy to gain access to these documents, which over time were scattered across various administrative and judicial services and which were also to be found among private individuals and agencies. The Committee was also faced with a lack of certainty regarding the completeness of the information, despite the substantial quantity thereof.

The complainant had provided the Standing Committee I with numerous documents (copies of records from the judicial files, conclusions of lawyers, correspondence, press articles and several documents with personal opinions).

In addition, judicial files were identified at the Office of the Public Prosecutor of Brussels which included various (documents from) State Security files. The latter proved particularly time-consuming.

State Security did have a 'Benoît de Bonvoisin' dossier, but this did not contain any documents from the period 1970–1980.[135]

The Committee also took note of the report of the Parliamentary Inquiry Committee on the problems related to the maintenance of law and order and the private militias (the so-called Wijninckx Committee[136]). However, it did not receive permission from the Senate to consult the statements of Albert Raes, the then Administrator-Director-General of Public Security.[137]

Access to confidential documents from the archives of journalist Walter De Bock, who had studied the case and published the CEPIC Memorandum in his article in De Morgen (*supra*), was denied by the Council for Journalism on grounds of the confidentiality of journalistic sources.

II.2.2.2. Hearing of the persons involved

Given the age of the facts, it was not easy to find witnesses to hear. The then managers of State Security and most of the agents who had worked in the cases involving Baron Benoît de Bonvoisin, had left or retired from State Security.

---

135 This is a file compiled following the request of the complainant addressed to the then Minister of Justice with regard to his rehabilitation.

136 The actions of the Vlaamse Militanten Orde (VMO) and the Front de la Jeunesse (FJ) on 19 March 1980 led to the establishment of a Parliamentary Committee in the Senate which was assigned the task of investigating the application of the Act on private militias and the operation of the competent public authorities in the field of law enforcement. On 19 February 1981, Albert Raes was questioned by this Committee. The hearing took place behind closed doors.

137 The President of the Senate informed the Standing Committee I that "*the statements of Mr Raes, the then Administrator-Director-General of Public Security, were made behind closed doors. The Inquiry Commission has at no time decided to make these reports available. In similar circumstances, it is impossible to grant access to these reports*" (free translation).

Moreover, some were seriously ill and others were deceased. The Standing Committee I also made every possible effort to hear the then Administrator-Director-General Albert Raes with regard to this case. But these negotiations, conducted via ample correspondence with the aforementioned and his advisers, were unsuccessful. Albert Raes could not be summoned to the hearing; since former members of intelligence services cannot be obliged to testify before the Standing Committee I (Article 48 of the Review Act). To optimise the effectiveness of future investigations, the Standing Committee I therefore suggests that this be rectified.[138]

These hearings were aimed not so much at obtaining information about the facts themselves, but rather at obtaining details about the organisation and working conditions of State Security at that time.

II.2.2.3. Use of classified documents in the reports submitted by the Standing Committee I to the Monitoring Committee

During its investigation, the Standing Committee I was confronted with certain classified documents[139] of State Security which had been confiscated in 1989 by the judicial authorities and subsequently also used *materialiter* in criminal cases. Thus, these documents had long acquired a virtually public character. The Standing Committee I was therefore of the opinion that there was nothing to prevent it from mentioning these documents in its report to the Monitoring Committee of the Senate. Since this could no longer harm the interests listed in Article 3 of the Classification Act (e.g. the internal and external security of the State or any other fundamental interest of the State).

II.2.3. FINDINGS

Based on the exhaustive desk research and the hearings, the Standing Committee I formulated the following findings.

It appeared that the 'interest' in the person of Baron Benoît de Bonvoisin only emerged relatively late.[140] It was only in December 1980 that a personal file was

---

138 See in this regard 'Chapter VIII.3. Recommendations concerning the effectiveness of the review' of the present Activity Report 2009.

139 In accordance with Article 31 of the Royal Decree of 24 March 2000 for the implementation of the Classification Act, documents dating from before 1 June 2000 which are marked as 'Top Secret', 'Secret' or 'Confidential' shall be considered to be marked with the corresponding classification level specified in Article 4 of the Classification Act.

140 At that time, State Security only had a few elements of information concerning the complainant. A first memorandum – a half page – on Benoît de Bonvoisin dates from 28 March 1975 and was drafted at the request of the then Deputy Administrator of State Security, Albert Raes. A second limited memorandum dates from 23 April 1975.

opened in his name, which means before this he had not been a target of State Security.

After 1980, it was notable that the memoranda specifically focused on Baron Benoît de Bonvoisin, while the names of (many) other persons also appeared in these. The Standing Committee I could see no reason why he was being distinguished from among these other persons and made the 'key figure' of the memoranda intended for the Minister of Justice. One example of this is the Ekkehard Weil[141] case, where the name of Benoît de Bonvoisin only appears as information in the first memorandum (early 1980), to subsequently become the main person to be received by Weil in his 'castle'.

There also appeared to be a link between the activities of the Wijninckx Committee and the more intensive monitoring of the complainant by State Security. However, the Standing Committee I has not managed to identify the reasons for this. It was only in the period shortly before the establishment of the Wijninckx Committee and in the period during which this Committee was active, that State Security suddenly deployed considerable resources to monitor Baron Benoît de Bonvoisin, particularly by enlisting the help of certain informants who were better compensated than others and through various surveillance operations. Baron Benoît de Bonvoisin was twice placed under surveillance prior to the first and second hearing of Administrator-Director-General Albert Raes before the Wijninckx Committee. These operations were discontinued on the day before or on the day of his hearing. De Bonvoisin was placed under surveillance a third time shortly before the Wijninckx Committee submitted its report.[142]

Furthermore, in the period under investigation, a parallel circuit emerged within State Security with an 'unofficial' section consisting of persons 'loyal' to the then Administrator-Director-General Albert Raes. Directives were issued directly by the Administrator-Director-General, via his deputy, without these traversing the usual hierarchical path. Agents also submitted their reports directly to the management[143] without informing their supervisors about the work performed and without their supervisors being able to validate the intelligence. Some of these reports were handwritten. Also, reports were often submitted verbally directly to the management. Some witnesses state that they

---

141 In the beginning of January 1980, State Security learns that a German extremist, who had made an assassination attempt in West Berlin, had fled to Belgium and was looking for identity documents. Like the Indictment Division of Brussels, the Standing Committee I could not deliver an opinion regarding the veracity of the information about the possible role of Baron Benoît de Bonvoisin in this.

142 From 26 February 1981 to 7 March 1981, Benoît de Bonvoisin was placed under surveillance by State Security. This was repeated from 20 March 1981 until 17 April 1981, albeit with some interruptions. From 11 to 14 June 1981, de Bonvoisin is again placed under surveillance.

143 Most of the witnesses name Albert Raes as a direct recipient of these reports.

have written or prepared more reports than those appearing in the investigation file of the Standing Committee I.[144]

The Standing Committee I was forced to conclude that the then State Security had neglected to perform its verification task in this matter as the Committee found no trace of any request for verification. Neither was any analysis found (in the meaning applicable within the intelligence services). According to several persons questioned, Albert Raes did not give any importance to this. Raw information without verification was sent directly to the management[145] and this information served as the basis for the memoranda for the Minister of Justice.

The Standing Committee I found that the information obtained, though sometimes initially formulated with some reservations was later presented – despite the lack of verification – elsewhere as facts. It was the management that intervened to influence the content of some reports, for example for the reports of State Security used by the then Minister of Justice for preparing the so-called 'CEPIC Memorandum' (*supra*). These reports were corrected and rewritten in the indicative mood – by the Deputy Administrator, but also at the request of the Administrator-Director-General – while they had originally been written in the conditional mood.

II.2.4. CONCLUSIONS

The investigation into the complaint of Baron Benoît de Bonvoisin against State Security was in relation to a bygone period; the first facts examined had occurred more than thirty years ago. The present investigation, therefore, did not deliver any judgment on the legality, coordination and efficiency of the current activities of State Security, especially since this service has only had an organic law since 1998.

Despite this reservation, the Standing Committee I formulated three conclusions:

– the creation of a 'parallel and unofficial circuit' inside an intelligence service should be condemned, especially when agents in the field are working directly for the management and reporting only to them;

---

144 The Standing Committee I has not found these memoranda and reports, and neither has it found any trace of their existence.

145 In its judgment of 12 March 1992, the Indictments Division of Brussels described this as follows: "*those who have contributed to writing these memoranda can certainly be blamed for having amalgamated intelligence, assumptions and even deductions into firm statements without any qualification; Since the formulation of these memoranda seems to indicate a lack of rigour, as State Security could not in any way verify the intelligence at its disposal, and thus could only determine the degree of credibility in terms of probability, that it is therefore surprising that these memoranda contained a series of statements without any reservations and without any value judgment with regard to the reliability of the sources used…*" (free translation).

– a 'normal' operation of the services must be absolutely guaranteed within an intelligence service. This implies that information obtained must follow the usual hierarchical path, which must also serve as a filter and a means to validate this information after checking and verification;
– information obtained must be analysed by experienced personnel. 'Intelligence' cannot be reduced to raw 'information' that is not verified. After all, 'intelligence' is the result of collecting, processing and analysing 'information'.

The Standing Committee I also judged that the interest shown by State Security in Baron Benoît de Bonvoisin was legitimate, considering his activities, his travels and his contacts, particularly with extreme-right movements. It appears, however, that he had become the 'target' of memoranda and reports of State Security which were intended for the Minister of Justice for reasons that are unclear. Moreover, the Standing Committee I could only conclude that these memoranda and reports contain allegations, assumptions and even deductions which were not verified for their credibility and reliability and had been formulated without any qualification. This criticism is not so much directed against the entire then State Security as an institution, but against the 'parallel and unofficial circuit' which was set up within this service in December 1980 and at the beginning of January 1981, and which operated outside the competent sections – and even without their knowledge – whose task it was to monitor the extreme right.

II.3. THE BELLIRAJ CASE

In February 2008, the Moroccan authorities announced the arrest of 32 persons allegedly involved in an organisation which intended to infiltrate the political parties and gain control of the country's institutions. Moreover, the clandestine network of this organisation was reported to have planned assassination attempts on Moroccan Ministers and high officials.

Among the detainees, were five persons who had a connection with Belgium. Three of them had the Moroccan as well as the Belgian nationality. Furthermore, one of them, namely Abdelkader Belliraj, was said to be the leader of the network. He was born in 1957 in Morocco and had moved to Belgium in the early '70s. In 2000, he became a naturalised Belgian. Belliraj appeared to have maintained contacts with several international terrorist organisations, including *Al Qaeda*, the *Salafist Group for Preaching and Combat* (GSPC), the *Moroccan Islamic Combatant Group* (GICM) and the Lebanese *Hezbollah*. In 2001, he was also said to have travelled to Afghanistan to meet the *Taliban* chiefs and heads of *Al Qaeda*.

In the weeks following the arrest, the revelations in the press followed in rapid succession. It was thus alleged that significant amounts of arms and ammunition, originating from Belgium, had been seized. The network was also said to have been responsible for the robbery in 2000 at the Brinks headquarters in Luxembourg. Belliraj himself was allegedly responsible for six unsolved murders in Belgium between 1986 and 1989. Concerning these murders, the person in question is deemed to have made detailed confessions to the Moroccan court.

When, in the beginning of March 2008, the Belgian press also reported that Belliraj was allegedly a paid informant of State Security, the Minister of Justice and subsequently his colleague from Defence requested the Standing Committee I to initiate an investigation into '*the manner in which the Belgian intelligence services had monitored the persons who were recently arrested in Morocco and who were apparently suspected there of forming a terrorist group*' (free translation). Soon after this, the Monitoring Committee of the Senate requested the Committee to extend its investigation to two more points: according to certain press articles, the Belliraj case was reported to have given rise to tensions between the intelligence services and the police services and secondly, the Standing Committee I needed to investigate whether State Security and the GISS had correctly applied the Classification Act of 11 December 1998 on the information at their disposal *in casu*. In September 2008, additional questions followed from the Monitoring Committee (they wished to know what intelligence had supposedly been given by the Moroccan services to State Security regarding the possible involvement of Belliraj in extremist and/or terrorist activities) and from the Minister of Justice (he wanted details regarding the cooperation between State Security and the CUTA).

The Standing Committee I was of the opinion that the investigation should not have restricted itself to the alleged involvement in a terrorist network. Certainly not in view of the reports in the media: Belliraj was reported to have been a State Security informant, despite his serious criminal past; he appeared to have been naturalised as a Belgian citizen without much ado, smuggled huge amounts of arms from Belgium… These aspects were included by the Committee in its investigation.

As a consequence, the Committee was faced with a very extensive investigation straddling several decades, since State Security's interest in Belliraj dated back to the '80s.

Belliraj was sentenced to life imprisonment on 27 July 2009 by the court in Salé. The sentencing was not solely related to the fact that he was considered to be leader of a radical Islamist network but because Belliraj was also found guilty of the six murders committed in Belgium. Belliraj appealed against his conviction. This procedure had not yet been completed by mid-2010.

In Belgium, a judicial inquiry was initiated against him for the murders and the terrorist activities. The Standing Committee I is not aware of the content of this inquiry. When requested, the Federal Prosecutor's Office stated in April 2009 that the examining magistrate did not wish to grant the right of inspection because the inquiry was still in progress. In July 2009, the Committee received the same reply. The Standing Committee I has invested a great deal of people and resources in this case. Numerous documents were requested, inventoried and examined and this was followed up by a considerable number of hearings of members of the intelligence services. Pursuant to Article 48, §2 of the Review Act, some of these interviews were conducted under oath.

The final report of this investigation was completed in 2009. The Belliraj case had previously been the subject of five preliminary reports.[146] With due consideration of the Intelligence Services Act of 30 November 1998 and the Classification Act of 11 December 1998, the results of these preliminary reports were published in the previous Activity Report of the Standing Committee I.[147] Where necessary, the answers from that Activity Report are supplemented or nuanced with information obtained in 2009.

II.3.1. WHAT WAS THE INFORMATION POSITION OF STATE SECURITY WITH REGARD TO THE DETAINEES?

Gaining a complete picture of the exact information position of State Security was important in several respects. First, to assess whether State Security has duly fulfilled one of its core tasks (i.e. the monitoring of (potential) extremist groups and individuals). But in the context of this investigation, knowledge about the information position of the service was also important in order to answer the following questions: Did State Security have any indications that the detainees were working for foreign services (see II.3.2)? Was State Security aware of any involvement of the concerned persons in punishable offences in Belgium and/or abroad (see II.3.3)? Was the manner in which State Security gave advice in the context of the naturalisation applications of Belliraj in accordance with the rules (see II.3.6)?

The Standing Committee therefore drew up an inventory of all the information and intelligence known to the service at a given moment. It also compared these elements with the information in the possession of the then

146 Report of 10 April 2008 for the Monitoring Committee of the Senate and the Ministers of Justice and Defence; Report of 2 October 2008 for the President of the Senate and the Minister of Justice; Report of 2 October 2008 for the Minister of Justice; Report of 20 October 2008 for the Minister of Justice; Report of 29 October 2008 for the Monitoring Committee of the Senate and the Minister of Justice.

147 See STANDING COMMITTEE I, *Activity Report 2008*, 34–43.

Mixed Anti-Terrorist Group (ATG), not to assess the information position of the ATG and the current CUTA, but to determine whether and to what extent the information of the ATG had been communicated to State Security. After all, State Security had a permanent representative in this group.

The Standing Committee I has been able to establish that Belliraj was closely monitored at various points of time. He was known to State Security since the early '80s as an extremist Islamist and a pro-Iran opponent of the Moroccan King. He had been placed under surveillance several times during that period. This was with the intention of gaining an insight into the contacts he maintained with the radical Islamist world. Even after this period, he was actively monitored by State Security.

In addition, two other detainees were known to State Security because of their close contacts with extremist groups with Shi'ite or salafist leanings. One of the two was also known for banditry.

II.3.2. DID STATE SECURITY HAVE INFORMATION ABOUT POSSIBLE RELATIONSHIPS BETWEEN DETAINEES AND FOREIGN INTELLIGENCE SERVICES?

The Standing Committee I has not been able to establish whether State Security had information which would help conclude that Belliraj or the other detainees known to the service had cooperated with one or more foreign intelligence services active in Belgium.

II.3.3. WAS STATE SECURITY AWARE OF ANY INVOLVEMENT OF THE DETAINEES IN PUNISHABLE OFFENCES IN BELGIUM AND/OR ABROAD?

In the press, Belliraj was linked to arms trafficking, terrorist activities, six unsolved murders in Belgium, a robbery in Luxembourg, involvement in a clandestine network aiming to overthrow the Moroccan regime…

Nevertheless, all State Security staff questioned by the Standing Committee I stated that they did not have any information, indication or suspicions in that regard. Belliraj had a clean criminal record. He did not seem to have the profile of a leader of a network of the level that had apparently been dismantled in Morocco. According to the same statements, there were never any indications of any involvement in the six unsolved murders. The State Security staff who were questioned also appeared to be surprised by the possible arms trafficking charges.

The Standing Committee I could only be amazed by some parts of these concurrent statements. Especially since the Committee was aware of elements indicating that Belliraj was (possibly) involved in a number of criminal offences. For instance, documents had been found that showed that he had actually been sentenced for theft and for assault and battery charges. But more importantly, in the files originating from State Security itself, Belliraj had been repeatedly linked, from the '80s and early '90s, with trafficking in arms and explosives, with a possible involvement in a group responsible for an attack against a foreign head of state, with a pro-Iran movement of which the leaders were wanted by the police in Morocco, with the creation of false documents and with maintaining contacts with a (non-Islamist) terrorist group… One report even mentioned the fact that Belliraj was looking for arms and explosives to carry out an attack in Belgium as a result of the arrest of GIA (Groupe Islamique Armé) leaders. Though it must immediately be pointed out that the person in question was never sentenced for terrorism-related offences and no judicial inquiry had been carried out against him, the statements of the State Security staff still remain surprising in the light of their own documentation.

However, the Committee did not find any elements in the State Security documents indicating any involvement in the robbery in Luxembourg[148] and in the murders of 1986 and 1989. What the Committee did have, via the CUTA, was a memorandum from its predecessor, the ATG, showing that Belliraj had entered into the picture at that time for one of these murders. Although State Security had a representative in the ATG and was informed in accordance with the normal procedures, via this person, of all incoming and outgoing information from the ATG, this particular information does not seem to have been included in the documentation of State Security.

Also, there was no mention in any report of State Security of the fact that Belliraj appeared to have been involved in the (alleged) terrorist cell targeted against Moroccan interests. Neither could the Standing Committee I establish that State Security had received such information – at least directly – from its Moroccan colleagues. But also in this respect, it could be gathered from the documentation of the ATG that in the '90s a Moroccan intelligence service had asked Belgium questions regarding some persons – including Belliraj – who appeared to have links with Iranian Islamist movements. This information was also not found in the State Security files.

II.3.4. WAS BELLIRAJ A STATE SECURITY INORMANT?

The Standing Committee I was, of course, unable to get past the question as to whether Belliraj was recruited by State Security as an informant and if so, how

[148] But State Security was aware of the fact that one of the other detainees, with whom Belliraj was in contact, was involved in the hold-up at BRINKS in Luxembourg.

had he been handled. The Committee investigated the matter and reported on this to the Minister of Justice, the competent authority in this case. The Committee has neither the power nor the authority to offer an affirmative or negative answer to other persons or agencies regarding the question as to whether the concerned person was an informant.[149]

II.3.5. DOES STATE SECURITY HAVE PROCEDURES, REGULATIONS AND GUIDELINES WITH REGARD TO WORKING WITH INFORMANTS?[150]

At the request of the Monitoring Committee, the Committee investigated whether State Security has procedures, regulations and guidelines with regard to working with informants.

For most staff members of the information sections of the field services of State Security, the recruitment, *running* and assessment of human sources is a daily activity which is closely monitored by the direct manager(s).

There are a number of written guidelines in this respect (e.g. regarding the decision for accepting a person as a 'centrally registered informant' and the elements which are to be investigated, regarding the assessment and compensation…) although these are spread over various documents. In addition, certain aspects of informant operations are only included in the course material for trainees or are only part of practices specific to the service. The Standing Committee I found this surprising, considering the importance of the use of informants for the service. A HUMINT office was, however, set up in 2007. Its task is to implement State Security policy on this matter in practice, contribute to the organisation of staff training and cooperate with regard to the assessment and protection of sources. One of the achievements of this agency is the syllabus for training new inspectors, in which the issue of working with informants is handled in its entirety. At the same time, State Security was to work on developing a general internal regulation on this subject.

In 2009, the Standing Committee I looked closely into one of the aspects of the use of informants: the assessment of possible risks associated with working with informants.

---

149 See STANDING COMMITTEE I, *Activity Report 2008*, 38–39.

150 The Standing Committee I has focused its attention on informant operations on various occasions in the past; the first time, through an extensive thematic investigation (Investigation of the informants of State Security and of the GISS (*Rapport d'activités 1997*, 139-168)) and later through more ad hoc investigations in which certain aspects were examined in more detail: *Rapport d'activités 1999*, 95-96; *Rapport complémentaire d'activités 1999*, 72-75; *Rapport d'activités 2004*, 24-35; *Rapport d'activités 2000*, 163-170 and 192; *Rapport d'activités 2003*, 9-10; *Rapport d'activités 2003*, 207-208 and 230-232 and *Rapport d'activités 2004*, 111 and *Activity Report 2008*, 54–43.

The Standing Committee I is not aware of any instruction or a manual for the State Security personnel which lists or describes the risks in recruiting and running an informant. Such risks can be inferred implicitly from a number of service memoranda and other documents.

The most obvious risk, according to State Security, is the source itself. For obvious reasons, therefore, the service attaches utmost importance to preserving the anonymity of the source. This protection is, of course, primarily aimed at protecting the environment of the informant, but it is also extended to other services and is even applicable within State Security.

But State Security also acknowledges the risks for the service itself. This can take various forms. A (potential) source can be used by its original environment or by an unfriendly intelligence service, for example, to find out about the methods used by the Belgian State Security and its information position. Another possibility is that State Security, whether or not deliberately, is saddled with inaccurate information. Finally, it is not inconceivable that an informant is only interested in the possible compensation, without delivering any usable intelligence.

A particular risk is associated with informant operations involving persons who were or are involved in crimes. During the training course, agents are explicitly warned about cooperating with people who have criminal records.

However, the general method used shows that no formal risk analyses are carried out by State Security with regard to working with informants.

II.3.6. DID STATE SECURITY UNLAWFULLY INTERVENE IN THE NATURALISATION PROCESS OF BELLIRAJ?

Another question was whether State Security had, in any way whatsoever, facilitated the naturalisation of Belliraj as a Belgian citizen.

Here it is important to note that Belliraj had submitted an initial application at the end of the 1980s. After a long procedure, his application was rejected in 1998 by the House of Representatives. The most notable aspect was the distinctly negative advice of State Security. The service had knowledge of various elements linking Belliraj to criminal and extremist activities (see II.3).

Equally important is the fact that the then wife of Belliraj (further referred to as 'X') submitted a naturalisation application in early 2000. The recommendation of State Security stated that "*State Security has nothing to report concerning X. However, her husband, Belliraj (…) is known to our services owing to his activities within the Algerian and Moroccan Islamist radical movements*" (free translation).

When the so-called Fast-Track Belgian Naturalisation Act came into effect in 2000 – which implied that one could receive the Belgian nationality within a month – Belliraj submitted a new application. As a result of this application, a Deputy Head of the relevant department of State Security formulated the

following advisory opinion on 6 June 2000: "*I have the honour to inform you that Belliraj is known to our services owing to his activities within the Algerian and Moroccan Islamist radical movements.*" (free translation).

In other words, the advisory opinion developed for Belliraj was identical to the words used about Belliraj in the advisory opinion drawn up shortly before for his wife X.

However, from 13 June, the case takes an unexpected turn: a new advisory opinion is drafted for both X and Belliraj and sent to the Prosecutor's Office in Ghent. Yet the two advisory opinions did not have the same date: the advice on X dated from 24 March; that on Belliraj from 6 June. The advisory opinion for X stated that "*State Security has nothing to report regarding X*"; the advisory opinion for Belliraj is as follows: "*I have the honour to inform you that Belliraj was known to our services during the 1980s owing to his activities within the pro-Iran Moroccan milieu. Since then however, he has not come to our attention either in this context or due to any other political activity.*" (free translation). This second advisory opinion regarding Belliraj was signed by the Head of the concerned department. Only this advisory opinion was found in the naturalisation file at the competent Prosecutor's Office. Since there were no indications to the contrary, the Belgian nationality was granted.

The Standing Committee I has conducted an intensive investigation into how and why these two advisory opinions were formulated for Belliraj. According to the members of State Security questioned under oath, no actions were carried out at any time with a view to facilitating the acquisition of the Belgian nationality. State Security has – according to the Director-General – delivered a second advisory opinion at that time which still exposed his radical profile, although less pronounced than in the first advisory opinion. At that time, the Fast-Track Belgian Naturalisation Act was also in effect, so the service had to handle hundreds of applications a day.

The Standing Committee I can only conclude and regret that State Security is not in a position to give a satisfactory explanation about these two advisory opinions. This naturally provides fertile ground for speculation and guesswork.

II.3.7. HOW DID THE COOPERATION WITH THE CUTA PROCEED?

The Minister of Justice asked for clarifications regarding the earlier report of the Standing Committee I which revealed that State Security had apparently not shared all the intelligence it had regarding Belliraj, with the CUTA. Yet Article 6 of the Threat Assessment Act obliges State Security to pass on all intelligence which is relevant within the framework of the execution of the assignments of the CUTA (in particular, the drawing up of ad hoc or strategic threat assessments with regard to terrorism or extremism).

It is true that State Security did not communicate any information to the CUTA, even though they knew Belliraj and two of the other detainees. The Standing Committee I is therefore of the opinion that State Security has not fulfilled its legal obligation. As a result, the CUTA was not in a position to assess a possible threat against persons (Art. 2, 1°, RD CUTA). Since the reports in the press that certain persons were allegedly informants of State Security also mentioned their place of residence, this meant that their safety and that of their next of kin could be in danger. This possible danger is not necessarily related to the fact of whether or not these persons are also actually informants.

But the Director-General of State Security contested the fact that the information available to his service could be regarded as 'relevant' under the meaning of Article 6 of the Threat Assessment Act. Moreover, he pointed to a possible conflict between two legal provisions, one of which implies an obligation and the other a ban on the communication of certain information. In view of these elements, specific to this case, the Committee was of the opinion that though Article 6 of the Threat Assessment Act had indeed not been respected, no criminal or disciplinary violations could be established on the part of any member of State Security.

II.3.8. HAS THE BELLIRAJ CASE GIVEN RISE TO TENSIONS BETWEEN THE INTELLIGENCE SERVICES AND THE POLICE SERVICES?

At the request of the Monitoring Committee, the Standing Committee I tried to investigate whether the Belliraj case had given rise to tensions between the intelligence services and the police services. Some press sources even referred to a 'war between anti-terror services' and it sometimes seemed that this war was being fought out in the media with allegations flying back and forth from mostly 'anonymous sources'.

A certain amount of friction between the two services was already evident from certain statements made following the investigation into the terror alert in the end-of-year period of 2007.[151] Based on statements from various open sources and from interviews with the management of State Security, the Standing Committee I has concluded that there was increased tension in certain areas. Though the Director-General of State Security refuted these reports and referred to good relations in the field, the fact remained that one could read of many 'revelations', 'insinuations' and 'accusations' in the press.[152] The Committee found several (possible) reasons for this.

---

151 STANDING COMMITTEE I, *Activity Report 2008*, 11-23.

152 In a reaction to this, the Director-General lodged two complaints. A civil complaint lodged against unknown parties for violation of the principle of professional secrecy and of the

Firstly, there is the fear of a possible overlapping of authorities. After all, the intelligence services are not the only agencies that gathers intelligence information. Article 44 of the Police Function Act of 5 August 1992 also grants the police services the authority to collect and process intelligence on persons, groups and events which are relevant to the 'administrative police'. Moreover, since the Act of 12 March 1998, the police services are also authorised to perform proactive investigations. The Federal Police has also started investing a great deal of resources in their proactive approach to the fight against terrorism. In doing so, it has encroached on State Security's territory. The fact that this can lead to conflicts was evident, as mentioned, from the investigation into the terror alarm in the end-of-year period of 2007.

Another possible explanation for the sometimes less than optimal understanding between the two services, dates from the period that the police were granted new, special investigative powers by the so-called Special Investigative Methods Act. This made it possible to adopt a more police-oriented approach to the phenomenon of terrorism. The Federal Police could therefore build up a strong information position in this area and also became a discussion partner for foreign secret service agencies.

This imbalance can now be restored since the intelligence services can also avail, from 1 September 2010, of specific and exceptional methods via the so-called Special Intelligence Methods Act. But this Act, in its turn, can also result in new frictions. Since the police now appear to be pressing for a regulation on methods for administrative police (Special Administrative Methods Act). This Act should allow administrative police to operate in the phase where currently only the intelligence services are active.

The Standing Committee I observes that, in the fight against terrorism and radicalism, there is an overlapping of authorities which could lead to competition. It appears that a solution can only be found if there is a clear division of tasks and if the exchange of information proceeds smoothly. That is why it is vital that both services enter into a cooperation agreement. The competition must make way for cooperation.

II.3.9. WAS THE CLASSIFICATION OF THE INFORMATION JUSTIFIED?

The Monitoring Committee of the Senate has requested the Standing Committee I to extend its investigation to the question of whether the classification introduced in the documents of the intelligence services was justified pursuant

classification principle; a second complaint, lodged with the Standing Committee P, targeting a particular section of a police service.

to the Act of 11 December 1998 on classification and security clearances, certificates and advice.

One must immediately point out the fact that the safety of informants of intelligence services is not part of the interests protected by Article 3 of the above-mentioned Act. The fulfilment of the assignments of the intelligence services is also not part of those interests.

Nevertheless, Article 18 of the Intelligence Services Act of 30 November 1998 states the following: "*In fulfilling its assignments, the intelligence and security services may enlist the help of human sources. In that case, these services must safeguard the safety of the information related to the human sources and the intelligence that they share*" (free translation). The Act therefore requires the intelligence services to safeguard '*the safety of the information related to the human sources*' and not the safety of the persons as such.

But in its *Activity Report 2004*, the Standing Committee I had stated that the obligation referred to in Article 18 of the Intelligence Services Act can only be respected by classifying the identity of informants.[153]

In practice, the intelligence services safeguard the safety of both the intelligence and the informants themselves by assigning a high level of classification to the information they receive from their human sources.

In casu, the Standing Committee I was of the opinion that the classification of the investigated documents was necessary and justified, in view of the legislation applicable to the intelligence services. No cases of misuse were found in this context.

II.4. THE GENERAL INTELLIGENCE AND SECURITY SERVICE AND THE PERFORMANCE OF A SECURITY INVESTIGATION

In the beginning of May 2007, a private individual strongly expressed his displeasure with the conduct of a security investigation by the military intelligence service. The investigation was with regard to his partner, who needed a security clearance for performing a particular position within the army. But because it involved a 'TOP SECRET' clearance, he also became a subject of investigation.[154] In addition, the investigators also inquired about the tax and commercial problems of his trading company. Especially this last point was

153 STANDING COMMITTEE I, *Rapport d'activités 2004*, 116-118.

154 Persons who have reached the age of eighteen and who live with a person requiring a 'TOP SECRET' security clearance are also subjected to a security investigation. They are not required to give their permission thereto; they are only informed of this (Article 16 § 4 of the Classification Act and the Directive of 16 February 2000 of the Ministerial Committee for Intelligence and Security).

considered unjustified by the complainant. But he also had numerous other complaints. He stated that he and his partner had separated and that he had allegedly withdrawn his 'permission' to include him in the investigation. He also complained about the manner in which they had been questioned, the fact that the investigation had apparently not been conducted in an objective manner and the fact that his file had been sent to the Minister of Defence.

Though the Committee decided that the complaint itself was admissible[155], it concluded that most of the complaints raised were without any substance.

Therefore, it was quite normal that further investigation was conducted into the company of which the complainant was the founder and partner, of which his then partner was the managing director and business manager, while the registered office of the company was located at the address of their joint place of residence. The information available on the complainant was such that it could, indeed, give rise to doubts about his reliability.[156] Since a further assessment could not be kept separate from his professional conduct, the Standing Committee I was of the opinion that the interest of the GISS in how the complainant managed his commercial activities within the company, was justified. Indeed, by personally inviting the complainant, the GISS had offered him the opportunity to explain the negative elements related to him.

But the complaint was also directed against this hearing itself. Firstly, the way in which both of them had been invited for an interview, was denounced: this was done by telephone and without them being informed of the reasons for the notification. The Standing Committee I found that there is no precise directive about the manner in which someone must be invited to such a hearing.[157] In general, nothing is communicated in advance about the content of the interview. The Committee felt, however, that it would have been more polite, clear and effective to have sent a personal invitation to the complainant, briefly explaining the reasons for the hearing. However, the Committee underlines the fact that no one is legally liable to act upon a request to attend a hearing issued by an intelligence service. Participation in such a hearing is entirely voluntary,

---

155 Article 3 of the Appeal Body Act states that "*when an appeal is brought before the Appeal Body, (…) the Standing Intelligence Agencies Review Committee (…) may not conduct, for the duration of the procedure, any investigation into, respectively, complaints and reports within the meaning of the aforementioned Act of 18 July 1991 (…) which is related to any security investigation or any security verification carried out as part of procedures in the context of security clearances, security certificates or security advice constituting the subject of that appeal*" (free translation). Since *in casu* no appeal was made and the complaint falls perfectly within the scope of the Review Act of 18 July 1991, the Committee was entitled to start this investigation. However, the investigation could not include the formulation of an advisory opinion about the validity of the decision taken (or to be taken) by the GISS in relation to the security clearance.

156 The thorough security investigation in relation to the woman had, however, not brought any negative elements to light.

157 However, the GISS does have internal directives specifying how the various other aspects of security investigations must be conducted.

although a refusal means that it is impossible for the investigators to gain a better understanding of any negative elements.

According to the complainant, the hearing itself could be compared to 'police interrogations'. The investigators from the GISS, however, claimed that the complainant had behaved in an arrogant and condescending manner from the start. From the detailed report drawn up of the hearing, it did seem that the mood was tense during the hearing. According to the Standing Committee I, this situation was due to the attitude of the complainant. But the Committee did not feel that the investigators were authoritarian, aggressive or impolite.

The complainant further claimed that the investigators displayed an unfavourable or even sexist bias towards his partner. The result of the security investigation *had to be* negative so in order to thwart her appointment. But the Standing Committee I could not find any evidence to that effect.

The complainant also protested against the fact that the report of the hearing was never presented or communicated to him and that he had not been able to sign it. The Standing Committee I pointed out that neither the Classification Act of 11 December 1998 nor the Implementation Decree of 24 March 2000 requires such formalities. A security investigation is not comparable to a criminal investigation.[158]

The complainant also disputed the fact that he was subjected to further investigation despite having withdrawn his 'permission' thereto. In this respect also, the complaint was unfounded. As mentioned, the Classification Act does not require the consent of cohabiting adult persons; they are merely informed of the fact that they will also be subjected to a security investigation.

Finally, the complainant condemned the fact that the security investigation file had been sent to the Minister of Defence. However, the Standing Committee I noted that this had happened at the request of the concerned Minister after the Minister had received a complaint letter from the complainant himself. Since the appointment of the woman in question was dependent on a decision of the Minister of Defence, it may appear perfectly normal to send the security file to the Minister. However, the Standing Committee I referred to Article 22 of the Classification Act, according to which the investigation report and file of an intelligence service are sent only to the security authority (*in casu* the Head of the GISS). This security authority is obliged to take the necessary internal measures to safeguard the confidential nature of the personal information contained in such files. Although one can hardly deny the Minister of Defence the right to consult the personal information of members of the armed forces, it can be questioned whether this also implies that the personal information of a person not under his authority (in this case, the partner) may be provided to him. Was it not sufficient in this case to send a copy of the reasoned decision of

158 The complainant did have, in principle, the opportunity to view the report on the basis of the Open Government Act of 11 April 1994.

whether or not to grant the security clearance, so the Minister of Defence could take his decision regarding the appointment of woman in question?

Besides the various components of the complaint, the Standing Committee I made two other comments.

Firstly, it appears that there is neither any Royal or Ministerial Decree nor any internal guideline that determines which positions within the Armed Forces require a security clearance. It was only in the security provisions of the GISS that the Committee found an explicit reference to the security clearance required for the position aspired to by the woman in question.

Secondly, the Committee concluded that none of the members of the GISS who conducted the hearing, were part of the Security Investigations Detachment. Yet Article 18 of the Classification Act specifies that security investigations may only be carried out by the members of the GISS who, on the recommendation of the Head of the GISS, have been specifically appointed by the Minister of Defence for this purpose. They then become holders of a specific identify card which they must display on simple request. However, the legal and regulatory provisions on security clearances and investigations do not make any of these formalities enforceable under penalty of nullity.

II.5. GATHERING AND PROCESSING INFORMATION ON PERSONS NOTICED IN THE NEIGHBOURHOOD OF MILITARY INSTALLATIONS

Mid-2008, a complaint of a private individual led to the initiation of an investigation into the reasons for and the manner in which State Security gathered and processed information on persons observed in the neighbourhood of a military complex.[159]

State Security was informed by the Federal Police of an allegedly suspicious act of the occupants of a vehicle that had stopped in the neighbourhood of this military site. State Security decided to gather further information regarding the incident.

Since, according to the members of State Security, this only involved an 'administrative investigation', the State Security employee entrusted with

[159] The complaint also had a 'police component', i.e. the possible description of the persons in question in the Central Descriptions Register (now Investigation and Information Bulletin). Since this is a database related to police matters, the Standing Committee I did not have any (investigative) authority in this matter. This aspect of the complaint was therefore transferred to the Standing Committee P. The Standing Committee P has informed the complainant that the necessary verifications had been carried out and that the situation was in line with the applicable regulations and legislation.

carrying out the investigation, contacted the owner of the vehicle by telephone. He identified himself, informed her of his position within State Security and asked her openly regarding the reasons for her vehicle being present in the neighbourhood of the military installation.

The Standing Committee I questioned the relevance of the method used by the State Security employee to carry out this investigation; namely (a) contacting the person who is the subject of the investigation by telephone and (b) identifying himself to the person concerned, notifying him of the reason for the investigation and giving the person a State Security telephone number for further contacts. The Committee was of the opinion that such conduct is not appropriate for an agent of the intelligence services. Revealing one's identity and position to persons who are the subject of an investigation may endanger one's own safety as well as the restraint which State Security agents are normally obliged to exercise when gathering intelligence information. The suspicious behaviour of the occupants of the car was sufficient reason to handle the so-called 'administrative investigation' being conducted against them with caution and with full discretion.

Finally, the Standing Committee I felt that an intervention by the local police of the place of residence of the owner of the vehicle would have been more appropriate in this case for obtaining the desired explanation from the persons concerned regarding the presence of their vehicle and the behaviour of the passengers near a military domain.

II.6. COLLABORATION BY STATE SECURITY IN A HOUSE SEARCH

Mid-February 2007, house searches were conducted in the judicial districts of Brussels, Nivelles and Verviers, in the context of a judicial inquiry into Muslim extremism. These were so-called 'house searches with reinforcements'.[160] This operation was described by certain media as being extremely brutal. The Standing Committee P, which monitors the police forces, was called in to investigate the manner in which the operations had been conducted.

In the context of this investigation, the Chairman of the Standing Committee P requested the Standing Committee I to verify whether the intelligence services had been contacted in advance in connection with this operation and, in particular, in connection with the suspected persons. Subsequently, the Standing Committee I initiated an investigation into '*the possible contribution of the intelligence services (whether or not) prior to the house searches conducted by the Federal Police on 16 and 17 February 2007*'.

[160] This is a house search in which assistance is provided by the special units of the Federal Police.

State Security reported that it had participated, in the context of its task of providing 'technical assistance (Article 20 of the Intelligence Services Act), in a coordination meeting of the examining magistrate and the Federal Prosecutor's Office. It stated that it had shared all its information at the meeting, in line with the protocol agreement between the intelligence services and the judicial authorities. However, State Security did not participate in the strictly operational phase.

But, since this concerned a judicial case, State Security referred to the secrecy of the investigation and did not wish to share – as in many other investigations – the reports it had sent to the judicial authorities.[161] Nevertheless, State Security emphasised the fact that it has never participated in the decision-making process and that it was not directly informed of the results of the house searches and of the problems faced by the Federal Police during those searches.

The Standing Committee I had shared the information at its disposal with the Standing Committee P. At the same time, it had been discussed whether a common investigation was required. In September 2009, however, the investigation of the Standing Committee P was completed, so that the Standing Committee I could also consider its investigation as closed.

II.7. COMPLAINT IN RESPONSE TO THE NON-RECOGNITION OF A MOSQUE

Early 2008, the members of management of a non-profit organisation associated with a mosque in Flanders approached the Standing Committee I. They wished to know the reason why their house of worship was being denied recognition. They assumed that this was possibly due to a negative advisory opinion from State Security and feared that this service was misinformed.

State Security had indeed provided information about this mosque to the Minister of Justice who, in his turn, had sent an advisory opinion to the Flemish Minister of Local Government.

The investigation of the Standing Committee I focused on two questions: had State Security acted in a lawful manner and was the intelligence sent to the Minister relevant?

[161] Although *in casu*, within the precise framework of the investigation requested by the Standing Committee P, it was not necessary to continue the investigation in this area, the fact remains that the Standing Committee I was again restricted in its review of the intelligence services.

II.7.1. LEGAL BASIS FOR THE COMMUNICATION OF INTELLIGENCE

State Security does not have any authority with regard to the recognition of religious communities (such as mosques); it also does not provide any advisory opinions in this regard. Decisions are taken by the competent regional government (*in casu*, the Flemish Minister of Local Government) and advisory opinions are given by the Minister of Justice. These opinions may contain elements '*that concern the security of the state and the maintenance of law and order*' (Article 3 §1 of the Cooperation Agreement of 27 May 2004[162]). It is obvious that for this the Minister can rely on information provided by State Security. The legal basis for this transfer of information is defined in Article 19 of the Intelligence Services Act. This provision states that State Security may share relevant information obtained in the context of its normal intelligence assignment (i.e. a potential extremist threat to the internal and external security of the state and to the continued existence of democratic and constitutional order) with all competent authorities '*in line with the objectives of their assignments*'. State Security was therefore entitled to send, at the request of the Minister of Justice, all relevant intelligence which could facilitate the assessment of the possible risks that the place of worship might signify for the security of the state and the maintenance of law and order. Relevant intelligence in the context of mosques is information which, according to State Security, is related to:

- the ideological profile of the imam;
- the possible existence of extremist elements among the mosque management;
- the possible existence of extremist elements among the worshippers;
- the general tenor of the preaching;
- the tenor of possible lessons and courses organised by the mosque;
- the possible structural links or occasional contacts of the mosque with extremist groups and/or foreign powers;
- the relationships with other mosques and mosque unions;
- the attitude of the mosque with respect to civil society in general and the local government in particular.

[162] Cooperation Agreement of 27 May 2004 between the Federal Government, the Flemish Region, the Walloon Region and the Brussels-Capital Region concerning the recognition of the religious orders, the salaries and pensions of ministers of religious orders, the church councils and the organisations responsible for managing the assets of the recognised religious orders (*BOJ* 14 June 2004), meanwhile replaced by the Cooperation Agreement of 2 July 2008 (*BOJ* 23 July 2008).

II.7.2. RELEVANCE OF THE ELEMENTS COMMUNICATED TO THE MINISTER OF JUSTICE

State Security prepared three memoranda for the Minister of Justice. The wording used showed evidence of caution and neutrality. Moreover, the first two memoranda followed very shortly after the request for information. The service therefore responded very promptly to the ministerial request. The third memorandum followed almost a year later. The successive memoranda contained qualifications and 'recent information'. Despite this, certain observations need to be made.

In drawing up the first memorandum, the assessment service of State Security based itself on information which was almost five months old and which was clearly related to a temporary situation. Yet the field services were not asked to update the information.

In the second memorandum, which *quasi* immediately followed the first, 'recent information' was reported. This concerned the identity of the imam of the mosque. But apparently that person had already held this position for one and a half years. This fact must have been known during the drafting of the first memorandum because the 'ideological profile of the imam' was obviously an important criterion in the assessment of the ideological profile of a mosque (see above). The Standing Committee I was, therefore, of the opinion that the assessment services had not operated optimally in this regard. But this was equally true for the field services, as they had informed the assessment services only one and a half years after the appointment of the Imam. The Committee therefore asked itself whether the field services were aware of the criteria for assessing the ideological profile of a mosque and whether they paid constant attention to keeping their information up-to-date.

Finally, the third memorandum only mentioned one change of imam, while the field services had already reported several changes of imams. Moreover, when comparing the reports of the field services and those sent by the assessment services to the Minister of Justice, it appeared that there was a noticeable difference in the assessment of the imam. Therefore, the final product delivered by State Security to the Minister of Justice certainly lacked accuracy, both in terms of being 'current' as well as in terms of 'nuance'.

In this regard, State Security stated that an update is requested from the field services only when the analyst considers this useful and opportune. Here, factors such as the reliability of the available information and the time play a role. *In casu*, no update was requested because the assessment services considered the issue of the concerned mosque to be sufficiently known. This proved to be a false assessment. The Standing Committee I also looked into the way in which this case had been monitored. The Committee found it surprising that the field services are not automatically informed, let alone consulted, in case of

'applications for recognition' from local religious communities. According to the Committee, there seems to be an obvious need for this.

II.7.3. CONCLUSIONS

The Standing Committee I was of the opinion that State Security had acted fully within its statutory mandate in this case. The Committee also noted that the criteria used by State Security in assessing the ideological profile of a mosque, are relevant. However, it appeared that the efficiency and internal coordination of the service could be improved.

With regard to this case, it was concluded that the first assessment sent to the Minister, although generally correct, was based on intelligence that was no longer up to date. Subsequently, more recent information gathered by the field services was not taken into consideration, whereas this would have made it possible to provide useful details to the Minister.

This situation was caused by the speed with which State Security sought to respond to the Minister's request for information. All things considered, this situation also seemed to be the result of the applied methodology. This led the Committee I to decide that there is a structural dysfunction in the information chain.

Indeed, it has not been proved that the field services of State Security would be systematically informed and consulted whenever the assessment services were requested to provide useful intelligence to the Minister for the purpose of obtaining an advisory opinion regarding the security of the State or the maintenance of law and order as a result of an application for recognition by a religious community.[163]

Therefore, the Standing Committee I was of the opinion that in this case the collection, assessment and provision of intelligence was not adequately organised to be able to anticipate and adapt to the information needs of the competent Minister.

II.8. COMPLAINT AGAINST AN OFFICER OF THE GENERAL INTELLIGENCE AND SECURITY SERVICE

In July 2008, the Standing Committee I received a complaint from a private individual against a public prosecutor, the Federal Police, a governor and an officer of the military intelligence service. Naturally, the Committee stated that it

163 *Ditto.*

was only competent with regard to the latter person and initiated an investigation '*into the complaint of a private individual against an officer of the GISS*'. The officer in question had allegedly carried out actions which had prevented the complainant from developing his commercial activities.

After investigating the elements submitted by the complainant, the Committee decided that there was no serious indication that the officer had acted in an illegal or improper manner. The Committee therefore decided to close this investigation and file the complaint.

II.9. INVESTIGATION INTO ALLEGATIONS AGAINST THE DIRECTOR OF THE CUTA

In September 2009, an anonymous complaint was sent to the Committee. Mention was made of several problems with regard to the operation of the CUTA, problems that had arisen since the arrival of the new director. It was said that the director did not show much interest in his service and took many trips outside Europe. He was said to be mainly concerned with matters that had nothing to do with the operation of the CUTA and had even made some dubious purchases.

Therefore, the Standing Committees P and I initiated a joint investigation into these allegations.

However, after questioning various concerned parties within the CUTA and from the analysis of the necessary documents, no dysfunction could be established. The file was therefore closed in 2009.

II.10. INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2009 AND INVESTIGATIONS INITIATED IN 2009

This section contains a list and a brief description of all the investigations started in 2009 and of the investigations which continued during the operating year 2009 but could not be completed as yet. Some investigations take a lot of time, sometimes even several years. Unfortunately, this is not only because of the nature and complexity of those investigations. There are two external causes which are outside the Committee's control. Firstly, there are investigations on subjects which are also being dealt with in the context of a criminal or judicial inquiry. In these cases, the Committee is dependent on the permission of the judicial authorities to inspect the information in the files. A second reason lies with the intelligence services. The Committee must sometimes wait several

months before it receives a (complete) response to its investigative questions. Such unnecessary delays are, of course, regrettable.

II.10.1. ESPIONAGE IN THE EUROPEAN JUSTUS LIPSIUS BUILDING

On 19 March 2003, the European Council revealed that its security services had found apparatus in the Justus Lipsius building in Brussels which made it possible to eavesdrop on various delegations, including those of Spain, Germany, France, Italy, the United Kingdom and Austria.

However, the Council was unable to find out who was responsible for the installation of the electronic apparatus connected to certain telephone lines. In response to a series of countermeasures and a prior internal investigation, the Deputy Secretary-General of the European Council lodged a complaint with the Brussels Prosecutor's Office.

At the end of May 2006, it was decided to initiate an investigation '*into the manner in which the Belgian intelligence services (State Security and the GISS) intervened in response to a bugging case in the offices of the delegation of the European Council in Brussels*' (free translation). In view of the fact that State Security had been indicated as an expert for the relevant judicial inquiry, it felt that it could not respond to questions of the Standing Committee I.

It was only in the autumn of 2008 that the Standing Committee I was given the right to inspect the judicial dossier. In October 2009, State Security provided the Standing Committee I with all kinds of hitherto unknown documents (letters, internal memoranda and reports). The investigation of these turned out to be crucial and has made it possible for the Committee to reconstruct and understand the intervention of State Security.

In early December 2009, the Committee was able to finalise a draft report. This draft was submitted to the intelligence services (and the Federal Prosecutor's Office) for any possible comments. The final report, which was approved in March 2010, will be included in the Activity Report 2010.

II.10.2. INFORMATION MANAGEMENT AT THE MILITARY INTELLIGENCE SERVICE

At the end of November 2005, an investigation was initiated into the way in which the military intelligence service manages and uses the information it obtains. In this respect, the existing instructions were studied, and clarifications were sought regarding the way in which the GISS stores, manages and uses any personal information it obtains.

The initial reason for starting this investigation was that in an actual case, there had been a lack of information flow between the pillars *Intelligence* and *Counterintelligence* of the military intelligence service. The GISS had, however, announced plans to fundamentally change the structure of the service in order to solve this problem. From this perspective, it was obviously not advisable to conclude this investigation, and it was accordingly suspended in 2008 till after the implementation of the proposed reforms. In 2009, concrete plans were duly communicated to the Standing Committee I. In the beginning of 2010, the GISS was asked about the new state of affairs. The response of the GISS now revealed, however, that the reform was limited to a few small changes. The Standing Committee I has drawn its conclusions from this, which will appear in a subsequent report.

II.10.3. HARMFUL SECTARIAN ORGANISATIONS

State Security is required to pay attention to phenomena such as '*any individual or collective activity, developed at home or from abroad, which is related to espionage, interference, terrorism, extremism, proliferation, harmful sectarian organisations, criminal organisations (…)*'. These threats are individually defined in Article 8 of the Intelligence Services Act. For example, the concept of 'harmful sectarian organisation' is defined as '*any group having or claiming to have a philosophical or religious purpose and whose organisation or practice involves harmful illegal activities, causes harm to individuals or society, or impairs human dignity*' (free translation).

In the beginning of January 2007, the Standing Committee I decided to initiate an investigation '*into the manner in which State Security carries out its legal assignment with regard to harmful sectarian organisations, as stipulated in Articles 7 and 8 of the Intelligence Services Act*'.

The Standing Committee I intends to identify which organisations are monitored by State Security in this context and how are they monitored. The criteria used by the intelligence service to determine whether to consider a sectarian movement as dangerous, and the analyses sent by State Security to the authorities and their purpose will also be examined. Finally, the Standing Committee I wants to gain an insight into the human and material resources made available by State Security for this assignment.

In 2009, hearings were conducted with State Security and several specific questions were presented to this service. A preliminary report was drafted at the end of 2009; however, it has not yet been possible to finalise this due to the absence of some data.

II.10.4. PROTECTION OF COMMUNICATION SYSTEMS AGAINST POSSIBLE FOREIGN INTERCEPTIONS AND CYBER ATTACKS

The issue of protecting information and telecommunication systems managed via new IT technologies, has regularly come up for discussion in the Federal Parliament. The security of these systems is essential in an information society. In February 2010, State Security again warned the ministers and top officials about the risks related to the use of BlackBerries in exchanging political and/or confidential information.[164]

This is because the current interception possibilities form a possible threat not only for the security, military interests and economy of a country, but also for the fundamental rights and freedoms of citizens.

The Monitoring Committee of the Senate expressed the desire to be kept informed by the Standing Committee I regarding the manner in which the intelligence services monitor these developments. It also wished to receive an *update* of the Echelon Report presented by the Standing Committee I in 2000.[165]

All these elements resulted in the Standing Committee I deciding at the end of December 2007 to initiate an investigation into '*the manner in which the Belgian intelligence services consider it necessary to protect the communication systems against foreign interception*' (free translation).

This investigation was started in 2008 and numerous investigative actions were undertaken. The Committee did not focus so much on the actual facts leading to the initiation of the investigation, but rather on the general issue of securing communication systems against possible foreign interceptions. Since then, the investigation has also been extended to threats from cyber attacks.

In 2009, the remarks of the intelligence services were included in an initial interim report, various briefings were organised and additional investigative acts were undertaken. The final report, which will include the views of the National Security Authority (ANS/NVO), is scheduled for completion in 2010.

II.10.5. PROTECTION OF CLASSIFIED INFORMATION ON NON-SECURE SITES

Mid-December 2007, the Standing Committee I decided to initiate an investigation into '*the manner in which the GISS protects classified information*

---

164 Question of P. Wille to the Minister of Justice on 'BlackBerries – Easy interception of e-mail traffic – Advice of State Security – Measures' (Senate, 2009–2010, 1 December 2009, Q. no. 4–5097).

165 See STANDING COMMITTEE I, *Rapport d'activités 2000*, 'Synthesis report of the investigation into the manner in which the Belgian intelligence services respond to the possible existence of an American system, named Echelon, for the interception of telecommunications in Belgium', 29–59.

and/or personal data on non-secure sites' as a result of several incidents in which such data had been lost. The aim of the investigation was to examine the procedures applied with regard to security. In 2009, there was a need for additional intelligence. The completion of the investigation was therefore postponed to 2010.

II.10.6. ANONYMOUS COMPLAINT AGAINST ALLEGED ILLEGAL SURVEILLANCE OPERATIONS CONDUCTED BY STATE SECURITY

The Standing Committee I received an anonymous complaint in February 2009 mentioning a current surveillance operation of State Security that could be problematic in light of earlier recommendations formulated by the Standing Committee I.[166] According to the complainant, a certain person had been placed under observation each time his case was handled by the judicial authorities. It was alleged that there was no legal basis for this.

The Committee decided to initiate an investigation in this regard in the beginning of March 2009. The investigative actions in the context of this file were completed at the end of 2009; the final report has meanwhile been approved.

II.10.7. A PLANNED FOREIGN MISSION BY THE CUTA

The Standing Committee I learned that the Coordination Unit for Threat Assessment had planned a foreign mission in the course of 2009 which, however, had been abandoned at the last minute.

In the plenary session of the Standing Committees I and P of June 2009, it was decided to initiate a joint investigation into this proposed mission. Although the mission in question had been cancelled, both Committees considered it useful for the future to determine whether – in general – undertaking certain foreign missions is a part of or results from the tasks assigned to the CUTA by the legislator. The investigation also aims at verifying whether the CUTA took, internally as well as externally, the necessary preparations and precautions for the purposes of coordination and effectiveness and whether these were adapted to the specific situation of the country to be visited. In 2009, various investigative actions were undertaken.

166 Cf. 'The Erdal Case' and 'The Kimyongür Case', resp. pp. 16–26 and pp. 43–53 of the *Activity Report 2006* of the Standing Committee I.

II.10.8. INVESTIGATION INTO THE MANNER IN WHICH THE BELGIAN INTELLIGENCE SERVICES HAVE OPERATED IN A CASE INVOLVING EXPORT TO IRAN

Mid-May 2009, the Minister of Environment and Energy was questioned in the House of Representatives about the export of an isostatic press for graphite to Iran.[167] The Advisory Committee for the Non-Proliferation of Nuclear Weapons (CANVEK/CANPAN) had apparently given a negative advice after reviewing an earlier positive advice, on the basis of additional information which suggested that this material would be used for nuclear purposes. Regardless of the response of the Minister – which gave a more nuanced picture – the claimant requested the President of the Senate to investigate this dossier. The President of the Senate, in turn, instructed the Standing Committee I to carry out an investigation into '*the role of State Security in this file and where possible verify whether the review procedures have been followed*'. Since, '*(…) past experiences compel us to be extremely vigilant in this matter*'.[168]

Since the Standing Committee I is not authorised to deliver an opinion regarding the advice given by CANVEK/CANPAN or on the merits of the decisions taken by the competent authorities in the area of export of material that is subject to a specific control, the investigation was reduced to the question of whether the Belgian intelligence services were in possession of relevant information and analyses regarding the ordering of material by the Iranian company, and if so, whether they had communicated this information and assessments via the appropriate channels to the competent authorities.

The investigation '*on the operation of State Security and the GISS with regard to the export of material to Iran*' was completed at the end of 2009 and submitted to both intelligence services for any comments. The final report will be sent to the principal in the course of the 2010.

---

167 Question from T. Van der Straeten to the Minister of Climate and Energy regarding 'the export of material to Iran' (Deliberations, House of Representatives, 2008–2009, 15 May 2009, COM 557, 15, Q. no. 13174).

168 Cf. 'Investigation into the manner in which the company EPSI was possibly monitored by the intelligence services in the context of the fight against proliferation', in STANDING COMMITTEE I, *Rapport d'activités 2005*, 16–33 and 'The role of the intelligence services within the framework of the fight against the proliferation of non-conventional and very advanced weapons', in STANDING COMMITTEE I, *Activity Report 2008*, 43–57.

II.10.9. ASSESSMENT OF THE MANNER IN WHICH STATE SECURITY PERCEIVES ITS ROLE WITH REGARD TO THE FIGHT AGAINST PROLIFERATION AND THE PROTECTION OF THE SCIENTIFIC AND ECONOMIC POTENTIAL

The Standing Committee I had already conducted various investigations into the manner in which the intelligence services carry out the fight against proliferation[169] and the protection of the scientific and economic potential (SEP).[170] In both these matters, State Security has an extremely important role to play with respect to the various government services. But the intelligence provided by State Security or the manner in which this intelligence information is used, can lead to adverse consequences for (legal) persons. Moreover, the interests with regard to the fight against proliferation and those with regard to the protection of the SEP do not always necessarily coincide. With this investigation, the Standing Committee I wants to determine, on the basis of an actual case, whether State Security has worked meticulously in this context. The chosen case offers the opportunity to carry out an assessment that covers a fairly long period.

In the course of 2009, various questions were asked to State Security. The answers are still awaited. The investigation could therefore not be completed as yet.

II.10.10. COMPLAINT OF TWO PRIVATE INDIVIDUALS IN THE CONTEXT OF THE 'DECLARATION OF NATIONALITY' PROCEDURE

In September 2009, two private individuals filed a complaint with the Standing Committee I. The complainants, both foreigners, stated that they had submitted an application for acquiring the Belgian nationality in June 2009 which, however, was rejected. Information received from State Security was allegedly the reason for this refusal.

The Standing Committee I limited its investigation to the information collected, processed and provided by State Security to the public prosecutor in the context of the application for acquisition of Belgian nationality, since the Standing Committee I is not authorised to verify or assess the advisory opinions and decisions of judicial authorities.

The investigative actions were completed in the course of 2009 and a final report was drafted in early 2010.

---

169 See for example, *Rapport d'activités 2005*, 16–33 and *Activity Report 2008*, 42–57.

170 See for example, *Activity Report 2008*, 60–66, *Rapport d'activités 2005*, 37 and *Rapport d'activités 2005,* 102–146.

II.10.11. INFORMATION POSITION OF STATE SECURITY WITH REGARD TO THE RIOTS IN BRUSSELS

At the end of December 2009, the President of the Senate requested the Standing Committee I to initiate an investigation '*into the monitoring by State Security and the GISS of the phenomena/group(s)/persons behind the riots in the capital in 2009, and the weapons possessed by (the) persons involved in these riots*'. In 2009, activities on this investigation were limited to notifying the various responsible Ministers regarding the initiation of the investigation and sending a request to the relevant departments for further information. The investigation will be continued in 2010.

II.10.12. BELGIAN REPRESENTATION IN INTERNATIONAL MEETINGS ON TERRORISM

The Belgian police and intelligence services and the CUTA regularly participate in binational or multinational meetings on the fight against terrorism. The question arises, however, whether the participation in these meetings is organised efficiently and effectively and the extent to which there are coordinated agreements regarding this. To answer this question, in November 2009 the meeting of the Standing Committees I and P decided, in accordance with Article 53, 6° of the Review Act, to initiate a joint investigation into '*the participation in international meetings on the fight against terrorism by the Belgian police and intelligence services, the CUTA and the supporting services of the CUTA*'. The aim is to complete this investigation in 2010.

II.10.13. PROBLEMS RELATED TO THE HOUSING OF THE PROVINCIAL POSTS OF STATE SECURITY

In the context of its investigation into 'harmful sectarian organisations' (cf. II.10.3) the Standing Committee I could *de visu* establish that the state of some buildings in which the provincial posts of State Security are housed, was pitiful. The continuing delays in rectifying this problem are not part of the responsibility of State Security. However, the failure to create a proper working environment for everyone within State Security can certainly affect the efficiency of this service. Therefore, at the end of December 2009, the Standing Committee I decided to officially initiate an investigation into '*the housing of some of the provincial posts of State Security*'. The results of this investigation are expected in the course of 2010.

CHAPTER VIII
RECOMMENDATIONS

Based on the investigations concluded in 2009, the Standing Committee I has formulated the following recommendations. These relate in particular to the protection of the rights which the Constitution and the law confer on individuals (VIII.1), to the coordination and efficiency of the intelligence services, the CUTA and the supporting services (VIII.2) and finally, to the optimisation of the review capabilities of the Standing Committee I (VIII.3).

VIII.1. RECOMMENDATIONS WITH REGARD TO THE PROTECTION OF THOSE RIGHTS WHICH THE CONSTITUTION AND THE LAW CONFER ON INDIVIDUALS

VIII.1.1. A LEGAL REGULATION FOR SCREENING (POTENTIAL) INFORMANTS

The Standing Committee I is of the opinion that a legal framework must be developed which allows the intelligence services to use special intelligence methods for assessing the reliability of an informant. The deployment of such methods could form an essential element in the implementation of risk analyses. That is why the Committee had previously recommended the creation of a legal basis for *screening* informants not only prior to their recruitment, but also during their 'activities'.[171] The Standing Committee I reiterates this recommendation.

VIII.1.2. ROLE OF THE MINISTERS IN CASE OF SECURITY INVESTIGATIONS

The investigation into the manner in which the military intelligence service had conducted a security investigation[172] revealed that the Minister of Defence had

171 STANDING COMMITTEE I, *Activity Report 2008*, 86.
172 See Chapter II.4, *Activity Report 2009*.

requested a security file after he had received a letter of complaint. The results of the security investigation were of interest to the Minister because they could be decisive for an appointment decision.

However, according to Article 22 of the Classification Act, an investigation report and file belonging to an intelligence service may only be sent to the security authority (*in casu* the Head of the GISS). This security authority is obliged to take the necessary internal measures to safeguard the confidential nature of the personal information contained in such files. Although one can hardly deny the Minister of Defence the right to consult the personal information of members of the armed forces under his authority, it can be questioned whether this also means that this right extends to the personal information of a third person (in this case, a partner of a member of staff). The Standing Committee I wondered whether it was not sufficient to send a copy of the reasoned decision of whether or not to grant the security clearance to the Minister, to help him take the decision of whether or not to appoint the person in question.

The Committee therefore recommends that the role of the Minister of Defence (as well as that of the Minister of Justice) with regard to the procedure for granting security clearances for personnel under his (their) authority be clarified in the Royal Decree of 24 March 2000 on classification and security clearances, certificates and advice.

VIII.1.3. SECURITY INVESTIGATIONS CARRIED OUT BY STAFF MEMBERS APPOINTED THERETO

The same investigation showed that the security investigation was only partially carried out by staff members of the GISS who had been specifically appointed thereto. This, however, is a requirement based on Article 18, second paragraph of the Classification Act. The Standing Committee I therefore recommends that the GISS ensure in future that only staff members who have the statute of 'security investigator' are entrusted with the responsibility of carrying out the security investigations.

VIII.2. RECOMMENDATIONS CONCERNING THE COORDINATION AND EFFICIENCY OF THE INTELLIGENCE SERVICES, THE CUTA AND THE SUPPORTING SERVICES

VIII.2.1. RECOMMENDATIONS BASED ON THE AUDIT AT STATE SECURITY

The recommendations formulated by the Standing Committee I as a result of the performance audit[173], were subdivided into four topics: leadership, information management, work processes and satisfaction with quality. Considering the focus of the audit, these recommendations are directed solely at State Security. State Security needs to pay constant attention to these aspects. Where necessary, the period within which a recommendation must be realised, was indicated. A distinction was made between the short term (six months to one year) and the medium-long term (one to two years).

VIII.2.1.1. Recommendations related to leadership

VIII.2.1.1.1. Strategic management

- With a view to the formulation of its strategic objectives, an assessment must be made, based on a thorough SWOT analysis, of the current status of the organisation (strengths and weaknesses) and what lies ahead (opportunities and threats). The result of this SWOT analysis should be documented.
- As specified in Article 3 of the Royal Decree on State Security, a formal action plan for the realisation of a Strategic Plan should be presented each year to the Minister of Justice. This plan should contain the following elements: the strategic objectives; a draft staffing plan; an estimate of the budgetary requirements; the general rules for the organisation and the proper functioning of the services and an evaluation of the work performed by the Support Cell.
- The strategic objectives must be always translated into measurable and concrete operational objectives which meet the SMART principle. The objectives at the lower levels must be aligned to the objectives at the higher levels and must always support these. The individual objectives (of the directors, their deputies, the pillar heads, the section heads), which emerge directly from the operational objectives of the organisation, must be defined in the short term.

---

173 See Chapter II.1, *Activity Report 2009*.

- In the short term, a plan must be drawn up for internal and external communication, including SMART objectives.
- Strategic and action plans must be drafted on a project basis and developed according to a well-founded project management methodology. In the context of these projects, the management committee should keep the following elements in mind: write out in detail the requirements (the Strategic Plan, the action plan…) to be met by the final product; identify the concerned parties and specify the responsibilities and powers; select a project manager; specify a start date and a feasible end date; list obstacles, limitations and initial risks; prepare a formalised and approved project plan; document discussions and decisions; monitor capabilities; compare interim results with the proposed quality standards; test the final product (such as the Strategic Plan and the action plan) against predetermined acceptation criteria; build up and archive project documentation; evaluate the project in its totality.
- The principles of risk management should be systematically applied at the strategic as well as at the operational level (including monitoring and evaluation), and for this a standardised method for identifying internal and external risks should be used.
- The management must intensively promote the mission, vision and strategic and operational objectives among the internal stakeholders.

VIII.2.1.1.2. Performance management

In the area of performance management, firstly a plan must be drawn up in the short term, in which it is specified what, why, for whom and when management information is required. Based on the management information needs, a measurement and monitoring system must be implemented in the medium-long term. This provides the opportunity to regularly monitor and evaluate the workload of various entities, in order to detect and remedy more quickly any possible under- or over-loading. The measurement results should be incorporated in reports which make it possible to specify responsibilities with regard to the functioning of the organisation and to adjust these in time. It must be decided to which internal (and external) target groups the reports on the realisation of the objectives must be directed as well as the form of these reports.

VIII.2.1.1.3. Management of values

State Security must invest more efforts in creating a general positive work climate. This should be done by:

- carrying out a gap analysis between the prevailing culture and the desired organisational culture in order to outline and implement the necessary cultural transformation(s) in the medium-long term;

– developing codes of conduct and behaviour for leaders, managers and employees with regard to teamwork and leadership in the medium-long term;
– implementing the code of ethics in the short term.

VIII.2.1.1.3. Management of professionals

– In the medium-long term, job descriptions must be drawn up for the department commissioners responsible for special units.
– The management must involve its personnel more closely in change projects, in order to create the necessary support and utilise all the available expertise.
– The HRM objectives must be formally monitored, evaluated and – if necessary – adjusted by the HRM manager(s).
– The competencies for *all* positions in the assessment services and the general services must be defined in the medium-long term.
– In the short term, a training plan must be developed for the internal services as well as for the field services; this plan should be focused on removing the difference between the present and desired competencies.
– In the medium-long term, the management must explain the HRM policy for competency development to the staff members.
– The HRM Cell should be expanded in the medium-long term.
– In the medium-long term, an objective evaluation system must be made applicable to all the personnel in the organisation. The individual objectives emerging from the evaluation must be formulated in specific and measurable terms with mention of a timing. The management must give each staff member regular feedback about how the job is performed and give the staff member the freedom to also give feedback.
– The retention and transfer of knowledge, if an employee is temporarily absent or leaves the organisation permanently, must be ensured.
– For the appointment of a staff member in a particular position, care should be taken to externalise the objectivity of the applied criteria.
– The times for recruitment and training must be better aligned to one another.

VIII.2.1.2. Recommendations related to information management – Knowledge management

The management must regularly interview users of ICT applications regarding the effectiveness and user-friendliness of the IT applications with a view to their optimisation.

In the short term, a 24-hour on-call service should be set up for the operational centre.

VIII.2.1.3. Recommendations related to the work processes – Process management

In the short term, a process manager should be appointed for the management and implementation of the management, core and supporting processes. This full-time position should be assigned exclusively to one employee and not to a team.

In addition, all primary processes must be defined in the short term. The core and supporting processes should be defined in the medium-long term. These should be drawn up such that the objectives and mission are achieved (within the proposed or specified period). In drawing up processes, one must take into account the needs and expectations of internal and external stakeholders.

In the short term, a process manager should be appointed for each work process and the processes should be regularly evaluated with a view to adjusting and redefining these, if necessary.

VIII.2.1.4. Recommendations related to satisfaction with quality – Quality management

A quality manual should be drafted in the medium-long term.

In the short term, the external stakeholders and their needs and expectations should be outlined. There must also be a clear code that specifies how to conduct a dialogue with external stakeholders and defines the boundaries of this dialogue.

VIII.2.2. A CLEAR, COMPREHENSIVE DIRECTIVE FOR WORKING WITH INFORMANTS

In the context of the Belliraj case[174], the Standing Committee I concluded that the guidelines regarding working with informants are scattered across various documents which only give a fragmented picture of the subject matter. This is even more problematic now that informant operations only have a very limited legal basis (Article 18 of the Intelligence Services Act). Despite the Standing Committee I having repeatedly called, partly as a result of the discussions on the Act on methods of collection of information by the intelligence and security services, for further legislation in this area[175], no such legislative initiative has been taken.

---

174 See Chapter II.3, *Activity Report 2009*.

175 STANDING COMMITTEE I, *Activity Report 2006*, 79 and Advice of the Standing Committee I on the Special Intelligence Methods Act.

For these reasons, the Standing Committee I recommends that State Security further develops and clearly defines its internal directives and best practices with regard to informants in its memoranda. It would be advisable to combine all relevant regulations in a single coordinated memorandum.

In particular, more attention should be paid to a formal risk assessment with a listing of the various risks, for which one works along with a person or department who/which was not involved in preparing the initial recruitment proposal. This is done in order to arrive at more critical and objective presentation of the facts.

This critical attitude should be present with respect to the recruitment and the annual evaluation as well as the reports in the informant file. This should enable the service to constantly question its attitude towards the informant. It should also give State Security staff insight into the (possible) risks related to the cooperation with a particular informant. Finally, this should enable them to verify, in case of incidents, whether the risks had been sufficiently assessed and draw lessons from this, if necessary.

The Standing Committee I will verify which initiatives are taken by State Security in this regard.

VIII.2.3. A CONSIDERATION FOR CERTAIN INFORMANTS

The Standing Committee I recommends that State Security considers the advisability of – in absolutely exceptional cases and provided there is a thorough democratic control – providing the option of granting a fixed consideration to informants who could have information crucial for the security of the constitutional state. At present, only a financial compensation may be granted to informants. In some case, a different 'concession' may be more appropriate. Without anticipating the outcome of the debate, the Committee is thinking, for example, of a naturalisation or a residence permit. A similar regulation already exists under the witness protection scheme, where the government can assign a new identity to certain persons in exchange for their testimony.

The Standing Committee I reiterates, however, that such a possibility may only be considered provided there is a clear legal framework with thorough in-built democratic control, in order to exclude or detect any possible misuse. Also, the possibility should be left open for withdrawing the 'favour' if the informant misuses the situation.

VIII.2.4. A LEGAL REGULATION FOR CIVILIAN INFILTRATORS

An informant is sometimes managed or controlled such that, at certain times, he starts acting as a civilian infiltrator who is assigned actual intelligence

assignments (e.g. foreign missions and infiltration within an organisation to which he does not belong). This form of gathering intelligence is even more problematic in several respects than the 'normal' informant operations. Here, the Standing Committee I is thinking about the safety of the person concerned and the possibility of him being 'enticed' to commit illegal acts. Moreover, the possibilities for the service to control the way in which its 'assignments' are fulfilled are also limited.

The Standing Committee I therefore reiterates its recommendation that a legal regulation be defined in this regard.[176] In the meantime, the intelligence services should include this issue in their directives.

VIII.2.5. A COOPERATION AGREEMENT BETWEEN POLICE AND INTELLIGENCE SERVICES

Despite repeated recommendations[177], the Standing Committee I finds that there is still no protocol agreement between State Security and the police services, whereas these services are required to combine their forces in the fight against terrorism and radicalism and they are not allowed to regard each another as competitors.

The Standing Committee I is of the opinion that no solution can be found for the existing tensions between the two services as long as a clear division of tasks and regulations related to the exchange of information are not agreed upon.

VIII.2.6. APPOINTMENT AS 'SECURITY INVESTIGATOR'

The investigation into the manner in which the military intelligence service had carried out a security investigation[178] showed that certain investigative actions had been taken by staff members of the GISS who were not specifically appointed thereto in conformity with Article 18 of the Classification Act. According to the preparatory activities of the Classification Act, agents authorised to carry out such investigations may also be deployed for other investigations. Consequently, it is not impossible to award the statute of 'security investigator' to members of the GISS who are not part of the 'Security Investigations' detachment.

Therefore, the Standing Committee I recommends that the GISS award such a statute to the staff members of other detachments who can be involved in the hearing of persons in the context of security investigations.

---

176 See STANDING COMMITTEE I, *Activity Report 2006*, 79.

177 See STANDING COMMITTEE I, *Activity Report 2006*, 135 and STANDING COMMITTEE I, *Activity Report 2007*, 76.

178 See Chapter II.4, *Activity Report 2009*.

VIII.2.7. ADJUSTMENT OF THE INFORMATION POSITION ACCORDING TO THE NEEDS OF THE COMPETENT AUTHORITIES WITH REGARD TO APPLICATIONS FOR RECOGNITION BY RELIGIOUS COMMUNITIES

In view of the information needs of the Minister of Justice for issuing an advisory opinion regarding the security of the State and the maintenance of law and order in case of an application for recognition by a religious community, the Standing Committee I recommends that State Security ensures that it systematically updates the information collected by it on this matter.

With this in mind, State Security must ensure that its concerned sections and provincial posts systematically provide the necessary updates when they are consulted by the Minister of Justice for the purpose of issuing an advisory opinion to a regional authority in the context of an application for recognition by a religious community. This recommendation emerges from the investigation into the role of State Security in the recognition of a mosque.[179]

VIII.2.8. SUPERVISION IN THE CONTEXT OF THE ASSESSMENT[180]

The Standing Committee I is of the opinion that State Security should arrange for the supervision of the – sometimes undoubtedly difficult – choices facing analysts so that the accuracy of the final product is maximally ensured.

VIII.3. RECOMMENDATIONS CONCERNING THE EFFECTIVENESS OF THE REVIEW

VIII.3.1. HEARING OF FORMER MEMBERS OF INTELLIGENCE SERVICES AND OF THE CUTA

Article 48 of the Act of 18 July 1991 governing the review of police forces and intelligence services and of the Coordination Unit for Threat Assessment allows the Chairman of the Standing Committee I to instruct the bailiff to summon members of the intelligence services, the CUTA and its supporting services. If necessary, they are bound to testify after having taken the oath prescribed in

179 See Chapter II.7, *Activity Report 2009*.
180 See Chapter II.8, *Activity Report 2009*.

Article 934, paragraph 2 of the Judicial Code. They are, in principle, also obliged to answer the questions asked by the Committee as part of the investigation.

However, it is not possible to issue a summons to former members of these services. As evident from the investigation resulting from the complaint made by Baron de Bonvoisin,[181], it can be considerably important to question these persons in order to establish the truth. The Standing Committee I therefore recommends that Article 48 of the Review Act be modified in this respect.

181 See Chapter II.2, *Activity Report 2009*.

ANNEX

18 JULY 1991
ACT GOVERNING REVIEW OF THE POLICE AND INTELLIGENCE SERVICES AND OF THE COORDINATION UNIT FOR THREAT ASSESSMENT

[Valid from 1 January 2008 until 31 December 2009]

CHAPTER I – GENERAL PROVISIONS

Article 1

Both a Standing Police Services Review Committee and a Standing Intelligence Agencies Review Committee shall be established. In particular, review shall relate to:

1° The protection of the rights conferred on individuals by the Constitution and the law, as well as the coordination and effectiveness of the police services on the one hand and the intelligence and security services on the other;

2° The protection of the rights conferred on individuals by the Constitution and the law, as well as the coordination and effectiveness of the Coordination Unit for Threat Assessment;

3° The way in which the other supporting services satisfy the obligation laid down in Articles 6 and 14 of the Act of 10 July 2006 on threat assessment.

An Investigation Service shall be established for each of these committees.

Art. 2

The review governed by this Act does not relate to judicial authorities nor to the actions taken by them in the exercise of the prosecution function. The review does not relate to the administrative police authorities either.

The review referred to in this Act is governed without prejudice to the review or inspection governed by or by virtue of other legislation. In the event of review or inspection governed by or by virtue of other legislation, the review referred to

in this Act relating to the activities, methods, documents and directives of the police services and of the intelligence and security services, shall only be undertaken to ensure fulfilment of the assignments provided for in this Act.

Art. 3
For the purposes of this Act, the following definitions shall apply:
1° "Police services": in addition to the Local Police and the Federal Police, the services that come under the authority of the public authorities and public interest institutions, whose members have been invested with the capacity of judicial police officer or judicial police agent;
2° "Intelligence and security services": State Security and the General Intelligence and Security Service of the Armed Forces;
3° "Coordination Unit for Threat Assessment": the service referred to in the Act of 10 July 2006 on threat assessment;
4° "Other supporting services": the services other than the police services and the intelligence and security services referred to in this Act, that are required, in accordance with the Act of 10 July 2006 on threat assessment, to pass on information to the Coordination Unit for Threat Assessment;
5° "Threat Assessment Act": the Act of 10 July 2006 on threat assessment;
6° "Ministerial Committee": the Ministerial Committee referred to in Article 3, 1° of the Act of 30 November 1998 governing the intelligence and security services.

Shall be equated to police services for the purposes of this Act, the people who are individually authorised to detect and establish criminal offences.

CHAPTER II – REVIEW OF THE POLICE SERVICES

This chapter that concerns review of the police services by the Standing Committee P is not reproduced.

CHAPTER III – REVIEW OF THE INTELLIGENCE SERVICES

SECTION 1 – THE STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE

Subsection 1 – Composition

Art. 28
The Standing Intelligence Agencies Review Committee, hereinafter referred to as the "Standing Committee I", shall consist of three full members, including a Chairman. A substitute shall be appointed for each of the members. They shall all

be appointed by the Senate, who may dismiss them if they perform one of the functions or activities or hold one of the positions or mandates referred to in paragraph 4, or for serious reasons.

The Standing Committee I shall be assisted by a secretary.

At the time of their appointment, the members and their substitutes shall satisfy the following conditions:
1° Be Belgian;
2° Enjoy civil and political rights;
3° Have attained the age of 35 years;
4° Reside in Belgium;
5° Hold a Bachelor of Law degree and demonstrate at least seven years' relevant experience in the field of criminal law or criminology, public law, or management techniques, acquired in positions related to the operation, activities and organisation of the police services or of the intelligence and security services, as well as having held positions requiring a high level of responsibility;
6° Hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.
The members and their substitutes may not hold a public elected office. They may not perform a public or private function or activity that could jeopardise the independence or dignity of the office. They may not be members of the Standing Police Services Review Committee, nor of a police service, an intelligence service, the Coordination Unit for Threat Assessment, or another supporting service.

The Chairman shall be a magistrate.

The decisions assigned to the Standing Committee I by this Act or other acts shall be taken in plenary session.

Art. 29
The secretary shall be appointed by the Senate, who may dismiss him or terminate his appointment in the cases referred to in Article 28, paragraph 4. At the time of his appointment, the secretary shall satisfy the following conditions:
1° Be Belgian.
2° Enjoy civil and political rights;
3° Have knowledge of the French and Dutch languages;
4° Have attained the age of 30 years;
5° Reside in Belgium;
6° Hold a Bachelor of Law degree;
7° Have at least two years' relevant experience;
8° Hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

Before taking up his duties, the registrar shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the President of the Senate.

Art. 30
The members of the Standing Committee I and their substitutes shall be appointed for a renewable term of five years. The term of the permanent members is only renewable twice. At the end of this term, the members shall remain in office until such time as they are replaced.

In the event of termination of the term of office by a member, the substitute shall complete that term. If a position of substitute member should become vacant, the Senate shall appoint a new substitute member forthwith.

For the appointment of a substitute member, the conditions laid down in Article 28, paragraph 4, shall be verified by the Senate upon taking up his duties. Before taking up their duties, the members of the Standing Committee I shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the President of the Senate.

Subsection 2 – Definitions

Art. 31
For the purposes of this chapter, "the competent ministers" shall mean:
1° The minister responsible for National Defence, with regard to the General Intelligence and Security Service;
2° The minister responsible for Justice, with regard to State Security;
3° The minister responsible for a service referred to in Article 3, 2°, *in fine*;
4° The minister responsible for the Interior, with regard to the assignments of State Security relating to the maintenance of law and order and the protection of people, as well as the organisation and administration of State Security when that organisation and administration have a direct influence on the execution of assignments relating to the maintenance of law and order and the protection of people;
5° The Ministerial Committee, with regard to the Coordination Unit for Threat Assessment or the other supporting services.

In this chapter, "the competent authority" shall mean the director of the Coordination Unit for Threat Assessment.

Subsection 3 – Assignments

Art. 32
If the investigation concerns an intelligence service, the Standing Committee I shall act either on its own initiative, or at the request of the House of Representatives, the Senate, or the competent minister. If the investigation relates to the implementation of the Act of 10 July 2006 on threat assessment, the Standing Committee I shall act either on its own initiative, or at the request of the competent minister or the competent authority.

When the Standing Committee I acts on its own initiative, it shall forthwith inform the Senate thereof.

Art. 33
Within the framework of the objectives laid down in Article 1, the Standing Committee I shall investigate the activities and methods of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services, their internal rules and directives, as well as all documents regulating the conduct of the members of these services.

The intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services shall, on their own initiative, send to the Standing Committee I the internal rules and directives, as well as all documents regulating the conduct of the members of these services. The Standing Committee I and the Investigation Service for the intelligence services shall have the right to be provided with all texts that they consider necessary for the performance of their assignment.

The Standing Committee I shall provide the competent minister or the competent authority, as well as the Senate with a report on each investigation assignment. This report shall be confidential until its communication to the Senate in accordance with Article 35.

This report shall include the conclusions relating to the texts, activities or methods that could jeopardise the objectives laid down in Article 1.
The competent minister or the competent authority may, with regard to the investigation reports, hold an exchange of views with the Standing Committee I. The Standing Committee I may itself propose that such an exchange of views be held.

The competent minister or the competent authority shall inform the Standing Committee I within a reasonable period of time of his/its response to its conclusions.

The Standing Committee I may only advise on a Bill, Royal Decree, Circular Letter, or any documents expressing the political orientations of the competent ministers, at the request of the House of Representatives, the Senate, or the competent minister.

When the Standing Committee I acts at the request of the competent minister, the report shall only be submitted to the Senate at the end of the term laid down in accordance with Article 35, 3°. The Chairman of the Monitoring Committee concerned referred to in Article 66*bis* shall be informed of the request of the minister to the Standing Committee I and of the content of the report before the end of the term laid down in Article 35, 3°.

Art. 34
Within the framework of the objectives laid down in Article 1, the Standing Committee I deals with the complaints and denunciations it receives with regard

to the operation, the intervention, the action or the failure to act of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services and their personnel.

Without prejudice to the provisions of Article 46, the Standing Committee I may decide not to follow up a complaint or a denunciation that is clearly unfounded. It may delegate this responsibility to the Head of the Investigation Service for the intelligence services.

The decision of the Standing Committee I not to follow up a complaint or denunciation and to close the investigation shall be justified and communicated to the party who made the complaint or denunciation.

When the investigation is closed, the results shall be communicated in general terms.

The Standing Committee I shall inform the managing officer of the intelligence service, the director of the Coordination Unit for Threat Assessment, or the managing officer of the other supporting service, depending on the case, of the conclusions of the investigation.

Art. 35

The Standing Committee I shall report to the House of Representatives and the Senate in the following cases:

1° Annually, through a general activity report, which shall include, if applicable, conclusions and proposals of a general nature, and which shall cover the period from 1 January to 31 December of the preceding year. This report shall be sent to the Presidents of the House of Representatives and the Senate, and to the competent ministers by 1 June at the latest.

2° When the House of Representatives or the Senate has entrusted it with an investigation.

3° When at the end of a period that it believes to be reasonable, it notes that no action has been taken concerning its conclusions, or that the measures taken are inappropriate or inadequate. This period may not be less than sixty days.

Art. 36

In order to prepare their conclusions of a general nature, the House of Representatives and the Senate may request the Standing Committee I to provide each and every investigation dossier, according to the terms and conditions that they determine and which in particular aim to safeguard the confidential nature of these dossiers and to protect the privacy of individuals. If the investigation was initiated at the request of a competent minister, his consent shall be required before handover of the investigation dossier, unless the term laid down in Article 35, 3° has expired.

Art. 37
After acquiring the advisory opinion of the competent ministers or the competent authority, the Standing Committee I shall decide, within a period of one month from the request for advice, to make public all or part of its reports and conclusions, according to the terms and conditions it stipulates.

The reports and conclusions made public shall include the advisory opinion of the competent ministers and the competent authorities.

Art. 38
The Prosecutor-General and the Auditor-General shall ex-officio send to the Chairman of the Standing Committee I a copy of the judgments and judicial decisions relating to the crimes or offences committed by the members of the intelligence services and the Coordination Unit for Threat Assessment.

The public prosecutor, the labour prosecutor, the federal prosecutor or the prosecutor-general of the Court of Appeal, depending on the case, shall inform the Chairman of the Standing Committee I whenever a criminal or judicial investigation into a crime or offence is initiated against a member of an intelligence service or the Coordination Unit for Threat Assessment.

At the request of the Chairman of the Standing Committee I, the prosecutor-general or the auditor-general may provide a copy of the deeds, documents or information relating to criminal proceedings against members of the intelligence services and the Coordination Unit for Threat Assessment for crimes or offences committed in the execution of their duties.

However, if the deed, document or information concerns an ongoing judicial inquiry, it may only be communicated with the consent of the examining magistrate.

The copies shall be delivered without charge.

Art. 39.
The Standing Committee I shall exercise its authority over the Investigation Service for the intelligence services, assign investigations to it, and receive reports on all investigations that are carried out.

However, when they perform a judicial police assignment, the Head and the members of the Investigation Service for the intelligence services shall be subject to review by the prosecutor-general of the Court of Appeal or the federal prosecutor.

SECTION 2 – THE INVESTIGATION SERVICE FOR THE INTELLIGENCE SERVICES

Art. 40

By order of the Standing Committee I or, except with regard to the Coordination Unit for Threat Assessment and the other supporting services, on its own initiative, in which case it shall immediately inform the Chairman of the Standing Committee I, the Investigation Service for the intelligence services, hereinafter referred to as the "Investigation Service I", shall supervise the operations of the intelligence services, the Coordination Unit for Threat Assessment and the other supporting services, through investigations, within the limits of Article 1.

It shall examine the complaints and denunciations of individuals who have been directly concerned by the intervention of an intelligence service, the Coordination Unit for Threat Assessment or another supporting service. Any public officer, any person performing a public function, and any member of the armed forces directly concerned by the directives, decisions or rules applicable to them, as well as by the methods or actions, may lodge a complaint or file a denunciation without having to request authorisation from his superiors.

On its own initiative or at the request of the competent public prosecutor, military public prosecutor or examining magistrate, it shall, together with the other officers and agents of the judicial police, and even with a right of priority over them, investigate the crimes and offences which the members of the intelligence services and the Coordination Unit for Threat Assessment are charged with. With regard to the members of the other supporting services, this provision only applies with respect to the obligation laid down by Articles 6 and 14 of the Act of 10 July 2006 on threat assessment.

If the person filing a denunciation so wishes, his anonymity shall be guaranteed. In this event, his identity may only be disclosed within the Service and to the Standing Committee I.

Art. 41

A person may not be appointed Head of the Investigation Service I if he has not been a magistrate or a member of an intelligence or police service for a period of five years, or if he cannot demonstrate at least five years' relevant experience as a public servant in positions relating to the activities of the intelligence or police services. At the time of his appointment he must have attained the age of 35 years.

The Head of the Investigation Service I shall be appointed by the Standing Committee I for a term of five years, renewable twice.

Before taking up his duties, the Head of the Investigation Service I shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the Chairman of the Standing Committee I.

He must have knowledge of the French and Dutch languages.
He shall retain his right to advancement and salary increase.
He may be dismissed by the Standing Committee I.

Art. 42
The Head of the Investigation Service I shall manage it and set out the tasks.

He shall be responsible for relations with the Standing Committee I, from which he shall receive the assignments and to which he shall send the reports.

He shall be responsible for relations with the judicial authorities, from which he shall receive the requests and to which he shall send the reports referred to in Article 46.

Art. 43
Except for the cases laid down by Articles 40, paragraph 3, and 46, the Head of the Investigation Service I shall inform the competent minister or the competent authority that an investigation is initiated.

He shall send a report to the Standing Committee I at the end of each investigation assignment.

However, in the cases referred to in Articles 40, paragraph 3, and 46, the report shall be limited to the information necessary for the Standing Committee I to perform its assignments.

Art. 44
The members of the Investigation Service I shall be appointed and dismissed by the Standing Committee I on the recommendation of the Head of the Investigation Service I.

At least half of the members, and this for a renewable term of five years, shall be seconded from an intelligence or police service or an administration in which they have acquired at least five years' experience in positions relating to the activities of the intelligence or police services.

The members of the Investigation Service I shall take the same oath as the Head of the Service.

In the service or administration that they have been seconded from, they shall retain their right to advancement and salary increase.

Art. 45
The Head and the members of the Investigation Service I shall have the capacity of judicial police officer, assistant public prosecutor and assistant military public prosecutor.

In order to be appointed, they must hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

Art. 46
When a member of the Investigation Service I has knowledge of a crime or offence, he shall produce a formal report that is forthwith sent by the Head of the Investigation Service I to the public prosecutor, to the military public prosecutor, or the examining magistrate, depending on the case.

The person who lodged the complaint or filed the denunciation, or the authority who called upon the Standing Committee I, shall be informed thereof by the Head of the Investigation Service I.

Art. 47
When a member of the Investigation Service I observes facts during an investigation that could constitute a disciplinary offence, the Head of the Investigation Service I shall forthwith inform the competent disciplinary authority thereof.

SECTION 3 – INVESTIGATION PROCEDURES

Art. 48
§1. Without prejudice to the legal provisions relating to the immunity and privilege, the Standing Committee I and the Investigation Service I may summon for hearing any person they believe useful to hear.

The members of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services which are being heard may testify about facts covered by professional secrecy.
§2. The Chairman of the Standing Committee I may have members of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services summoned through the medium of a bailiff. The members of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services are bound to testify after having taken the oath prescribed by Article 934, paragraph 2 of the Judicial Code.

The members of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services are bound to disclose to the Standing Committee I the secrets that they know of, except if those secrets relate to an ongoing criminal or judicial inquiry.

If the member of the intelligence service, the Coordination Unit for Threat Assessment, or the other supporting services is of the opinion that he must not disclose the secret he has knowledge of because its disclosure would risk exposing a person to physical danger, the question shall be submitted to the Chairman of the Standing Committee I, who shall rule, or, if it concerns a member of the Coordination Unit for Threat Assessment or another supporting service, the Chairmen of the two Standing Committees, who shall rule jointly.

§3. The Standing Committee I and the Investigation Service I may request the collaboration of interpreters and experts. They shall take the oath in the way used in the Assize Court. The remuneration due to them shall be paid in keeping with the rates for fees in civil cases.
§4. Article 9 of the Act of 3 May 1880 on parliamentary investigations shall apply to the members of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services who are heard or summoned by the Standing Committee I as witnesses, and to the experts and interpreters who are called upon.

The formal reports establishing the offences committed before the Standing Committee I shall be drawn up by the Chairman and sent to the prosecutor-general of the Court of Appeal in the district where they were committed.

The members of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services who refuse to testify before the Standing Committee I, and the experts and interpreters who refuse to collaborate, shall be liable to imprisonment of between one month and one year.

Art. 49
The members of the Investigation Service I may request the assistance of the forces of law and order in the performance of their assignments.

Art. 50
Any member of a police service who observes a crime or offence committed by a member of an intelligence service shall draw up an information report and send it to the Head of the Investigation Service I within a period of fifteen days.

Art. 51
The members of the Investigation Service I may make all observations in any location.

They may at all times, in the presence of their Head of Department, or his substitute, and of the chief of police, director or senior civil servant concerned, or his replacement, enter the premises where members of an intelligence service, the Coordination Unit for Threat Assessment or other supporting service perform their duties, in order to make substantive observations. In these locations, they may confiscate any objects and documents useful to their investigation, except for those relating to an ongoing criminal or judicial inquiry. If the chief of police or his substitute is of the opinion that the confiscation of classified information would constitute a threat to the performance of the assignments of the intelligence and security services referred to in Articles 7, 8 and 11 of the Act of 30 November 1998 governing the intelligence and security services, or would risk exposing a person to physical danger, the question shall be submitted to the Chairman of the Standing Committee I, who shall rule. If the director or the senior civil servant or his replacement is of the opinion that the confiscation of classified information

would constitute a threat to the performance of the assignments of the intelligence and security services referred to in Articles 7, 8 and 11 of the Act of 30 November 1998 governing the intelligence and security services, or would risk exposing a person to physical danger, the question shall be submitted to the Chairmen of the two Standing Committees, who shall rule jointly. The confiscated objects and documents shall be recorded in a special register kept for this purpose.

CHAPTER IV – JOINT MEETINGS OF THE STANDING POLICE SERVICES AND INTELLIGENCE AGENCIES REVIEW COMMITTEES

Art. 52
The Standing Committees shall exchange information on their activities and send each other the reports and conclusions referred to in Articles 9, 11, 33 and 35.

At least twice a year, they shall hold joint meetings, during which additional information may be exchanged.

Art. 53
During their joint meetings, the Standing Committees shall jointly perform their assignments (laid down in Articles 9, 10, 11, 33, 34 and 35):
1° With regard to the public services that perform both police and intelligence assignments;
2° With regard to the division of the assignments and the coordination of the operation between the police services on the one hand, and the intelligence services on the other;
3° With regard to any question put to them, either by a joint request from the ministers responsible for the Interior, Justice and National Defence, or at the request of the House of Representatives or the Senate;
4° With regard to any question that each Standing Committee believes does not fall within its exclusive competence;
5° With regard to any question considered by a Standing Committee to be sufficiently important to warrant a joint meeting;
6° With regard to the Coordination Unit for Threat Assessment or another supporting service.

A report shall be produced jointly by the Standing Committees at each joint meeting. This report may include advisory opinions and recommendations. It shall be sent as stipulated in Articles 9, 11, 33 and 35.

Art. 54
These joint meetings shall be chaired alternately by the Chairmen of the Standing Committees.

The functions of the secretariat of the joint meetings shall be performed by the longest serving secretary or, in the event of equal length of service, by the youngest secretary.

Art. 55
During the joint meetings, the Standing Committees may decide to assign investigation assignments to the two Investigation Services or to either one of them. They shall receive the reports on all the investigations that are carried out.

CHAPTER V – COMMON PROVISIONS

Art. 56
Each Standing Committee shall examine the complaints that are lodged with it by its former members or by former members of the Investigation Services who believe they have been subject to prejudicial measures because of the functions they have carried out in the Standing Committees or in the Investigation Services.

Art. 57
The funds required for the operation of the Standing Committees and the Investigation Services established by this Act shall be imputed to the appropriations budget.

The Chairmen, the members and the secretaries of the Standing Committees, as well as the Director-General of the Investigation Service P and the Head of the Investigation Service I shall enjoy exemption from postal charges for official business.

Art. 58
Each Standing Committee shall appoint and dismiss the members of its administrative staff, on its own initiative or at the proposal of the secretary.

It shall have authority over the members of its staff. It may delegate all or part of this authority to its Chairman or to the secretary.

The Director-General of the Investigation Service P and the Head of the Investigation Service I shall have authority over the members of their administrative staff.

Art. 59
The travel and subsistence expenses of the Chairman, the members and the registrar of each Standing Committee, the Director-General of the Investigation Service P, the Head of the Investigation Service I and the members of these services shall be determined according to the provisions applicable to the public services.

Art. 60

Each Standing Committee shall adopt its rules of procedure. The rules of procedure for the joint meetings shall be adopted jointly by the two Standing Committees.

The rules of procedure of the Standing Committee P shall be approved by the House of Representatives. The rules of procedure of the Standing Committee I shall be approved by the Senate.

The rules of procedure for the joint meetings shall be approved by the House of Representatives and by the Senate.

In accordance with paragraphs 2 and 3, the House of Representatives and the Senate may amend the rules of procedure after acquiring the advisory opinion of the Standing Committee concerned. The advisory opinion shall be deemed favourable if it has not been given within sixty days of the request.

Art. 61

§1. The members of the Standing Committees shall enjoy the same status as the councillors of the Court of Audit. The rules governing the financial statute of the councillors of the Court of Audit, contained in the Act of 21 March 1964 on the remuneration of the members of the Court of Audit, as amended by the Acts of 14 March 1975 and 5 August 1992, shall apply to the members of the Standing Committees.

The members of the Standing Committees shall enjoy the pension scheme applicable to the civil servants of the General Administration. The following special conditions shall also apply.

The pension may be granted as soon as the person concerned has attained the age of fifty-five years. It shall be calculated on the basis of the average remuneration of the last five years, in proportion to one twentieth per year of service as a member of the Standing Committee.

A member who is no longer able to perform his duties due to illness or infirmity, but who has not attained the age of fifty-five years, may retire irrespective of his age. The pension shall be calculated according to the method laid down in the preceding paragraph.

The services that do not fall under the regulations referred to in paragraphs two to four and that qualify for the calculation of a state pension, shall be taken into account in application of the laws governing the calculation of the pensions for these services.

§2. Unless he has been dismissed, the member of a Standing Committee shall, when his duties are terminated or if his term of office is not renewed, receive a fixed severance grant equivalent to the gross monthly salary of the last eighteen months.

If this severance grant is granted before expiry of the first period of five years, it shall be reduced accordingly.

The following are excluded from this allowance:

1° The members to which Article 65 applies.
2° The members who were members of a police service or an intelligence and security service before their appointment to the Standing Committee and who rejoin this service.
§3. The secretaries of the Standing Committees shall enjoy the same statute and pension scheme as the secretaries of the Court of Audit.

Article 365, §2, a), of the Judicial Code shall apply to the secretaries of the Standing Committees.

Art. 61*bis*
The Chairman of each Standing Committee shall, in accordance with the principle of collective responsibility, preside the meetings of that Committee and assume the day-to-day management of its activities. He shall ensure the application of the rules of procedure, the proper functioning of the Committee, as well as the proper performance of its assignments. He shall also ensure that the performance of the judicial police assignments does not impede the performance of the investigations. To this end, he shall hold the necessary consultations with the competent judicial authorities.

Art. 62
Under the supervision of the Standing Committee in question, the secretary of each Committee shall assume the secretariat of the Committee meetings, draw up the minutes of the meetings, ensure the sending of documents, and the preservation and protection of the secrecy of the documentation and archives. He shall manage the administrative staff, insofar as the authority over them has been delegated to him in accordance with Article 58, paragraph 2, and the infrastructure and equipment of the Committee, prepare its budget, and keep the accounts.

Art. 63
The members of the Standing Committees are prohibited from attending the deliberations on affairs in which they have a direct or personal interest, or in which relatives by blood or marriage to the fourth degree inclusive, have a direct or personal interest.

Art. 64
The members of the Standing Committees, the secretaries, the members of the Investigation Services, and the administrative staff shall be obliged to preserve the secrecy of the information that comes to their attention in the performance of their duties. The obligation of confidentiality shall also apply after they leave office.
Without prejudice to Article 458 of the Penal Code, they shall be liable to imprisonment of between eight days to one year, and a fine between one hundred francs and four thousand francs, or only one of these penalties, if they divulge

these secrets in circumstances other than those stipulated by law or by the rules of procedure.

Art. 65
§1. Articles 1, 6, 1 and 12 of the Act of 18 September 1986 instituting political leave for the members of staff of the public service shall apply, where appropriate and with the necessary adaptations, to members of the Standing Committees.
§2. Members of the judiciary may be appointed as members of the Standing Police Services Review Committee and as members of the Standing Intelligence Agencies Review Committee, and as Director-General of the Investigation Service P or Head of the Investigation Service I.

Article 323*bis*, paragraph 3, of the Judicial Code shall apply if a magistrate from the public prosecutor's office is a chief of police.

Art. 66
Excluding its Chairman, each Standing Committee shall have as many French-speaking members as Dutch-speaking members.

The Chairman of one of the Standing Committees shall be French-speaking, the Chairman of the other Dutch-speaking.

Art. 66*bis*
§1. The House of Representatives and the Senate shall each create a permanent committee responsible for monitoring the Standing Committee P and the Standing Committee I respectively.

The House of Representatives and the Senate shall stipulate in their respective regulations, the rules relating to the composition and functioning of each monitoring committee.
§2. Each monitoring committee shall supervise the operation of the Standing Committee concerned, and ensure observance of the provisions of this Act and the rules of procedure.

The monitoring committee of the House of Representatives shall also perform the assignments assigned to the House of Representatives by Articles 8, 9, 11, 1°*bis*, 2° and 3°, 12, 32, paragraph 1, 33, paragraph 7, 35, 2° and 3°, 36 and 60.

The monitoring committee of the Senate shall also perform the assignments assigned to the Senate by Articles 8, paragraph 1, 9, paragraph 7, 11, 1°*bis*, 2° and 3°, 12, 32, 33, 35, 2° and 3°, 36 and 60.
§3. The permanent committees shall sit together in order to:
1° Examine the annual reports of the Standing Committees before their publication, in the presence of their members. The conclusions of the monitoring committee shall be attached to the reports;
2° Examine the draft budget of the Standing Committees;
3° Supervise the operation of the Standing Committees in the cases referred to in Articles 52 to 55.

They may also sit together to analyse the results of an investigation requested by the House of Representatives to the Standing Committee I or by the Senate to the Standing Committee P.

§4. Each monitoring committee shall meet at least once per quarter with the Chairman or the members of the Standing Committee concerned. It may also meet at the request of the majority of the members of the monitoring committee, or at the request of the Chairman of the Standing Committee, or at the request of the majority of the members of the Standing Committee.

Every denunciation by a member of the Standing Committee concerned relating to the inadequate functioning of that Standing Committee, the non-observance of this Act, or the rules of procedure, may be brought before the monitoring committee.

The monitoring committee may issue recommendations to the Standing Committee concerned, or to each of its members, relating to the functioning of the Standing Committee, the observance of this Act, or the rules of procedure.

§5. The members of the monitoring committees shall take the necessary measures to safeguard the confidential nature of the facts, acts or intelligence that they have knowledge of by virtue of their position, and shall be subject to an obligation of confidentiality. They shall be obliged to preserve the secrecy of any information that comes to their attention in the performance of their duties. The obligation of confidentiality shall also apply after they leave office.

Any violation of this obligation of confidentiality shall be penalised in accordance with the rules of the Chamber they belong to.