ACTIVITY REPORT 2006
ACTIVITY REPORT 2007

ACTIVITY REPORT 2006
ACTIVITY REPORT 2007
Investigations and Recommendations

Belgian Standing Intelligence Agencies
Review Committee

Belgian Standing Intelligence Agencies Review Committee

intersentia
Antwerp – Oxford – Portland

Activity Report 2006. Activity Report 2007. Investigations and Recommendations
Belgian Standing Intelligence Agencies Review Committee

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

ISBN 978-90-5095-841-7
D/2008/7849/80
NUR 823

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ATG	Mixed Anti-Terrorist Group (*Antiterroristische gemengde groep – Groupe interforces anti-terroriste*)
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)*
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 (*Wet 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*)
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*)
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*)

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*)
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)*
State Security	State Security (*Veiligheid van de Staat – Sûreté de l'État*)
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 its military counterpart, the General Intelligence and Security Service. In addition, it supervises the functioning of the Coordination Unit for Threat Assessment and its 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 for a period of five years – renewable twice. 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 at the request of the Senate, the House of Representatives or the competent minister or authority. Additionally, the Standing Committee I can act at the 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 2006 and 2007 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, Board Member
Peter De Smet, Board Member
Wouter De Ridder, Secretary

1 July 2008

ACTIVITY REPORT 2006

TABLE OF CONTENTS OF THE COMPLETE ACTIVITY REPORT 2006

CHAPTER VI.
THE ADMINISTRATION OF THE APPEAL BODY FOR SECURITY CLEARANCES, CERTIFICATES AND ADVICE

APPENDICES

PREFACE

2006 was an eventful year for the Belgian intelligence community: Fehriye Erdal's escape, a new Director-General for State Security, the CIA using European airports to transport terror suspects, U.S. authorities having access to personal banking information from SWIFT, the alleged cooperation of State Security in the arrest of Bahar Kimyongür in the Netherlands, etc.

At such times, the need is felt more than ever for independent and external review. Such review should focus as much on legitimacy (guaranteeing in particular the protection of those rights which the Constitution and the law confer on individuals) as on effectiveness (in particular the coordination and effectiveness of the intelligence and security services), whilst giving equal weight to transparency and secrecy. Achieving an equitable balance between these conflicting requirements is no easy matter. Yet this is the challenge that the Standing Committee I seeks to address.

In the wake of the establishment of the Coordination Unit for Threat Assessment (CUTA) in 2006, the Standing Committee I was charged with an important additional task, as the CUTA and its supporting services were placed under the common review of the Standing Committee I and the Standing Committee P.

2006 was also a year in which the composition of the Standing Committee I changed: Jean-Claude Delepière was replaced as Chairman at his own request, Peter De Smet joined as a board member and Gérald Vande Walle's mandate was extended.

But does such a change in composition signal a new approach? As regards form: definitely. The present activity report bears witness to this. The exhaustive descriptions were abandoned and an attempt was made to outline the essence of the investigations.

But the Standing Committee I wishes to shift its strategy regarding content as well as form. Previously, the operation of the review body may have been perceived as a model where the interests of the *supervisors* and the *supervised* differed fundamentally. As of now, the Standing Committee I wishes to represent a model in which both parties recognise each other's value and communicate on the basis of equality. No energy is therefore wasted through fear and mutual distrust. The philosophy at the basis of this approach is the continuing acceptance of and respect for each other's position, within the framework of each other's legal assignments. Such trust and confidence is not easily obtained and incidents are

bound to occur during this process. But it would go a long way if all parties could embrace the views of Tristan d'Albis, of the *École Nationale d'Administration française*: "*Le contrôle externe des services [de renseignements], loin d'être une sanction, serait, pour eux, tant un gage de modernité qu'un signe indubitable de reconnaissance*".[1]

Guy Rapaille,
Chairman of the Belgian Standing Intelligence
Agencies Review Committee

1 June 2007

[1] T. D'ALBIS and P.-A. MIQUEL, "Au service de l'État", *Magazine des Anciens Elèves de l'ENA*, file Le Renseignement, 2006, October, n° 365, 2–3 ("*The external supervision of the [intelligence] services should, far from being a sanction, be proof to them of both a modern approach and an undeniable sign of recognition.*" – free translation).

CHAPTER II.
INVESTIGATIONS

With the Review Act of 1991, the Belgian legislator created the Standing Committee I as a body that exercises an external and independent review on the intelligence and security services. The Standing Committee I, its Investigation Service and its secretary have been given a number of assignments: they provide advice about legislation and regulations concerning the intelligence services; they are charged with the review of security interceptions by the General Intelligence and Security Service of the Armed Forces (GISS); they sometimes carry out criminal investigations; they are the registry of the appeal body for security clearances, certificates and advice; and they carry out investigations regarding the operations of the two intelligence services.[2] In addition, the Standing Committee I investigates the general operation of these services and, if applicable, reports shortcomings or dysfunctions of the system, the structures, the methods or the interventions of the intelligence services, and it formulates proposals for remediation. The present chapter covers the handling of these investigations.

With regard to such investigations, the Standing Committee I may decide to intervene on its own initiative, at the request of Parliament or the competent minister (the Minister of Justice with regard to State Security and the Minister of Defence with regard to the military intelligence service) or on the basis of a complaint.[3]

Ten investigations were initiated in 2006: two at the request of the monitoring committees of the House of Representatives and the Senate (investigations that were carried out jointly with the Standing Police Monitoring Committee), two at the request of the monitoring committee of the Senate, two on the initiative of the Standing Committee I itself, and four as a result of a complaint by a member of the public.

In total, the Standing Committee I dealt with 17 investigations during 2006. In other dossiers, no investigation activities were conducted because they were suspended or because a judicial inquiry was ongoing.

With regard to the year 2006, six dossiers were completed.

---

2 As of 1 December 2006, the scope of competence of the Standing Committee I was extended to include the review of the CUTA and its supporting services.

3 If such an investigation concerns the implementation of the Act of 10 July 2006 on threat analysis, the Standing Committee I may intervene either on its own initiative, or at the request of the competent minister or competent authority.

In the following, the completed investigations are discussed in chronological order.

II.1. THE ERDAL CASE

II.1.1. GENERAL CONTEXT

In 1996, Ozdemir Sabanci, a member of a family of industrialists in Turkey, was murdered together with two other persons in the offices of the Sabanci Holding in Istanbul by a commando of the Revolutionary People's Liberation Party/Front (DHKP-C).[4] At the time of this triple murder, Fehriye Erdal, a woman of Turkish nationality, was working for a cleaning agency that was responsible for the maintenance of the offices of the holding. She is accused of letting the murderers in and of bringing them to the floor where the office of Ozdemir Sabanci was located.

F. Erdal disappears without a trace until the end of September 1999, when she is arrested together with other militants of the DHKP-C during the discovery of a clandestine cell in Knokke (Belgium). She is accused of belonging to a criminal organisation, arms possession, forgery, and use of forged documents, and she is locked up in the Bruges prison.

From that moment, an especially complex administrative, judicial and political situation develops around her person. There is, after all, not only the judicial inquiry and a pre-trial detention; there are also the request for extradition by the Turkish government[5] and F. Erdal's application for recognition as political refugee.

F. Erdal is eventually released, both within the framework of the pre-trial detention and within the framework of the extradition procedure. However, she is not effectively released. The Minister of the Interior decides to place her at the Government's Disposal, in execution of Article 52*bis* of the Aliens and Immigration Act.[6] At the end of July 2000, however, it becomes apparent that an extension of this custodial title will not be permitted for much longer by the judiciary. In addition, F. Erdal's health condition was deteriorating as a result of a hunger strike. Eventually it was decided to oblige her to stay in a certain place pending

---

4 See also Chapter II.4. The Kimyongür case.

5 That request was repeated several times. Belgium has, however, always refused to accede to this demand. A real judicial procedural fight developed around the issues and problems of the extradition, which resulted in new legislation (the Act of 22 December 2003, which was intended to make it possible to prosecute Erdal for acts committed prior to 2003) and a number of judgments of principle by the Constitutional Court (judgment no. 73/2005 dated 20 April 2005) and the Court of Cassation (judgment dated 27 June 2006, P.05.1491.N).

6 Act of 15 on the entry, residence, settlement and expulsion of foreign nationals (Aliens and Immigration Act).

the outcome of the asylum procedure[7] (Article 22 and 52*bis*, §3, Aliens and Immigration Act). A number of conditions were attached to the assignment of such a permanent place of residence, as a result of a global agreement between the government on the one hand, and F. Erdal and her lawyers on the other hand. F. Erdal was thus only permitted to leave her place of residence (except for medical reasons) if a written permission had been granted by the Minister, and she had to see to it that she could be reached at her place of residence at all times.[8]

In preparation of her release, a meeting is held at the cabinet of the Minister of the Interior in August 2000. State Security also takes part in this meeting. State Security is given the assignment to conduct a surveillance assignment in close cooperation with the Rijkswacht/Gendarmerie.[9] Since that day, State Security has been involved to a greater or lesser extent in the surveillance of F. Erdal. In the beginning, a member of the service was posted outside the residence of F. Erdal; this static surveillance post was quickly reduced to one or two cameras; at times the service was charged with controlling compliance with the imposed conditions; in the days before her escape, F. Erdal was permanently shadowed by an extensive team, etc. However, State Security has never made a secret of its dissatisfaction with these assignments. Quite to the contrary. The service repeatedly and emphatically requested to be relieved of these assignments.

As of August 2000 and up to the evening of her disappearance, several ministerial decrees were issued to impose permanent residence on the basis of the fact that she was a threat to public order and national security. F. Erdal is moved a large number of times (especially in the beginning) and on 28 February 2006, she is sentenced to four years in prison by the correctional court of Bruges.[10] Her immediate arrest is ordered and granted. On 27 February 2006, however, F. Erdal nevertheless managed to escape despite the surveillance.

---

7 The Minister of the Interior had already decided to deny her refugee status, but this decision was first suspended and later recalled by the Council of State on the grounds that a better motivation had to be provided and that a host country had to be assigned for Erdal.

8 Erdal also commits herself not to undertake any political activities in Belgium, to arrange for her own security and to waive the offered police protection. On the issue of the investigation of the Erdal case, a 'secret agreement' between the Minister of the Interior and Erdal's lawyers was mentioned on several occasions. On the assumption that this concerns a written agreement, neither of the Committees has received such a document. The Standing Committee I nevertheless considers it possible that the above-mentioned agreements were later viewed by some persons as a 'secret agreement', being subsequently also termed as such.

9 This is the former Federal Police service.

10 The sentence of four years' effective imprisonment was confirmed by the Court of Appeal in Ghent. On 19 April 2007, however, the judgment was annulled by the Court of Cassation on procedural grounds. There is still no final decision in this case.

II.1.2. AN ASSIGNMENT FOR A JOINT INVESTIGATION

Both the Standing Committee I and the Standing Committee P had been charged by the Ministers of Justice and the Interior with the investigation of the manner in which State Security and the police service carried out their surveillance assignments within the scope of their applicable legal possibilities and taking into account the administrative situation of the person concerned. It quickly becomes clear that there is a substantial amount of vagueness around the decision of assigning an obligatory place of residence to F. Erdal. For instance, it is not always clear whether (and if so which) conditions were attached to these decisions. Other questions also arise, such as "Who was responsible for checking whether the conditions were being fulfilled?" or "Was it possible to institute sanctions if the conditions were not being fulfilled?".

The investigations by both Committees resulted in two separate reports. At the request of the parliamentary monitoring committees of the House of Representatives and the Senate, both Committees prepared a joint synthesis of the decisions and recommendations.

II.1.3. THE ROLE OF STATE SECURITY

For the exhaustive report of this long and complex history of the Erdal case, the Standing Committee I refers to its declassified report (in French and Dutch), which can be consulted on its website (www.comiteri.be). The present report confines itself to a brief summary of a number of key moments.

II.1.3.1. The period between the arrest and the assignment of a permanent place of residence

In December 1999, State Security already presented a report about a meeting that took place within the framework of the judicial inquiry that had been initiated after the arrest of the DHKP-C members in Knokke. At that time, there was no mention of (static or mobile) surveillance by State Security. From that date, however, the service issues memorandums that bear witness to the deadlock in which the involved authorities found themselves concerning this case (extradition or no extradition, the assignment of an obligatory place of residence, the search for a host country, etc.).

As of July 2000, State Security became more closely involved, and the Director-General at the time, ordered the service departments to follow up on the case of Mrs. Erdal (who at that time was still detained) and to obtain information from the Immigration Service about the evolution of her residential situation and the

decisions that had been taken in her case. On the other hand, there were good reasons for observing the reactions of the DHKP-C in Belgium. This, of course, was part of the general intelligence assignment of State Security.

In the middle of August 2000, the case takes a new turn. F. Erdal is released, but she is obligated to reside at a previously agreed address (see II.1.1). At a meeting, different services are given the following assignments: State Security[11] and the (then) Federal Police called Rijkswacht/Gendarmerie are charged with the surveillance of the defined address; the Rijkswacht/Gendarmerie and the Immigration Service must monitor that the imposed conditions are observed; and, finally, the Rijkswacht/Gendarmerie is made responsible for the security of F. Erdal.

About one month later, the physical presence of the member of State Security at the surveillance post is no longer required. This is possible, because the security presence of the Rijkswacht/Gendarmerie at F. Erdal's place of residence is strengthened. The property is, however, still subject to permanent surveillance with a camera, the pictures of which are viewed twice a week.

II.1.3.2. The period between December 2000 and February 2006

This long intervening period can best be summarised on the basis of the following assessments:

– The State Security agents do not always know whom they are observing or why. The Standing Committee I thus came to the conclusion that initially, only the then Director-General and the Director of Operations were informed about the context of this assignment;[12]

[11] The competent section of State Security was orally given the assignment by its superiors to install a surveillance post.

[12] Also at the end of November 2002, the commissioner who was in charge of the operation reported to his superiors that the objectives of the operation had never been precisely defined from the beginning. And in 2004, the following statement is made in a letter from the Director-General to the Minister: "*In the case that we are working on, my predecessor had been given the assignment by the then Minister of Justice to observe specified premises, without being able to reveal the reason for this operation, not even to State Security staff. State Security has been carrying out this 'blind assignment' for many years.*" (free translation).

- When State Security is informed about whom they must observe, it appears that they are not always informed about the exact place of residence of F. Erdal[13] or about her appearance;[14]
- The objective of the intervention by the intelligence service is not always clear and sometimes shifts. This lack of clarity did not only exist for the agents in the field and for the executive officials (who had requested clarification in writing at various times[15]), but also for the Standing Committee I itself. In addition, it was at some moments difficult to accommodate the objective of the intervention by State Security under the assignments assigned to the service by the legislator;[16]
- On numerous occasions, State Security requests to be relieved from this assignment, which it describes as "useless",[17] "exceedingly time-consuming"[18] and "not within their scope of competence".[19] These requests, however, are in vain: each of the consecutive Ministers of the Interior demand that the service

---

13 Already on 1 December 2000, a State Security report about developments regarding the DHKP-C in Belgium shows that the service no longer knew where Erdal had been housed. Barely a half year later, a new memorandum is sent to the competent ministers, in which the difficulties of localising Erdal are once more reported. Despite regular surveillance of the premises in which the information office of the DHKP-C is accommodated, it was not possible for the service to confirm that Erdal was staying at that address.

14 In 2002, the service reports the following: "*It is true that we have very little information on her physiognomy.*" In 2005, the following statement is released: "*State Security emphasises that it does not have any recent photographs of Erdal at its disposal and points out that she strongly resembles (…).*"(free translation).

15 For example, the Director-General informs the competent minister in 2004 that "*In this precise context (...) it (would be) more than ever fitting to redefine more formally the expectations of the executive power in this case and to rationalise the corresponding assignments of the various security services, and – on the other hand – to optimise their activities, taking into account their intrinsic characteristics.*" (free translation).

16 See II.1.4 for an analysis of the different objectives.

17 "*Although we were not 'objectively' asked to monitor F. Erdal, we can confirm that the surveillance post has never seen her.*" The surveillance post also appears to have been useless because it "*provides no additional operational element whatsoever*" (2003). "*Indeed, even though a surveillance post was installed in August 2000, the camera has never filmed the person concerned. She was seen for the first time on 23 February 2006, when she went to the hospital*" (2006). The Standing Committee I has no knowledge of any information or analyses that are based on these observations and that have been passed on to the competent authorities. That Committee must, however, point out that the functioning of the cameras had not always been effective. (free translations).

18 In 2003, State Security reports that "*the operation of the post represents an enormous workload, both in the area of monitoring the cassettes and the logistical maintenance, as well as in the area of analysis.*" (free translation).

19 In 2004, the then Director-General sends a sharp message to the Minister: "*Since no technical-juridical reason existed, it only concerned a political order, the only objective of which was to be able to hold State Security responsible in the event of problems with or on the account of Mrs. F. Erdal. State Security therefore wishes to obtain a correction of this political decision and to be relieved from the assignment of the Minister of the Interior.*" (free translation).

continues its assignment, and they are supported in this request by each of the successive Ministers of Justice;[20]
- As of 2005, State Security is the first to consider the possibility that F. Erdal could try to escape (or could be kidnapped by the DKHP-C itself) if the legal procedure should take an unfavourable turn for her. State Security reports to the competent ministers on several occasions that – in contrast to the police – it cannot take any action in the event of a possible escape;[21]
- The contacts and the coordination with the police do not always proceed smoothly.[22] Especially during the first years, cooperation with the police services did not proceed in a very structured way. An improvement in the contacts came about in 2005 and 2006. New problems appeared in the days before the escape of F. Erdal.

II.1.3.3. The period from 17 February 2006 up to the escape of F. Erdal

A new period starts on 17 February 2006. On that day, a meeting took place in the Governmental Coordination and Crisis Centre. All political, administrative, police and judicial authorities involved were represented. The objective of the meeting was to coordinate the actions of the various services involved on the day on which the sentence would be passed (namely 28 February 2006), or, in the words of the various authorised persons of State Security: this coordination meeting was necessary, so that they would not lose track of F. Erdal.

---

20 At the beginning of 2003, for instance, the Minister of the Interior reports that he has taken note of the arguments of State Security, but that he is of the opinion "*that there were reasons for continuing the assignment without interruption, in view of the sensitive nature of the case*." (free translation).

21 In April 2005, the service concluded its memorandum to all of the ministers concerned as follows: "*In light of the developments in the Erdal case, we deem it appropriate to transfer the surveillance assignment with regard to Erdal for the duration of the trial to the Federal Police observation group (POSA), which is the only competent authority for ensuring the compliance of the agreements between Erdal and the Minister of the Interior, and for preventing a* possible escape." But in 2004 as well, State Security was already of the opinion that it would be better that this assignment is entrusted to the police services. "*For many years, State Security has been carrying out this ' blind assignment', which a police service could carry out much more efficiently. After all, even if the person who is probably the subject of this measure, should leave the corresponding premises, it would be impossible for State Security to intervene, since this service may not use any force outside the scope of its assignments with regard to the protection of persons.*" (free translations).

22 For instance, State Security declared that it had informally been informed at the start of its assignment that an officer of the then Rijkswacht/Gendarmerie had been given the personal and exclusive assignment to take up contact with Erdal's confidant. State Security, however, was never informed of the existence of such meetings, nor of any results thereof. This is illustrated by the fact that on 1 April 2004, a house search is held in the premises that are being observed by State Security, without the Service being notified in advance.

The meeting, however, started from a wrong legal premise, namely that F. Erdal was a completely free person and that no coercive measures could be taken against her. This perception had apparently already existed with authorities since 2005. For instance, the Governmental Coordination and Crisis Centre informed the Minister of the Interior that "*it is not up to the Federal Police to conduct surveillance of the person concerned, as suggested by State Security, given the lack of coercive measures. The police could, however, ascertain the presence of the person concerned by means of a control, namely by the community police inspector*" (free translation). In a letter dated May 2005, which was directed to both the Prime Minister and the Minister of the Interior, the Minister of Justice agrees with this analysis: neither the police nor State Security can take any actions in the event of a possible escape of F. Erdal.

A judicial analysis by the Standing Committee I[23] and the Standing Committee P made it clear, however, that a permanent place of residence must be viewed as a form of house arrest. Non-compliance of the conditions attached to the measure is even punishable by a prison term of up to three months.[24] This also means that F. Erdal could have been deprived of her liberty by the police for a maximum of 24 hours at the moment of her escape.[25]

Since this option had been missed by all of the authorities, a different plan was developed to prevent a possible escape by F. Erdal. The report of the meeting of the Governmental Coordination and Crisis Centre concludes: "*For six years, the residence of Erdal has been under observation, including video registration. As of 20 February and up to 2 March, several shadowing teams will be deployed in order to follow Erdal <u>at all times</u>. State Security will continue to observe Erdal, until the possible arrest by the Bruges Police Zone or the Directorate of Special Units of the Federal Police. A contact between both will be guaranteed (...) for the purpose of providing a 24-hour shadowing team*" (free translation).

State Security therefore had to organise a round-the-clock surveillance and – in the event of a conviction and an immediate arrest – report to the Directorate of Special Units on 28 February where F. Erdal was. An operational plan was developed, which was approved by the Minister of Justice. Starting on 23 February, several teams were charged exclusively with this case. Their task: "*Every movement*

---

23 The Standing Committee I examined two other judicial options to deprive Erdal of her liberty: a new placing at the Government's Disposal within the framework of the Aliens and Immigration Act, and an arrest warrant within the framework of a new Turkish extradition request.

24 Article 75 of the Aliens and Immigration Act.

25 From a purely legal perspective, the members of State Security could also have proceeded to the arrest. On the basis of Article 1, 3°, of the Law on pre-trial detention, they can, like any other person, detain persons whom they catch in flagrant delict. As for shadowing operations, however, they do not have priority vehicles at their disposal and it is not certain whether they were always informed of the permissions (day and time) that Erdal was granted to leave the premises.

of Mrs. F. Erdal must be followed, also in an ostentatious manner"[26] (free translation).

On the eve of 27 February, things take a wrong turn. F. Erdal leaves the premises together with M. Asoglu and gets into a Volkswagen Golf. The vehicle escapes the surveillance of State Security.

The Standing Committee I examined in detail the operational developments of the shadowing assignment on 27 February 2006. The Committee has come to the conclusion that the work of the Shadowing department can in no way be the subject of any complaints, neither with regard to the professional behaviour of the agents that participated in this operation, nor about the manner in which it was carried out. After all, the specific assignment of this service is to obtain intelligence information and not to localise persons, whereby it has been explicitly asked not to lose sight of the person concerned and to follow her as long as possible. The *modus operandi* of this department focuses on discretion. When such discretion is no longer guaranteed, then shadowing is normally discontinued. Within such a context, following F. Erdal with the purpose of localising her, is *a priori* an assignment with a very high risk of failure, not to say a *mission impossible*.

After F. Erdal had managed to escape the persons that were shadowing her, a number of measures were taken in an attempt to localise her potential hiding places. This, however, did not lead to any results.

II.1.4. THE LEGAL BASIS FOR THE INTERVENTION OF STATE SECURITY

The Standing Committee I established that the objective for the intervention of State Security in this dossier has not always been the same throughout the years. *A posteriori,* the Committee could differentiate between five possible objectives, namely:

– a classic intelligence assignment (Article 7, 1°, of the Intelligence Services Act), under the authority of the Minister of Justice;

---

[26] Within the context of this investigation, the Standing Committee I also pointed out that surveillance and shadowing methods by definition violate privacy rights, and therefore require a sufficient and clear legal basis (Article 8 European Convention on Human Rights and Article 22 of the Belgian Constitution). At the present time, the Intelligence Services Act does not govern these methods. The lack of such a legal basis is certainly felt if State Security uses these methods for any other assignments than those it has been explicitly given (monitoring the compliance of the administrative conditions (II.1.4.4) or surveillance/localisation assignments (II.1.4.5)).

- an intelligence assignment within the framework of the maintenance of public order and public security (Article 5, §2, of the Intelligence Services Act), under the authority of the Minister of the Interior;
- an assignment to protect the physical integrity of F. Erdal;
- an assignment to monitor the compliance by F. Erdal of the conditions that were attached to the obligatory permanent place of residence;
- an assignment to localise F. Erdal for a possible arrest.

Before presenting a short discussion of these objectives, the Standing Committee I would once more like to draw attention to the importance of clearly differentiating the identity of the intelligence services towards the police services, especially when these services are simultaneously working on identical cases. This distinction is not merely intellectual or formal. The Erdal case once again shows that, when such identity is insufficiently recognised, this can lead to a shift in the assignment, prejudicing both the legal character and the operational efficiency.

II.1.4.1. The classic intelligence assignment

State Security had already been following F. Erdal and the DHKP-C long before her release. This was fully justified because the DHKP-C is listed as an extremist organisation.[27] Tracking such a group and its members is one of the core tasks of State Security and is based on Article 7, 1°, of the Intelligence Services Act.

Setting up a surveillance camera, *in casu* at the request of the Minister of the Interior, can make a technical contribution to achieving this objective.

In this regard, it must also be noted that the surveillance measures that were instituted in 2000 and that were continued up to the day of F. Erdal's disappearance, have apparently made no significant contribution to the acquisition and analysis of information. This fact is corroborated by the many documents that were submitted by State Security to the competent authorities. In these documents, a discontinuation of the measures is requested and the effectiveness in terms of intelligence is evaluated as *practically non-existent*.

II.1.4.2. The public order assignment: acquiring intelligence within the framework of the maintenance of public order

In addition to the assignment that is provided for in Article 7, 1°, of the Intelligence Services Act mentions another, less well-known assignment: "*The Minister of the Interior can nevertheless make demands on State Security in connection with the execution of assignments provided for in Article 7, if these concern the maintenance*

[27] This is also apparent from the investigation conducted previously by the Standing Committee I, published in the *Activity Report 2001*, 26 ff.

of public order and the protection of persons" (Article 5, §2, of the Intelligence Services Act) (free translation).

After F. Erdal's escape, this clause was very frequently referred to as the legal basis for the assignment to the intelligence service. It is remarkable, however, that the term 'demand' and the reference to Article 5, §2, of the Intelligence Services Act do not appear before the beginning of May 2003 (when they appear in a legal memorandum prepared by State Security).

With regard to the justification of the assignment given to State Security by the Minister of the Interior, there is absolutely no doubt that a permanent threat to public order and public security was present from 2000 to 2006. It nevertheless appears that the formulation of these demands to State Security was not as clear or precise as it could have been.

II.1.4.3. The protection assignment: protection of the physical integrity of F. Erdal

The efforts that the police authorities have put into the Erdal case over many years were also based on a concern for her security: F. Erdal had to be protected. This was, however, never the objective of the intervention of State Security, even if the protection of persons is included in the list of competences of this service – Article 7, 3°, of the Intelligence Services Act, does after all give State Security the assignment to "*carry out assignments for the protection of persons, that are entrusted to it by the Minister of the Interior"* (free translation).

The Standing Committee I has found no indication of such a ministerial demand. In any event, a protection assignment would have to be carried out by specially assigned protection officers. In this case, the services of such officers were never called upon.

II.1.4.4. The control assignment: monitoring the compliance of the conditions attached to the 'permanent place of residence'

Even if this task was initially reserved exclusively for the Immigration Service and the then Rijkswacht/Gendarmerie, State Security was sometimes called upon to monitor the conditions that had been imposed on F. Erdal. In April 2001, for instance, the Minister of the Interior asked the Minister of Justice: "*In order to make sure that these conditions (...) are being observed, I would like to formally request that State Security carry out observations*" (free translation). In reply to this letter, the Minister of Justice instructed the Director-General to cooperate in this assignment, even if State Security had clearly indicated that it was of the opinion that this assignment falls outside its competency.

The Standing Committee I is of the opinion that this assignment certainly does not fall within the scope of competence of State Security, but was gradually and wrongly imposed on the service.

II.1.4.5. The surveillance or localisation assignment: localising F. Erdal with a view to a possible immediate arrest

As of 19 February 2006, the objective of the intervention of State Security changes once again: F. Erdal must not be let out of sight and it must be possible to localise her in order to arrest her in the event of a conviction.

As for the previous objective, the Standing Committee I is of the opinion that this objective does not specifically fall within the scope of competence of State Security.

II.1.5. CONCLUSION

The Standing Committee I favours the opinion that tracking the DHKP-C in general and its members in particular, is without doubt an assignment for State Security. The permanent observation assignment and certainly the localisation assignment with regard to F. Erdal that were entrusted to State Security by the Minister of the Interior, however, fall outside its competency.

II.2. THE CIA FLIGHTS

II.2.1. EXTRAORDINARY RENDITIONS AND THE START OF NUMEROUS INVESTIGATIONS

At the beginning of November 2005, *The Washington Post*[28] published an article claiming that the U.S. intelligence service CIA was incarcerating terror suspects in secret prisons, in eastern Europe among other places. To transfer the terror suspects, the intelligence service was reported to have used airplanes of private companies that also landed on European airports. This triggered a whole series of investigations, both at international and national level.

The Parliamentary Assembly of the Council of Europe was the first to launch an investigation.[29] Two months later, the European Parliament established a

[28] D. PRIEST, "CIA Holds Terror Suspects in Secret Prisons", *The Washington Post,* 2 November 2005.

[29] See the report of the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe: "Alleged secret detentions and unlawful inter-state transfers involving Council of Europe member states", Doc. 10957, 12 June 2006.

Temporary Committee on the alleged use of European countries by the CIA for the transport and illegal detention of prisoners.[30] A number of European countries (Italy, Sweden, Spain and Germany amongst others) initiated judicial inquiries, and numerous investigative journalists and NGOs (e.g. Human Rights Watch and Amnesty International) jumped on the case.

The case triggered a chain of reactions in Belgium as well. Parliamentary questions piled up[31] and numerous investigations were initiated. At the end of November 2005, the Belgian government received a request for an explanation from the Secretary-General of the Council of Europe; on 1 December 2005, the Minister of Foreign Affairs declared before the House of Representatives that the Belgian government would initiate its own investigations, to be conducted by several government authorities;[32] on 5 December 2005, the Standing Committee I was charged with an investigation; on 23 December, the case was discussed by the Ministerial Committee for Intelligence and Security, and the College for Intelligence and Security subsequently tackled the problem on several occasions[33]…

What was going on? In 1995, the Presidential Decision Directive 39[34] was adopted in the U.S.: with regard to terror suspects who are wanted for violation of U.S. law, but who are at large overseas, their return by force to the United States for prosecution shall be a matter of the highest priority. Return of suspects may be effected without the cooperation of the government of the host country where the suspects are staying (*rendition program*).

After the attacks of 11 September, the United States went still a step further: terror suspects would no longer be arrested in a foreign country in order to appear before an American court of law, but would instead be interrogated and imprisoned in other countries. Countries, it appeared, that are not very particular with regard to torture. In other words, this did not concern normal *renditions*, but so-called

---

30 See its final report: Report on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners, European Parliament, 2006/2200(INI), 30 January 2007.

31 *Annals*, House of Representatives, 2005–2006, 1 December 2005 and *Annals*, Senate, 2005–2006, 8 December 2005.

32 Apparently the government had already taken several steps, as the Minister was able to state on that day that no irregularities had been detected on military airports. This information had been provided by the army's Aircomponent (see II.2.2.2.3). Furthermore, the results of a first study by the Directorate-General of the Civil Aviation Authority on civilian airports, were already known on 6 December 2005.

33 Neither State Security nor the General Intelligence and Security Service informed the Standing Committee I of the fact that the Ministerial Committee for Intelligence and Security had requested the initiation of an investigation. This caused quite a lot of resentment within the government, and it was the direct cause for an additional investigation by the Standing Committee I.

34 See www.fas.org/irp/offdocs/pdd39.htm.

extraordinary renditions.[35] According to the European Parliament, at least 1,245 such flights operated by the CIA have flown into European airspace or stopped over at European airports between the end of 2001 and the end of 2005, not including an unspecified number of military flights with the same purpose.[36] Amongst others, the European Parliament pointed out that these extraordinary renditions are illegal and, at the same time, in conflict with international human rights standards.

II.2.2. THE CIA FLIGHTS AND THE BELGIAN INTELLIGENCE SERVICES

The assignment of the Standing Committee I consisted of investigating whether the Belgian intelligence services disposed of information regarding flights chartered by the CIA; investigating whether the intelligence services had been questioned about the subject by government authorities; and carrying out a judicial study[37] about the status of foreign aircraft that land in Belgium, as well as about the legal problems that could arise in the event of the transfer of non-convicted prisoners via Belgium.

The Standing Committee I then initiated an investigation in December 2005 about the acquired, processed and distributed intelligence of the Belgian intelligence services with regard to the possibility of the use of Belgian airport infrastructure by flights chartered by the CIA to transport prisoners who are suspected of having links to Islamic terrorist organisations. The objective of this investigation was therefore not to confirm or negate the existence of the CIA

---

35 "*Rendition* or *extraordinary rendition* are not legally defined terms. They are normally understood to mean the apprehension and subsequent transfer of a person from one jurisdiction to another, outside the framework of legally defined procedures such as extradition, deportation, or transfer of sentenced persons and possibly with the risk of being subjected to torture or inhuman and degrading treatment. Such renditions involve multiple human rights violations, including transfer in breach of the principle of *non-refoulement*, as well as arbitrary arrest and *incommunicado* detention. The victim is placed in a situation of complete defencelessness with no judicial control or oversight by the European Committee for the Prevention of Torture (CPT) leaving the door open for the use of torture and other forms of ill-treatment", in Council of Europe, Information Documents, SG/Inf (2006)5, 28 February 2006, Secretary General's report under Article 52 European Convention on Human Rights on the question of secret detention and transport of detainees suspected of terrorist acts, notably by or at the instigation of foreign agencies (www.coe.int).

36 See: Report on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners, European Parliament, 2006/2200(INI), 30 January 2007. Human rights organisation *Amnesty International* also published an elaborate report containing concrete flight data: *United States of America. Below the radar: secret flights to torture and 'disappearance'* (5 April 2006).

37 For a European comparison in this area, see the above-mentioned report of the Council of Europe under Article 52 European Convention on Human Rights.

flights on or over Belgian territory, but rather to examine what action(s) have been undertaken by the Belgian intelligence services in their investigation and in the analysis and communication of intelligence to political, administrative and (if applicable) judicial authorities. Within the framework of this investigation, however, the Standing Committee I has come to the conclusion that not a single element of the investigations carried out by State Security, the General Intelligence and Security Service and other government authorities involved, leads to the conclusion that airplanes chartered by the CIA and involved in extraordinary renditions, may have landed on a Belgian airport. It was only possible to link registration numbers of aircraft that had landed in Belgium or had used Belgian airspace, with aircraft that were assumed to have carried out flights for the account of the CIA.

The Standing Committee I presented two reports and a reflection paper to the parliamentary monitoring committee of the Senate. These reports were discussed at length, first by the monitoring committee and thereafter in a plenary session.[38]

This investigation showed that the two Belgian intelligence services reacted differently in part to the revelations in the press, and that they subsequently did not follow up the case in the same manner.

II.2.2.1. State Security

II.2.2.1.1. Investigation on its own initiative

State Security said not to have been informed of the problem prior to its publication in the press. No element from the investigation carried out by the Standing Committee I points to the contrary. Shortly afterwards (at the end of November), the service did undertake a number of initiatives, even if it was of the opinion that this issue falls outside its scope of competence (see II.2.2.1.3). Well aware of the political sensitivity of the dossier, the service monitored the issue via open sources, sent a request for information to friendly foreign services and invited a CIA representative to provide an explanation. The results of these initiatives were limited and did not really result in an analysis paper.

According to the then Director-General, the answer of the CIA with regard to the detention and transport of prisoners – see below – was the following: "*no comment*." Furthermore, the CIA representative declared that the service had

[38] *Verslag over de mogelijkheid dat Belgische luchtvaartinfrastructuur gebruikt werd door vluchten gecharterd door de CIA om gearresteerde personen die verdacht worden van betrokken te zijn bij het Islamistisch terrorisme te vervoeren*, *Document*, Senate, 2005–2006, 1762/1 (this document provides an integral version of the different investigative reports of the Standing Committee I) and *Annals*, Senate, 6 July 2006, 3–174, 18–36.

never taken into consideration to carry out an operation on Belgian territory without prior consultation with the Belgian government and intelligence services. n[39] State Security emphasises that it has never received any request for transporting prisoners via Belgium.

Not only was very little information obtained from the CIA representative, questions directed to European sister services also remained unanswered. According to the Standing Committee I, this shows that the exchange of information between intelligence services depends primarily on the political options taken by the national authorities.

At this stage, State Security did not request information from other (administrative) authorities (such as Belgocontrol or Eurocontrol), primarily because it would be far too time-consuming to analyse that mass of information.

The findings of this short 'investigation' by State Security were submitted to the Minister of Justice – albeit not in their entirety, as will be seen hereafter. The Minister of the Interior was also informed (verbally) of the available information prior to a visit by his American counterpart, when the latter was to provide NATO with an explanation about the relevant flights.

The Standing Committee I would like to draw attention to the meeting that the Director-General held with a CIA representative. The manner in which the information that has been obtained at this meeting was handled indicates to a number of specific problems. A report was drawn up of this meeting, which was first classified as 'top secret' and then as 'secret'. Even if the content of this memorandum did not directly involve Belgium, the fact remains that State Security did have information about the CIA flights, even if this was general information. Firstly, the Standing Committee I found that this report was not submitted after the initial request. But equally important is the conclusion that the memorandum, which State Security spontaneously submitted to the Minister of Justice, contained no reference to the classified document or to certain elements of the content of that document. Yet it is a core task of the intelligence services to

---

39 This statement is interesting when read together with an excerpt from the report by D. MARTY, who acted as rapporteur for the investigation of the Council of Europe: "*The body of information gathered makes it unlikely that European states were completely unaware of what was happening, in the context of the fight against international terrorism, in some of their airports, in their airspace or at American bases located on their territory.. Insofar as they did not know, they did not want to know. It is inconceivable that certain operations conducted by American services could have taken place without the active participation, or at least the collusion, of national intelligence services.*" (Council of Europe, Parliamentary Assembly, Alleged secret detentions and unlawful inter-state transfers involving Council of Europe member states, Doc. 10957, 12 June 2006). In the European Parliament report, it is said to be "*unlikely*" that the European governments were unaware that aircraft operated by the CIA could land on European airports while having illegally arrested persons on board. (Report on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners, European Parliament, 2006/2200(INI), 30 January 2007 (among others 48, 188 and 204)).

inform its government completely and truthfully. Once again, the Standing Committee I sees itself confronted with the problem that the content of a document appears to be relevant to its investigation, but is classified and protected by the so-called 'third party rule', a rule that apparently also applies to the competent Minister and the government.[40]

II.2.2.1.2. Investigation at the request of the Ministerial Committee for Intelligence and Security

As of the middle of December 2005, State Security also cooperated in the investigation of the Ministerial Committee for Intelligence and Security. A substantial number of man-hours were invested in an in-depth analysis of certain flight data. Data were also frequently exchanged, especially with the General Intelligence and Security Service and with the Directorate-General of the Civil Aviation Authority of the Federal Public Service Mobility and Transport. This once more leads the Standing Committee I to the conclusion that the cooperation, the exchange of information and the coordination, both between the two intelligence services and between the intelligence services and other authorities, is stimulated if there is an intervention at a higher level, *in casu* by the Ministerial Committee for Intelligence and Security.

II.2.2.1.3. The scope of competence of State Security

Despite all activities mentioned above, State Security always emphasised that it was of the opinion that the CIA flights issue fell outside its scope of competence. This position was also communicated as such to the Minister of Justice.

Even if the Intelligence Services Act of 30 November 1998 provides links to this competency regarding the *subject of the threat* (for example, Article 8 specifies that the service must collect information about threats against amongst others "*the continuity of the smooth operation of the constitutional state, the democratic institutions, the elementary principles which are inherent to every constitutional state, as well as human rights and fundamental liberties*" (free translation)), the Standing Committee I cannot deny that the CIA flights can hardly be classified as one of the threats that fall within the scope of competence of State Security (within the framework of a control on foreign intelligence services, there would have to be mention of 'interference' or 'espionage'). The Standing Committee I therefore fully supports the recommendation of the Senate to introduce a clearer regulation and to explicitly include in the law, the power to monitor the lawfulness of the

40 *Verslag over de mogelijkheid dat Belgische luchtvaartinfrastructuur gebruikt werd door vluchten gecharterd door de CIA om gearresteerde personen die verdacht worden van betrokken te zijn bij het islamistisch terrorisme te vervoeren*, *Print*, Senate, 2005–2006, 17621/1, 15–17 and 62.

activities of foreign intelligence services on our territory (see Chapter VIII.1.2). The European Parliament was also of the opinion that "*all European countries should have specific national laws to regulate and monitor the activities of third countries' secret services on their national territories, to ensure better monitoring and supervision also of their activities, as well as to sanction illegal acts or activities (...)*".[41]

Besides the fact that State Security considered the problem of the CIA flights to fall outside its competency, the service offered two more reasons for not treating the dossier as a matter of priority. The service declared that "*Belgium does not monitor the CIA in the same active manner as it does other services. A variety of parameters play a role in this choice. The most important of these is that the political authorities, who define the general policy framework of State Security, do not consider the United States to be a direct threat.*" (free translation) This attitude could also be observed by the Standing Committee I in other dossiers.[42] Secondly, State Security stated that they could not give priority to this dossier due to limited personnel resources.

II.2.2.2. The General Intelligence and Security Service

II.2.2.2.1. Investigation on its own initiative

Like State Security, the General Intelligence and Security Service said not to have been informed of the alleged facts prior to their publication in the press.[43] But in contrast to State Security, this service did not initiate its own additional investigation. The service even neglected to request information from ComOpsAir, the air force service responsible for managing military airports (see II.2.2.2.3). When the General Intelligence and Security Service was questioned on 8 December 2005 by the Minister of Defence, it immediately reported that it had not received any information from American colleagues or from any other services.

---

41 Report on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners, European Parliament, 2006/2200(INI), 30 January 2007 (among others 48, 188 and 204). Cf. T. DAVIS, Secretary-General of the Council of Europe: *"It would appear that most of Europe is a happy hunting ground for foreign secret services. While most of our member states have mechanisms to supervise the activities of their domestic intelligence agencies as well as the presence of foreign police officers on their territory, hardly any country, with the clear exception of Hungary, has any legal provisions to ensure an effective oversight over the activities of foreign security services on their territory*", in Council of Europe, Speaking notes for the press conference on the report under Article 52 of the European Convention on Human Rights, 1 March 2005 (*www.coe.int/t/e/com/files/events/2006-cia/speaking_notes%20_sg.asp*).

42 See, for instance, the case concerning the eavesdropping network Echelon.

43 Again, the Standing Committee I could not establish that this assertion might not be correct.

II.2.2.2.2. Investigation at the request of the Ministerial Committee for Intelligence and Security

Like State Security, the General Intelligence and Security Service was asked to cooperate in the investigation of the Ministerial Committee for Intelligence and Security. The contribution of the military intelligence service to this investigation was rather minimal: the internal information and open sources were examined, and only now and then, namely when specific questions were put by State Security, did the service carry out concrete verifications or pass on these questions to ComOpsAir.

II.2.2.2.3. The scope of competence of the General Intelligence and Security Service

The General Intelligence and Security Service and the Minister of Defence have always reiterated that the control of the airspace or of the military (and definitely the civil) airports falls outside its competency. The Intelligence Services Act of 30 November 1998 indeed delegates different powers to the military intelligence service than to State Security. The only weak point of connection to the scope of competence of the General Intelligence and Security Service is an excerpt from Article 11, §2, of this law: the GISS must collect information about "*every manifestation of the intention of bringing (...) the protection or the continued existence of the population (...) in danger by military means*" (free translation). In addition, the military intelligence services argued, like State Security, that they are not equipped – neither in terms of personnel nor in terms of technical resources – to conduct such a surveillance operation in this matter. Besides the initiatives that have been described above, the military intelligence services followed up on the case solely via the media.

Within the Armed Forces, the Aircomponent ComOpsAir is responsible for managing the military airports. It is therefore on the results of the investigation of this service that the Minister of Foreign Affairs based himself when he declared before the House of Representatives on 1 December 2005 that no suspicious flights had occurred on military airports.

II.3. THE SWIFT CASE

II.3.1. AMERICAN ACCESS TO SWIFT FINANCIAL MESSAGES TRAFFIC

II.3.1.1. An account of the facts

The *Society for Worldwide Interbank Financial Telecommunication* (SWIFT), which has its headquarters in Belgium and various subsidiary offices spread all over the world, acts as an intermediary for the transmission of secured financial messages between almost 8,000 financial institutions in more than 200 countries. This service provision is known as SWIFTNet Fin. SWIFT does therefore not qualify as a bank and it does not keep accounts for customers.

On 23 June 2006, *The New York Times*[44] reports – to the great anger of the U.S. government[45] – that SWIFT gives the intelligence services CIA and FBI and other agencies access to its database. By way of this access into financial messages – an intrusion that fits into a larger package of measures that the U.S. government had adopted after the terrorist attacks of 11 September 2001 – the United States traces possible money transactions of terrorist organisations. Access to the data is given on the basis of confidential subpoenas from government officials (the so-called *administrative subpoenas*), issued by the Office of Foreign Assets Control of the American Department of the Treasury to the American branch office of SWIFT. SWIFT America is one of the company's two operation centres.[46] Here, all messages are stored for a period of 124 days as a *back-up recovery tool* in case of data loss or disputes between financial institutions.

SWIFT America did not provide access to its data just like that. Agreements were made and limitations were introduced. For instance, no *real-time* access was possible. The American services could only view data that was of importance in combating the financing of terrorism, after SWIFT had made parts of its database available on the basis of well-defined criteria,[47] and by way of a so-called *black box*. Furthermore, an internal and external control mechanism was installed, and

---

44 E. LICHTBLAU and J. RISEN, "Bank data is sifted by U.S. in secret to block terror", *The New York Times, 23 June 2006*.

45 A number of press articles make mention of the fact that the Bush administration strongly advised the media against divulging that it had access to international payments. What's more, after the publication, a Republican member of Congress asked the American Justice Department to open an investigation into the leaks. The U.S. Treasury Secretary called the project – which had become public knowledge by then – "*a vital tool in the war on terror and the leaking out of this information as regrettable*". The secret Terrorist Finance Tracking Program provided the U.S. with "*a unique and powerful window into the operations of terrorist networks*".

46 The other is located in Europe.

47 For example, transactions from or to certain countries and/or banks and to be situated within a certain period of time.

SWIFT could stop providing access for valid reasons. Between September 2001 and November 2006, a total of 64 subpoenas are reported to have been issued. How many transactions were actually reported under each *subpoena* is, however, not known.[48]

Persons within the National Bank of Belgium (NBB) – including its Governor – had been acquainted with these *administrative subpoenas* since February 2002. Shortly afterwards, all national banks of the G-10 were informed. SWIFT tried to get approval for these data transfers from these institutions, which function as her 'supervisory body'.[49] The NBB refused to grant this request because it considered it to fall outside the scope of the protocol signed between the NBB and SWIFT. The transfer did not, after all, pose a risk for the stability of the financial system, according to the NBB.[50] It therefore took no position, either for or against the access to data by the American authorities. Neither did the National Bank of Belgium inform the Belgian authorities of this operation. It felt itself bound by the rules of professional secrecy. It was only in April 2006 that the Minister of Finance was informed via informal channels (see below).

II.3.1.2. The start of many investigations

Exactly as with the CIA flights, this practice gave rise to a number of national and international investigations, even if these were not so much directed at the activities of the intelligence services, but rather at the manner in which the European and the Belgian privacy regulations were observed.

The European Parliament passed a resolution on 6 July 2006 that demanded an explanation from Belgium and the European institutions about the legality of the information transfer.[51] At the request of this same European Parliament, the European Data Protection Supervisor initiated an investigation on 10 July 2006 on the role of the European Central Bank, which is both a customer of SWIFT and a member of its supervisory board. Furthermore, the Article 29 Data Protection Working Party[52] also tackled the issue. And the European Commission

48 For an extensive and technical explanation, see opinion no. 37/2006 of 27 September 2006 of the Belgian Data protection Commission relating to the transfer of personal data by the SCRL SWIFT following the UST (OFAC) subpoenas (*www.privacycommission.be*).

49 This concerns a voluntary supervision and not a legally imposed one. After all, SWIFT is not a financial institution and therefore it does not fall under the competence of the NBB. For the same reason, the Belgian Financial Intelligence Processing Unit and the Banking, Finance and Insurance Commission are unable to exercise control.

50 The assertion that the transfer did not pose a risk for the stability of the financial system was called into question by the European Data Protection Supervisor.

51 Resolution of the European Parliament on the interception of bank transfer data from the SWIFT system by the U.S. secret services (P6_TA-PROV(2006)0317). In October 2006, the European Parliament organised a public hearing with all of the involved players. This investigation has not yet been completed.

52 For instance transactions between legal persons.

will decide whether European regulations have been violated and whether sanctions have to be taken against Belgium. There was also a torrent of complaints at the European and non-European authorities that are responsible for data protection. In Belgium too, the Data Protection Commission was called to question, both by an NGO, the College for Intelligence and Security, and the Prime Minister. Finally, the Ministerial Committee for Intelligence and Security was guaranteed by the U.S. Treasury Secretary that it would be completely informed.

But already on 26 June 2006, the Chairman of the Monitoring Committee requested the Standing Committee I to open an investigation. The objective was to investigate whether there was question of violation of privacy in view of the Data Protection Act of 8 December 1992, whether the need exists for a supervision of the activities of foreign intelligence services on Belgian territory in those cases where these pose no specific threat such as described in the Articles 7 and 11 of the Intelligence Services Act (II.3.3), and whether the two intelligence services knew about this exchange of data (II.3.4).

II.3.2. A VIOLATION OF THE DATA PROTECTION ACT?

At the moment that the Standing Committee I was requested to make a judicial analysis, not all the facts were known. The Standing Committee I carried out this analysis – which by the way concerns a domain that does not belong directly to its competency and expertise – with the necessary reservations and on the basis of a number of hypotheses. The Standing Committee I reached the following conclusions, however:

- The Data Protection Act is certainly applicable to a (large) number of financial transactions that are carried out by SWIFT, even if exceptions are possible (both *ratione personae*[53] and *ratione loci*[54]*);*
- The fact that all data on financial transactions from Europe are transferred as a *back-up* to SWIFT America must be differentiated from a judicial perspective from the transfer of data by SWIFT America to the American government. In the first case, Articles 21 and 22 of the Data Protection Act are applicable; these provide that data may only be sent to non-EU countries if that country

53 This Working Party is an independent European advisory body on data protection.

54 The Data Protection Act is, for instance, not applicable to the processing of personal data by someone who does not have a permanent establishment within the EU, and if the resources used for the processing of the personal data are exclusively utilised to transfer the personal data over Belgian territory.

guarantees a suitable level of protection, unless one can refer to one of the provided exceptions;[55]
- The transfer of data by SWIFT America to the American government is a "*further processing*" step, during which the original objective of data processing is abandoned. Such a new processing is only permissible if the new objective has been clearly indicated to all persons involved (Article 4 of the Data Protection Act). This is a matter of fact that requires a thorough study of all elements of the dossier;
- There certainly are elements that point in the direction of the non-observance of certain obligations provided for by the Data Protection Act – which are subject to criminal sanctions. This does not, however, mean that one can conclude that the responsibility for this lies (solely) with SWIFT. Much is, after all, dependent on the question whether this company, together with the financial institutions, must be considered as '(co-)controllers'[56] or as 'processors'[57] in the sense of the Data Protection Act. The Data Protection Act only provides in sanctions for controllers. This, too, is a matter of fact which the Standing Committee I could not pronounce its opinion of at the time of its investigation.[58]

After the investigation of the Standing Committee I had been concluded, the opinions of the Data Protection Commission, of the Article 29 Data Protection Working Party and of the European Data Protection Supervisor were announced.[59] Their conclusions were identical: SWIFT is, together with the financial institutions, co-responsible for certain processings and had to fulfil all (criminally

---

55 Without being able to make a definitive statement about this, the Standing Committee I found it defensible to assume that the transfer of certain personal data which SWIFT or its customers dispose of, could be seen as falling at least under one of the provided exceptions.

56 Article 1, § 4, of the Data Protection Act reads as follows: "*A 'data controller' means the natural or legal person, factual association or public authority which alone or jointly with others determines the purposes and means of the processing of personal data*" (free translation).

57 Article 1, § 5, of the Data Protection Act reads as follows: "*A 'data processor' means the natural or legal person, the factual association or the public authority which processes personal data on behalf of the controller, with the exception of persons which are authorised to process data under the direct authority of the controller*" (free translation).

58 SWIFT considered itself to be a 'processor' of personal data.

59 Opinion no. 37/2006 of 27 September 2006 of the Belgian Data protection Commission relating to the transfer of personal data by the SCRL SWIFT following the UST (OFAC) subpoenas (*www.privacycommission.be*), Opinion no. 47/2006 of 20.12.2006 of the Belgian Data protection Commission relating to the preparation of an agreement with regard to the transfer of personal data by SWIFT to the U.S. Department of the Treasury (UST) (*www.privacycommission.be*), Opinion no. 10/2006 of 20 November 2006 of the Article 29 Data Protection Working Party on the processing of personal data by the *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) (*ec.europa.eu*); EDPS opinion on the role of the European Central Bank in the SWIFT case of 1 February 2007 (*www.edps.europe.eu*).

sanctionable[60]) obligations under the Data Protection Act and those provided by Directive 95/46/EC, such as the obligations of information, the proportionality principle, the storage period of the data, the declaration obligation at the Data Protection Commission, etc.

In the course of March 2007, SWIFT decided to comply with the privacy regulations. The company will accept a so-called *Safe Harbour* scheme, whereby it voluntarily submits to the European regulations in the matter.

II.3.3. IS A CONTROL ON FOREIGN INTELLIGENCE SERVICES POSSIBLE IN THIS CASE?

II.3.3.1. State Security

A large number of the transactions that are handled by SWIFT evidently relate to Belgian companies. Unauthorised access to this data (especially by means of 'espionage', to put it in the terms of Article 7 of the Intelligence Services Act) can certainly be considered as a possible[61] threat for our scientific and economic potential.[62] This was also evident from a letter that the Governor of the National Bank sent to the Standing Committee I on 4 April 2005 within the framework of his research for a definition for scientific and economic potential: "(…) *The correct functioning of the financial system and the important Belgian financial infrastructures is vital for the economic activity of the country and even beyond our frontiers, taking into account the interlacing of the Belgian system in international networks, particularly in connection with the positioning of several cross-border infrastructures on our territory. According to the elements in your report, these infrastructures are not included in the list of priority domains as cited by State Security, even though their protection and the protection of the continuity of the services they provide should surely be ranked as a priority for the conservation of the country's economic potential. This concerns systems operated by the Bank itself (ELLIPS, UCV/CEC and NBB Clearing) and important systems at national level (such as Banksys) or at European and global level (such as Euroclear (including CIK), SWIFT [*we underline*] and Mastercard Europe). (…) The Bank is itself strongly involved in the supervision of this type of activity. One of its judicial*

60 Despite these conclusions, the federal prosecutor's office, in consultation with the public prosecutor's office of Nijvel, decided not to initiate legal proceedings.

61 The Standing Committee I does not in the least want to claim that the American authorities have participated in espionage. A potential threat, however, is sufficient for establishing the competency of an intelligence service.

62 The European Parliament, too, referred in its resolution (see II.3.1.2) to the possibility of passing on information "*on the economic activities of the individuals and countries concerned, and this could give rise to large-scale forms of economic and industrial espionage*".

missions is in fact to contribute to financial stability and in this regard, it is responsible in particular for the oversight of the payment and securities settlement systems. (…)" (free translation)

The Standing Committee I is of the opinion that State Security was not only competent for tracking the operation because it could pose a threat for the scientific and economic potential. Because many financial transactions of Belgian citizens could become accessible to a foreign service, this could also imply a threat for human rights and fundamental liberties, and in particular privacy (Article 8, 2°, of the Intelligence Services Act).

The fact that a possible threat might possibly be posed by a so-called 'friendly service' is not relevant, at least at a theoretical level.

The Belgian legislative framework is sufficient in this case with regard to the possibility for State Security to exercise control on the activities of foreign (intelligence) services. A change in legislation is therefore not needed.[63] This also means that the Standing Committee I can – by way of its review of the effectiveness of the intelligence services – investigate in which manner our services track the operations of foreign intelligence services in Belgium.

II.3.3.2. The General Intelligence and Security Service

The GISS is only authorised to guard the economic potential of the country when this is endangered by military means (Article 11 of the Intelligence Services Act). The scope of competence of the military intelligence services in this case is therefore not self-evident. In view of the evident competency of the civilian intelligence service, no change in legislation is necessary in this respect.

II.3.4. WERE THE BELGIAN INTELLIGENCE SERVICES INFORMED?

Both the civilian and the military intelligence services assert that they had not been informed of the data transfer prior to the publication of the press article in *The New York Times*. The Standing Committee I does not dispose of any information that could invalidate this assertion. Nevertheless, the Standing Committee I noted that both services, even if to a different degree and from a different point of view, had previously shown a certain interest in SWIFT.

[63] It can be added here, for the sake of completeness, that the members of the foreign services are fully subject to Belgian legislation (with the exception of a diplomatic protection) and that they have no official competency to intervene.

II.3.4.1. State Security

II.3.4.1.1. Interest before 23 June 2006

Even before 23 June 2006 – the date on which the article appeared in *The New York Times* – did State Security have regular contact with persons from the financial world, in particular with representatives of the NBB and SWIFT. Since 2003, agents of State Security have participated in meetings of the Permanent Consultation Platform for Enterprise Security of the Federation of Enterprises in Belgium (*VBO/FEB*), in which SWIFT is also represented.[64] The investigation has shown nevertheless that State Security was not informed about the case at any point in time, neither by the personnel within the NBB nor by the responsible managers of SWIFT. The NBB subsequently declared that it was bound by the principle of professional secrecy provided for in Article 35 of the Act of 22 February 1998 establishing the organic statute of the National Bank of Belgium, and in Article 38 of the Protocol on the Statute of the European System of Central Banks and of the European Central Bank.

The Standing Committee I nonetheless pointed out that, even under the assumption that the professional secrecy from the above-mentioned Article 35 would be applicable in this matter, the NBB has the legal possibility to still inform State Security. Although it does not expressly say so, Article 14 of the Intelligence Services Act does provide a legal exception to the professional secrecy that applies to members of, amongst others, public services, such as NBB personnel.[65] This is clear from the preparatory documents.[66] The Standing Committee I is therefore of the opinion that the NBB could have informed State Security of the existence of the data transfers, and this without exposing itself to any penal sanctions.[67]

---

64 Various meetings of the working party 'protection of the economic and scientific potential' took place.

65 The term 'public service' from Article 14 must be understood in the broadest sense of the word and includes all institutions of the federal, community, regional, provincial and municipal authorities, amongst others every public utility institution (see, for instance, *Print*, House of Representatives 1995–96, 638/1, 14).

66 See W. VAN LAETHEM, "Kan, mag of moet een inlichtingendienst op uw medewerking rekenen? (Can, may or should an intelligence service depend on your cooperation)", *Vigiles*, 2004, Vol. 4, 116–127.

67 Independent of the question whether the secrecy provisions of the Protocol on the Statute of the European System of Central Banks and of the European Central Bank is applicable to the relationship between SWIFT and the NBB, it is unclear whether Article 14 of the Intelligence Services Act also applies to the secrecy provisions of that protocol. One may assume that the provisions of that Protocol, which was resolved in execution of the Treaty establishing the European Community, cannot be prejudiced by an internal legal provision, even if this is a law in the formal sense. But a violation of this obligation to secrecy seemingly does not lead to penal sanctions. It appears contradictory that the National Bank can appeal to the principle of professional secrecy in its dealings with the government, while the Governor of the NBB

The personnel of SWIFT could also have informed State Security about the operation (Article 16 of the Intelligence Services Act). Special about the SWIFT case is of course that the members of personnel of SWIFT apparently were subject to a strict secrecy obligation imposed by the American authorities. Of course, such a foreign obligation cannot prejudice the right to provide information. However, these persons were confronted with a dilemma in the matter: if they inform the Belgian authorities, they could possibly be penalised in the United States. Nevertheless, the Intelligence Services Act provides for the possibility to adequately protect the identity of informants,[68] so that our legal system offers sufficient possibilities for passing on information to our intelligence services in a 'safe manner'.

State Security did not only have regular contact with persons within the financial sector in general, but within SWIFT in particular. During the past 15 years, State Security had interested itself, even if at irregular intervals, for a number of events that possibly related to the security of the activities of SWIFT. As a consequence, contacts were regularly made between members of State Security and representatives of SWIFT and of the company responsible for the security of this organisation. Also during these contacts, the issue of the data transfers of banking data to American services was never mentioned.

It must also be mentioned that State Security analysts participated in October 2005 and May 2006 in the *Counterterrorism Analyst Course*, organised by the *Terrorist Financing Operations Section* of the FBI and the *Department of State*. The only subject of this training session was the policy for combating the financing of terrorism. The issue of access to personal financial data came up for discussion several times. However, an analysis of the international transactions via the SWIFT system was not discussed. Much to the surprise of State Security. According to State Security, one would expect to be informed of such an operation by a friendly intelligence service, certainly in view of the fact that SWIFT has its company headquarters in Belgium.[69]

And finally, there is the fact that State Security service was informed via a report by the Standing Committee I about scientific and economic potential, of the letter from the Governor of the NBB, in which the latter emphasised the importance of amongst others SWIFT (see II.3.3.1).

All of these elements leads the Standing Committee I to conclude that State Security should perhaps have taken further investigative steps, or should at least

---

recognised that within the framework of the protection of the scientific and economic potential, the SWIFT system, amongst others, deserves a priority attention (cf. II.3.3.1).

68 See Articles 18 and 43 of the Intelligence Services Act.

69 In its resolution (see II.3.1.2), the European Parliament insisted that the United States and its intelligence services should act in the spirit of good cooperation, and that they should inform their allies of intelligence operations that it wishes to carry out on EU territory.

have given special attention to SWIFT. State Security put forward a number of reasons, however, to justify why it was not informed about this matter:

- The Ministerial Committee for Intelligence and Security had not yet provided a definition of the scientific and economic potential;
- The Service is struggling with a lack of technical resources and personnel;
- State Security is a *defensive* service and it can therefore only deploy activities in the home country;
- Especially in this area, State Security is dependent on *HUMINT* (human intelligence).

The Standing Committee I partially understands that State Security appeals to a lack of technical resources and personnel. The Committee established, however, that the service had sufficient resources to obtain information with regard to SWIFT. Furthermore, the lack of a definition for the scientific and economic potential cannot be a pretext for not investing in this case. Moreover, the argumentation that State Security is not competent in this matter because it is a *defensive service* and because the data transfer took place in the United States, does not hold water. Firstly, the Intelligence Services Act does not state anywhere that State Security is a *defensive service*; this term was not provided with a legal definition. Besides that, this notion can be defined in a variety of ways. For State Security, this apparently means that it cannot intervene in a foreign country. For the Standing Committee I, this 'defensive' aspect of the operations of State Security means that it only collects and analyses information about threats, and that it does not actively combat such threats (for instance distortion). It is not the case that State Security is not permitted to collect and analyse data about events that pose a threat to Belgium, but which take place in a foreign country. Furthermore, the possible threat for the scientific and economic potential is situated practically entirely in Belgium.[70] And State Security did not have to travel to a foreign country either in order to gather intelligence.

II.3.4.1.2. Interest after 23 June 2006

After the facts were publicly announced, State Security actively searched for information about the case. Within this framework, it prepared several confidential reports for the executive power. State Security could, however, not establish which banking data had been transferred to the American government, in which way and for what purpose this information was used, nor whether subpoenas were

70 SWIFT's company headquarters are established in Belgium; the strategic decisions about the data transfer are taken in Belgium; this concerns, among other things, data about Belgian citizens or companies, etc.

still being issued at that time. The Standing Committee I could not rid itself of the impression that State Security was unable to find out much more via its channels than what was already known via the public sources, and this despite the fact that the CIA representative in Belgium was interviewed and SWIFT clearly indicated a readiness to provide an explanation once the case had become public knowledge.

II.3.4.2. The General Intelligence and Security Service

II.3.4.2.1. Interest before 23 June 2006

The General Intelligence and Security Service had not been in possession of any relevant dossier or a document with regard to SWIFT either.[71] The service presented two reasons for this: up to that day, no military personnel had been involved in the international transactions, and the GISS had not been requested to open an investigation with regard to a possible involvement in that sense. The GISS was therefore adamant: "*Up to today, no operation has been conducted with regard to SWIFT, firstly because, until proven otherwise, there is no connection between the Armed Forces and SWIFT, and secondly, because the GISS does not have the financial means at its disposal that are necessary to undertake such operations. Finally, this case falls within the scope of competence of State Security*" (free translation).

II.3.4.2.2. Interest after 23 June 2006

Since the publication of the American operation in the press, the GISS had been collecting all available information via open sources, at the request of the Ministerial Committee for Intelligence and Security. No contact was made with State Security within the framework of this dossier.

II.4. THE KIMYONGÜR CASE

On 28 February 2006, Bahar Kimyongür – who holds the Belgian as well as the Turkish nationality – is sentenced by the correctional court of Bruges to four years' effective imprisonment (together with amongst others Fehriye Erdal) for membership of an organisation that has committed attacks against the interests of the Turkish state and for participating in activities of a terrorist group, namely

[71] The existence of SWIFT as an organisation is nevertheless known at the GISS. SWIFT had, after all, been used as a theoretical study object within the framework of an advanced training.

the DHKP-C.[72] The judge, however, does not accede to the demand of the public prosecutor's office for an immediate arrest. B. Kimyongür, who lodges an appeal, therefore remains at liberty for the time being.

On 28 March 2006, the Turkish government issues an international arrest warrant in the name of B. Kimyongür to the prosecutor's office in Brussels.[73] As he also holds the Belgian nationality, however, his arrest on the basis of this warrant is not possible in Belgium for our country does not extradite citizens to Turkey. One month later, during the night of 27–28 April 2006, B. Kimyongür is arrested in the Netherlands. The Netherlands is able to act on this international arrest warrant.[74]

Shortly after the arrest, rumours are spread that State Security is supposed to have cooperated to this arrest.[75] Parliamentary questions are subsequently addressed to the Minister of Justice. On 28 June 2006, the Standing Committee I and the Standing Committee P are charged by their respective monitoring committees with a joint investigation with the purpose of "*assessing to which extent this arrest can be treated within the framework of your review investigation into the way State Security has accomplished its surveillance assignment of Mrs. F. Erdal*" (free translation). As a consequence, the Standing Committee I opens an investigation in order to extract all useful elements from the Erdal investigative dossier[76] and, if required, to carry out further investigations to find out whether State Security has provided Dutch authorities with intelligence that could have led or could have contributed to the arrest of B. Kimyongür in the Netherlands.

---

72 This sentence was increased by the Court of Appeal in Ghent to five years' effective imprisonment. Under appeal, Kimyongür was also considered to be a leading member of a terrorist organisation. On 19 April 2007, however, the judgment was annulled by the Court of Cassation on procedural grounds. There is still no final decision in this case.

73 The arrest warrant states that Kimyongür is a member of a terrorist organisation and that he has committed violations outside of Turkey. This relates to incidents of 28 November 2000. Among other things, he is alleged to have shown the flag of the DHKP-C during a speech in the EU Parliament in Brussels by the then Minister of Foreign Affairs of Turkey.

74 On 4 July 2006, the judge in The Hague declares that he cannot accede to the extradition request, because the request did not meet the double criminality requirement.

75 See for instance M. METDEPENNINGEN, "Avec l'aide des services belge?", *Le Soir*, 2 May 2006 and S. SOMERS, "België deed veroordeelde DHKP-C-er in handen van Nederlandse justitie lopen", *De Morgen*, 21 June 2006.

76 See Chapter II.1.

II.4.1. THE ARREST OF B. KIMYONGÜR: WAS IT PLANNED OR A COINCIDENCE? OR BOTH?

II.4.1.1. The run-up

The Kimyongür case starts with a classified memorandum sent to State Security by a foreign intelligence service on 27 March 2006 (one day before the Turkish arrest warrant). This memorandum apparently indicates that B. Kimyongür wants to keep out of the hands of the Belgian and Turkish judicial authorities. In the weeks that follow, State Security attempts to obtain confirmation of this information from the service concerned and via its proper channels. Even if there are some doubts within State Security about the significance of this information from the friendly service (no confirmation can be found and different opinions exist within State Security about its genuineness), the service nonetheless decides to inform the Minister of Justice and the federal prosecutor's office on 21 April 2006.

II.4.1.2. The meeting of 26 April 2006

At the request of the Minister of Justice, a meeting is held on Wednesday 26 April at the headquarters of the Governmental Coordination and Crisis Centre of the Federal Public Service of the Interior. Among the 25 persons that attend the meeting are representatives of the cabinet of the Prime Minister, of the Minister of Justice, of the Governmental Coordination and Crisis Centre, of the Administrative Technical Secretariat for the Integrated Police, of the federal prosecutor's office, of State Security, of the then Mixed Anti-Terrorist Group and of the local and Federal Police services. The report documents that B. Kimyongür will have to answer to the Court of Appeal in Ghent in the near future, and that "*it might be received badly by the public if Kimyongür were to slip away from the Belgian justice system*"[77] (free translation). After all, the Erdal case was still very fresh in memory.

Despite the fact that some State Security agents apparently did not believe in the existence of an escape plan, some of the members of the service who are present at this meeting, claim that they have "*alarming information (reliable and originating from a third service)*" (free translation) proving that B. Kimyongür intends to escape. All possible legal options are explored to deprive B. Kimyongür of his liberty by administrative or judicial means.[78] The conclusion is that none of these options is possible or useful as B. Kimyongür is a free citizen.

---

77 Report of the meeting of 26 April at the Governmental Coordination and Crisis Centre.

78 At that moment, the Governmental Coordination and Crisis Centre had already prepared an extensive judicial study about the options available for observing and arresting the person concerned.

The meeting leads to another option, however: firstly, State Security reports that B. Kimyongür will in all probability travel to the Netherlands on Saturday 29 April 2006;[79] and secondly, the Dutch authorities can arrest B. Kimyongür on the basis of an international arrest warrant issued by the Turkish authorities. The report of the meeting at the Governmental Coordination and Crisis Centre on 26 April 2006 – of which the first version dates from 28 April and an adapted version from 3 May – includes the following: *"OA3 and the federal prosecutor's office shall take up contact with the intention of arresting Kimyongür in the Netherlands the Dutch authorities in order to inform them of the possible presence of Kimyongür in the Netherlands and of the possibility of arresting him on the basis of the Interpol alert by the Turkish authorities with the purpose of making a provisional arrest with a view to his extradition to Turkey"* (free translation). The crossed-out text represents the original editing of the report; the underlined text contains the changes requested by the federal prosecutor's office on 3 May.

Before becoming acquainted with this report, one of the members of State Security who was present at the meeting in question prepared his own report for his superiors. In this report, the above-mentioned is confirmed: *"One possibility may be to organise surveillance in the hope that he will travel to the Netherlands on 29 April to participate in a large DHKP-C meeting (in 's Hertogenbosch); the Dutch police service may be able to intercept him and could, in this case, place him at the disposition of the Turkish authorities"*[80] (free translation).

As a result of this meeting, a number of different actions are undertaken. Both the federal prosecutor's office, the Directorate of Special Units of the Federal Police, OA3 (a unit of the Federal Judicial Police of Brussels) and State Security must inform their Dutch counterparts of the possible arrival of B. Kimyongür on that particular Saturday. The federal prosecutor's office will request a mandate from the investigating magistrate responsible for the investigation against 'unknown persons' within the framework of the escape of F. Erdal, to have the Directorate of Special Units carry out a cross-border observation as of noon Friday.[81] State Security finally has to localise B. Kimyongür on 27 April around noon and continuous has to follow him, so that the Directorate of Special Units may continue the observation assignment the following day. The Directorate of

79 According to some members of State Security, the Federal Police was also informed.

80 Many State Security employees who had been involved in this dossier to some degree, declared during their cross-examination by the Investigation Service I that they were shocked by the nature of the assignment. One of them expressed his surprise as follows: *"The scenario that was proposed at the meeting of the Crisis Centre was Machiavellian"* (free translation).

81 In February-March 2006, the federal prosecutor's office has indeed requested an investigation against unknown persons for cooperation in the escape and harbouring of Erdal on the basis of Article 140, § 1, of the Penal Code. Within this framework, the investigating magistrate requested technical assistance from State Security on 23 March 2006. This request was based on Article 20 of the Intelligence Services Act (see II.4.2.2).

Special Units will follow B. Kimyongür into the Netherlands, on the basis of the mandate issued by the investigating magistrate.

On the morning of 27 April, State Security takes up station at two different locations in the hope of localising B. Kimyongür.[82] At the same time a telex message is sent to the Dutch intelligence and security service AIVD.[83] No mention is made in this message of an international arrest warrant.

However, State Security is unable to immediately localise B. Kimyongür. An intervention by the Federal Police leads them to assume that they can find out where the person in question is located. But State Security does not manage to locate B. Kimyongür. The observation assignment is therefore discontinued in the late evening.

II.4.1.3. The actual arrest

It is very probable that B. Kimyongür left for Amsterdam the same evening in order to help with the organisation of a concert.[84] As far as the Standing Committee I has been able to establish, State Security was not informed about this. The service (and the Federal Police) was in the belief that the person concerned would not leave for the Netherlands until Saturday 29 April, for a different event at a different location.

In any case, it is certain that B. Kimyongür is arrested by the Dutch police services during the night of 27–28 April. The conclusion is therefore that the arrest could *surely not* have been the consequence of scenario that was discussed at the meeting of 26 April in the Governmental Coordination and Crisis Centre, since the assumption at the meeting had been that the person concerned would leave for the Netherlands only at a later time.[85] But this does not diminish the fact that

---

82 Originally the intention was to follow the person concerned as of noon. State Security perceived this as being possible. However, this was due to a misunderstanding. Although this misunderstanding should have come to light earlier, the Federal Police is not informed, indicating a lack of communication.

83 In compliance with the agreement, the other services also inform their counterparts. For example, a meeting takes place in the Netherlands between a delegation of the federal prosecutor's office and the Dutch national prosecutor's office (*Landelijk Parket*). "*During this meeting, the Belgian colleague informed us that he has information that the wanted person (who had not yet been irrevocably convicted for participation in a terrorist organisation) might possibly come to the Netherlands on Saturday 29 April for a visit to the DHKP-C festival in Den Bosch. Furthermore, it was pointed out that an international alert exists on the wanted person for Turkey. The Dutch officer subsequently verified this alert so as to be prepared for the event that the wanted person should actually arrive in the Netherlands that particular Saturday.*" (see amongst others, *Annals*, Senate, 2006–2007, 22 June 2006, no. 172, 9 (question by Mr J. Dubié)). (free translation).

84 X, "Interview de Bahar Kimyongür", *Pan*, 26 July 2006.

85 Nonetheless, it must be clear that the Standing Committee I is conscious of the fact that it probably does not dispose of all information with regard to the exact circumstances of the

State Security had provided cooperation that *could have led* to the arrest of B. Kimyongür if he had left for the Netherlands on 29 April as anticipated. Firstly, State Security was the first to disseminate the information that B. Kimyongür would leave for the Netherlands that Saturday. Furthermore, it promised its active cooperation to the localisation assignment with a view to continuing the observation by the Directorate of Special Units. And finally, it informed its Dutch counterpart about the impending arrival of the person concerned. In this context it must also be reported that State Security, in contrast to other services, apparently did not report the existence of an international arrest warrant.

Different versions exist of the manner in which the person concerned had been stopped. According to the federal prosecutor's office, that based itself on information from its Dutch colleagues, the arrest proceeded as follows: "*At a certain moment, the surveillance unit of the Haaglanden police service was told by its radio room that a pursuit was going on from the national trunk road A4 in the direction of 's-Gravenhage. An inconspicuous police vehicle of the Amsterdam Amstelland police service was pursuing a passenger car with a Belgian licence plate. The car was registered as having been stolen. Hereupon the surveillance unit drove in the direction of the national trunk road. From the radio room they then heard that in the meantime the chase was continuing on the national trunk road A13 in the direction of Rotterdam. Near the exit Delft Noord on the national trunk road A13, the surveillance unit noticed that several police vehicles were standing still near the exit and that a vehicle with a Belgian licence plate had been stopped. At the site they heard from a colleague that another vehicle was possibly involved and that this also carried Belgian licence plates. The surveillance unit then drove via the national trunk road A13 back in the direction of the national trunk road A4, where they noticed a vehicle with Belgium number plates driving in the direction of Amsterdam. The vehicle was subsequently brought to a stop on the Papeweg in Zoeterwoude for a control. Kimyongür Bahar was a passenger in that last vehicle. During the control it appeared that an alert existed on the person concerned for localisation and arrest for the purpose of extradition to the Turkish authorities for participation in a terrorist organisation (DHKP-C). For this reason he was arrested on Friday, 28 April 2006, at 1:45 a.m. by the Haaglanden police service, and was subsequently placed at the disposition of the public prosecutor at 's Gravenhage*" (free translation).

From the different versions, the Standing Committee I remembers the following elements:

– The vehicle is driven by an acquaintance of B. Kimyongür;

arrest of the person concerned in the Netherlands. Since the arrest was a police action, the Standing Committee I was not authorised to investigate it further.

- They used the same car as that with which F. Erdal escaped in February 2006;
- The car is followed by an anonymous police vehicle;
- The car is obliged to stop and two police officers in civilian clothes check the identity of both passengers;
- B. Kimyongür is arrested and is informed about the existence of an international arrest warrant; the driver of the car may continue on his way.

Although B. Kimyongür has already spent several hours in a Dutch prison cell, State Security resumes its localisation assignment early in the morning. No one in Belgium seems to have been informed of the events of the previous night. The news only trickles in after 10 a.m. After several telephone conversations back and forth, things are clear for everyone: B. Kimyongür has been arrested. The observation assignment is therefore discontinued.

II.4.2. SOME QUESTIONS WITH REGARD TO THE ROLE OF STATE SECURITY

II.4.2.1. Localisation assignment: a task for the intelligence services?

State Security had originally raised two reasons to legitimise the localisation and observation assignment that it had carried out on 27 and 28 April 2006. Firstly, they argued that the assignment falls within its general scope of competence (obtaining intelligence about the extreme left DHKP-C). Secondly, the assignment was executed within the limits of the 'technical assistance' that the investigating magistrate had requested with reference to the investigation into the disappearance of F. Erdal.

Although it is entirely normal that State Security tracks the DHKP-C, and therefore also B. Kimyongür,[86] the Standing Committee I has established that the objective of the specific and limited observation assignment delegated to State Security, was to localise and follow B. Kimyongür with a view to a takeover of this assignment by the Directorate of Special Units before his departure to the Netherlands. The underlying intention was apparently not to strengthen the intelligence position of State Security with regard to the DHKP-C, but to avoid another disappearance in the wake of the Erdal case. This is clear from the report prepared after the meeting of 26 April 2006 at the Governmental Coordination and Crisis Centre, and it has been confirmed by members of State Security, as well as by documents originating with that service.

[86] It concerns, after all, an extremist organisation that has been labelled as terrorist both by the EU and, at that moment, by the judge of first instance.

The objective of this observation was also not to gain information within the framework of the judicial inquiry of the disappearance of F. Erdal. It was, however, the intention that State Security could transfer the observation of B. Kimyongür to the Directorate of Special Units, which had been issued a mandate by the investigating magistrate to carry out a cross-border observation during 24 hours. *De facto*, State Security cooperated in bridging the period that was not covered by the judicial mandate. In addition, a number of questions arise in connection with the alleged judicial objective of the assignment. For instance, State Security has apparently not received a request for technical assistance from the investigating magistrate to carry out this localisation assignment. It is even very questionable whether the investigating magistrate was actually informed about the fact that this service had been asked to intervene. Moreover, the judicial inquiry appears to have been as good as closed, and there was not a single indication for supposing that B. Kimyongür would meet F. Erdal.[87]

Like in the Erdal case, the Standing Committee I must conclude that this localisation assignment does not fall within the scope of competence of State Security.

The Standing Committee I deplores that State Security apparently has not carried out a serious legal analysis about the legality of its mission. This is in distressing contrast with the thorough study carried out by the Governmental Coordination and Crisis Centre, in which it was investigated whether and when the police services were allowed to observe and arrest B. Kimyongür, and which showed that the person concerned was a free citizen.

II.4.2.2. The scope of the possibility to provide cooperation and technical assistance

Within the framework of this investigation, the Standing Committee I established that – shortly after the disappearance of F. Erdal and on the basis of Article 20 of the Intelligence Services Act – the investigating magistrate sent a request for technical assistance to State Security: "*The requested assistance relates to the provision of all relevant information with regard to the activities of the above-mentioned persons [*Ed.: unknown persons] *and the terrorist group whose activities they are thought to participate in*"[88] (free translation).

---

87 This can be read in the report of the meeting of the Governmental Coordination and Crisis Centre: "*With regard to the 2nd judicial dossier (inquiry by the investigating magistrate) against unknown persons on the basis of Article 140, § 1, the investigating magistrate has the intention of closing the dossier in view of the fact that the different lines of investigation do not lead to any results*". The same report also states: "*There is no intelligence that Kimyongür would meet with Erdal.*" (free translations).

88 The information which the Standing Committee I has at its disposal, has shown that State Security did not comply in any way with the request of the investigating magistrate.

This request for assistance appears to be related to information the service already had at its disposal within the framework of its regular intelligence assignment. In that case, the legal basis for such a request is Article 19 of the Intelligence Services Act.[89] This Act instructs the Ministerial Committee for Intelligence and Security to define the conditions under which such transfer of information can take place. The Standing Committee I is not in the possession of such a directive, even though such a directive is supposed to have been issued on 16 February 2000, in which the intelligence services and the other administrative authorities and services are requested to exchange as quickly as possible any documents and information that are necessary within the framework of the execution of their respective legal assignments.[90] Rules were drafted, however, with regard to an exchange of information with judicial authorities. These are contained in two confidential circular letters.[91] As far as the Standing Committee I has been able to ascertain, these were not submitted to the Ministerial Committee with reference to this aspect.

If the request of the magistrate refers to obtaining new intelligence (for instance via observations), then a new problem arises. As the Standing Committee I has already emphasised, the contents of the term 'technical assistance' must be reduced to its essence: supporting the judicial authorities by providing *technical* opinions or *technical* assistance for measures that are taken by the judicial authorities itself. The observation of persons, with only that as its objective, does not fall within this term.[92]

The request to carry out observations in the hope of gaining useful information for a judicial inquiry, however, could be considered a request for *cooperation* in the sense of Article 20, §2, of the Intelligence Services Act, insofar as one can give an autonomous meaning to this term.[93] Despite everything, this interpretation still poses two problems:

---

89 The Standing Committee I has already pointed this out in its Activity Report 2004 (p. 124 ff.). The circular letter COL 9/2005 of 15 July 2005 of the Minister of Justice and the College of Attorneys General relative to the judicial approach to terrorism, however, states that the federal prosecutor's office may request that the intelligence services provide relevant intelligence they dispose of, within the framework of technical assistance.

90 STANDING COMMITTEE I, *Activity Report 2003*, p. 123.

91 COL 9/2005 of 15 July 2005 – *Gemeenschappelijke omzendbrief van de minister van Justitie en het College van Procureurs-generaal betreffende de gerechtelijke aanpak inzake terrorisme* and COL 12/2005 of 5 October 2005 of the College of Attorneys General concerning the Act of 30 November 1998 on the intelligence and security services - Cooperation between State Security / General Intelligence and Security Service of the Armed Forces and the judicial authorities.

92 See STANDING COMMITTEE I, *Activity Report* 2004, p. 122–123.

93 Two interpretations appear to be possible. If one follows a literal interpretation, then the provision states that the intelligence services "*give their cooperation and in particular their technical assistance*", which it appears should be understood as "*more precisely*" and not as '*for instance*'. In the preparatory documents, this is stated differently: *"(…) defines the legal basis*

– The 'protocol approved by the competent ministers', as is required by the law, is still not available;[94]
– From a strictly legal point of view, the observation of persons still does not fall within the scope of competence of the intelligence services.

In conclusion, the Standing Committee I would like to emphasise once more that one has to be careful of requesting the intervention of the intelligence services all too quickly for judicial assignments via requests for 'technical assistance' or possibly 'cooperation'.

II.4.2.3. Passing personal data on to foreign intelligence services

Within the framework of this investigation, the Standing Committee I has examined the issues that occur when a foreign intelligence service requests and/or receives personal data from a Belgian intelligence service. An example is the communication from State Security to the Dutch intelligence and security service AIVD that B. Kimyongür will be travelling to the Netherlands for a demonstration at 's Hertogenbosch. But there are also requests for personal data of the person concerned and some relatives.

Can the intelligence services transfer such information just like that? The Intelligence Services Act of 30 November 1998 does instruct these services to cooperate with foreign intelligence services (Article 20, §1, of the Intelligence Services Act). But does this regulation, especially in view of the very strict requirements made in Article 22 of the Constitution with regard to interference with privacy, offer a sufficient legal basis for the transfer of personal data? The Standing Committee I does not have any knowledge of a directive in this matter that is supposed to have been drafted by the Ministerial Committee (Article 20, §3, of the Intelligence Services Act). The Standing Committee I also refers in this connection to Article 44/1 of the Act of 5 August 1992 on the police function. In contrast to the Intelligence Services Act of 30 November 1998, this regulation expressly provides that the police services can pass on personal data they dispose of within the framework of their assignments, to foreign police services that may need this information in the execution of their assignments. The Standing Committee I has no knowledge of a similar legal or treaty stipulation that is equally clear with regard to the intelligence services. Furthermore, reference must also be made to Articles 21 and 22 of the Data Protection Act, which are also

which makes it possible for the judicial and administrative authorities (to request) cooperation as well as technical assistance" (*Documents*, Senate, 1997–98, 758/3, 12). (free translation).

94 Within the framework of the cooperation between the judicial authorities and State Security, it is difficult to speak of a protocol between two ministers, since the Minister of Justice is competent for both 'services'. A ministerial directive determining the rules of the cooperation does have to be available in this case.

applicable to the intelligence services. They forbid, as a matter of principle, the transfer of personal data to non-EU countries that do not offer an adequate level of protection for personal data.

This means that, pending a change in legislation, the intelligence services can only base themselves on the general provisions from Article 20 of the Intelligence Services Act and on the general commitments that the member states of the Schengen treaty have approved, for the purpose of applying general principles of good cooperation.

II.4.3. THE JOINT CONCLUSIONS OF THE STANDING COMMITTEE I AND THE STANDING COMMITTEE P

On 21 December 2006, both Committees formulated the following joint conclusions:

> "*On the basis of their respective investigations, the Standing Committee P and the Standing Committee I are of the opinion that:*
>
> – *The Belgian police services cannot be accused of a single error or dysfunction within the framework of the arrest in the Netherlands of Mr Bahar Kimyongür, and we consider them to have acted entirely within the legal and regulatory framework in force;*
> – *As far as State Security is concerned, a legitimate interest existed in following Mr Kimyongür's every movement;*
> – *The localisation and/or an observation of a person by State Security, carried out solely with a view to putting him/her at the disposition of the judicial authorities, is not an assignment as provided for in Article 7 of the Intelligence Services Act of 30 November 1998 on the intelligence and security services;*
> – *The absence of a definition by the Ministerial Committee of the conditions under which intelligence can be passed on to a foreign service, denies the intelligence services a reference framework in the execution of their duty of cooperation.*" (free translation)

II.5. WRONGFULLY ACCUSED? A COMPLAINT

On 7 July 2006, a complaint was made against State Security. The complainant claimed to have been wrongfully accused by State Security of having links with Russian criminal networks and, among other things, of complicity in human trafficking. The complainant feels targeted by the numerous and unjustified 'interventions' of the intelligence and police services.

By way of evidence, the person concerned quotes various summons by the police services, in which he is linked with the Russian underworld. Furthermore, in April 2006 an unfavourable opinion is issued by the prosecutor's office in the context of the naturalisation procedure of his Russian wife, amongst other things because "we do not know the possible involvement of the person concerned in the criminal activities of her husband." (free translation) The involved person, however, asserts that he was acquitted in May 2005 in an insurance fraud case and that he has never been convicted of anything else.

However, the Permanent Committee I established that State Security did dispose of reliable intelligence coming from various sources and covering a long period. This information justified the fact that the intelligence service followed the person concerned. Nothing leads to the conclusion that the service would target the complainant. Furthermore, State Security also acted in conformity with the applicable legislation when it transferred intelligence to other authorities, such as the judicial authorities within the framework of a naturalisation procedure.

In this context, the Standing Committee I wishes to note that the opinions that the intelligence services provide within the framework of procedures for acquiring Belgian nationality, do not fall under the provisions of the Act of 11 December 1998 on classification and security clearances, certificates and advice.[95] The Belgian Nationality Code of 28 June 1984 provided in a proper regulation stipulating that the opinion of the prosecutor's office may be contested before the court of first instance. It does not fall within the scope of competence of the appeal body for security clearances, certificates and advice to assess the opinions of State Security. There are, by the way, other domains where a specific regulation exists.[96]

II.6. RELIGIOUS ORGANISATION OR HARMFUL SECTARIAN ORGANISATION?

II.6.1. A RELIGIOUS ORGANISATION AT THE 'UNDERCOVER' EXHIBITION

From 1 November 2005 until 31 January 2006, the exhibition 'Undercover, 175 jaar Veiligheid van de Staat/175 ans de la Sûreté de l'Etat' (*175 years of State Security*) ran in the State Archives. This exhibition was organised by State Security and offered the visitor an overview of the key moments of its 175-year history. But

95 See Chapter VI of the complete activity report.

96 This is, amongst others, the case for persons applying for a permit in the sector of private tracing and surveillance services.

not all visitors appeared to be happy. The Standing Committee I received a complaint from a member of a religious organisation, who reacted to the fact that the exhibition openly presented his religion as a 'harmful sectarian organisation'. A panel had been positioned with a text about sects and an excerpt from the Intelligence Services Act defining the scope of competence of State Security, containing an explicit reference to a particular well-known custom of this organisation. At the top and the bottom of this panel appeared general illustrations about sects, including various elements from public sources, such as newspapers, publications, printed advertisements, etc. One of these illustrations did, however, contain a direct reference to the organisation in the form of a reproduction of the cover of their magazine.

With his request, the complained intended to "*have this aspect of the exhibition rectified by removing every direct or indirect mention of his religion in the event that the exhibition was prolonged, in order to avoid that this type of confusion is repeated in the future and, finally, to ensure that State Security displays precision, a sense of differentiation, strictness, objectivity, discretion and transparency in the collection and processing of intelligence, with the greatest respect for legality*" (free translation). This complaint not only concerned a possible violation of subjective rights or of a matter of personal importance, but also a violation of the right to decency of the religious organisation in general. In other words, it was also a question of principle: is it justified or not that State Security considers the organisation as a harmful sectarian organisation?

The Standing Committee I investigated whether the issue does indeed fall within the scope of competence of State Security, what information this service disposed of in order to judge that the organisation deserved its attention within the framework of following harmful sects, and how the service treated this intelligence.

II.6.2. HARMFUL SECTARIAN ORGANISATIONS AND THE SCOPE OF COMPETENCE OF STATE SECURITY

II.6.2.1. The general framework

For a long time, the Belgian authorities dealt with organisations with a sectarian reputation with some restraint. This attitude was prompted by the difficulty of taking a standpoint in an area that touches on the fundamental freedoms of religion, thought, expression of opinion and association. The authorities therefore limited themselves for a long time to intervening only when public order was in danger or in case of specific violations.

This situation remained unchanged up until the 70s and 80s. A series of tragic events – such as collective suicides – and strongly mediatised individual dramas brought this phenomenon to the attention of both the general public and the authorities. Especially in the 90s, a number of far-reaching measures were implemented. A parliamentary investigation committee was established, for instance, "*with a view to the development of a policy to combat the illegal practices of sects and the hazards these pose to society and individuals, especially with regard to minors*"[97] (free translation). On 2 June 1998, Parliament approved a law establishing the Information and Advice Centre on Harmful Sectarian Organisations and an Administrative Coordination Cell of Fight against Harmful Sectarian Organisations. Finally, State Security was delegated the assignment of following harmful sectarian organisations by the Intelligence Services Act of 30 November 1998.

II.6.2.2. The legal definition of a harmful sectarian organisation

Articles 7 and 8 of the Intelligence Services Act oblige State Security to gather and analyse intelligence on particular threats. One of these threats is the one emanating from 'harmful sectarian organisations'. These organisations are defined as "*groups having or claiming to have a philosophical or religious purpose whose organisation or practice involves illegal or harmful activities, harms individuals or society, or impairs human dignity*" (free translation).

In order to put this rather general definition into practice, State Security elaborated its own detailed criteria. "*While it is not that difficult to understand the structural (there must be question of a group, not an individual acting on his own), religious or philosophic aspects, it has appeared to be necessary to describe the last paragraph of the legal definition more precisely (harming individuals...). It has appeared to be useful to make use of a number of criteria that make it possible to define more accurately what is meant by 'harmful nature'. This concerns the following criteria:*

- *Mental manipulation / psychological destabilisation;*
- *Excessive financial demands;*
- *A rift between the adherent and his reference environment;*

---

97 *Verslag van het parlementair onderzoek met het oog op de beleidsvorming ter bestrijding van de onwettige praktijken van de sekten en van de gevaren ervan voor de samenleving en voor het individu, inzonderheid voor de minderjarigen*, *Documents*, House of Representatives, 1997–98, nos. 313/7 and 313/8. In its final report, the investigation committee provided an overview of the different organisations that the members of the committee had interrogated or that were discussed during the parliamentary deliberations. Some persons take this summary for an official "black list". This is not the case at all. The investigation committee itself made clear that the list represented neither a position, nor a judgement on the part of the committee.

- *The exploitation of the adherent for the benefit of the organisation or its leaders;*
- *The recommendation and/or use of therapies or practices that can cause harm to the physical integrity of the adherents;*
- *The fate of (underage) children within the organisation;*
- *The risk of infiltration in the political and economic sectors of society;*
- *The organisation's discourse directed against society.*

These criteria need not be present cumulatively and this list is not exhaustive. If on-site observation of the practices of various sectarian organisations brings new harmful behaviour to light, then a new criterion can be added to the list. This has not occurred up to now. The harmful nature of a philosophic or religious organisation, or of an organisation that presents itself as such, is therefore ultimately assessed in the light of the above criteria"(free translation), according to the statements of State Security.

The Standing Committee I completely supports the fact that and the manner in which State Security has elaborated the definition of its legal assignment.[98]

II.6.3. THE MANNER IN WHICH STATE SECURITY TRACKS THE RELIGIOUS ORGANISATION IN QUESTION

On the basis of information that State Security acquires from public sources, it does not hesitate to consider the organisation that was the subject of the investigation as a harmful sectarian organisation in the sense of the law. The

---

98 This definition is very similar to the criteria that were used by the parliamentary investigation committee to check the harmfulness of religious organisations:
- fraudulent or misleading recruitment methods;
- use of mental manipulation;
- the bad physical or mental (psychological) treatment, to which the adherents or their families are subjected;
- denying medical care to the adherents or their families;
- violence, especially sexual violence, with regard to adherents, their families, third parties or even children;
- the obligation for adherents to break with their family, their husband or wife, children, relatives and friends;
- the fact that children are abducted or separated from their parents;
- deprivation of the freedom to leave the sect;
- excessive financial demands;
- fraud and embezzlement of money and goods at the expense of the adherents;
- illegal exploitation of the work of its members;
- a complete rupture with democratic society, which is considered evil;
- the desire to destroy society for the benefit of the sect;
- the use of illegal methods to gain power.

intelligence on which the service bases itself (mental manipulation, moral pressure, rift with the family, financial demands and exploitation of its members for the benefit of the organisation, 'internal' justice towards certain violations and danger for the adherents' health) illustrate at least five of the criteria that it has formulated itself. State Security does, however, state that it does not give priority to the surveillance of this organisation. "*Taking into account the fact that this organisation is well-known with the general public – and even has a negative reputation with the public – and considering the more than limited human resources that State Security has at its disposal to ensure the fulfilment of its legal assignment, State Security does not consider this organisation as a high-priority issue*" (free translation).

Nevertheless, the Standing Committee I is of the opinion that it would have been more discrete if the indirect reference to the religious organisation in question had been avoided during the 'Undercover' exhibition.

On the basis of its investigative results and given the current state of legislation, the Standing Committee I has come to the conclusion that State Security is right to follow the organisation in question without giving it priority. After all, the unpredictability and the insecurity that are characteristic for some organisations that are considered 'sectarian', justify the necessity to acquire intelligence with a view to informing the government authorities, even if this vigilance may possibly impair the freedoms of religion and association.

CHAPTER VIII.
RECOMMENDATIONS

On the basis of the investigations that were concluded in 2006, the Standing Committee I formulates the following recommendations, which relate to the protection of those rights which the Constitution and the law confer on individuals (VIII.1), to the coordination and efficiency of the intelligence services (VIII.2) and to the optimisation of the opportunities open to the Standing Committee I during the execution of its review assignment (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. CONTROL OF THE SPECIAL INTELLIGENCE METHODS

The need for additional opportunities for the intelligence services is evident and has been a high-priority recommendation of the Standing Committee I for quite some time. However, this must be founded on legal standards respecting the principles of subsidiarity and proportionality. At the same time, a proper control must be provided. For its view in this matter, the Standing Committee I refers to its opinion on the Draft law relative to the methods for the collection of data by the intelligence and security services (Chapter III.2.7). The Committee would also like to draw attention to the previous position taken by the monitoring committees in this regard, which will not accept any ambiguity whatsoever about the scope of competence of the Standing Committee I for controlling the special intelligence methods.[99] (Chapter I.2.1.1).

[99] *Documents*, Senate, 2003–2004, 725/1, and *Documents*, House of Representatives, 2003–2004, 1289/1.

VIII.1.2. CONTROL OF FOREIGN INTELLIGENCE SERVICES

Control of the activities of foreign intelligence services on Belgian territory is not included as such in the legal assignments of State Security or the GISS.[100] With regard to Europe, this would only be the case with Hungary. The Standing Committee I is of the opinion that this competency must be explicitly provided for in the law. The Belgian intelligence services are, after all, best positioned to recognise and assess the activities of (even friendly) foreign intelligence services.

The Standing Committee I established that ample support exists for this recommendation. In addition to the Belgian Senate and the Secretary-General of the Council of Europe,[101] the European Parliament was also of the opinion that "*all European countries should have specific national laws to regulate and monitor the activities of third countries' secret services on their national territories, to ensure a better monitoring and supervision also of their activities, as well as to sanction illegal acts or activities*„[102]

VIII.1.3. EXCHANGE OF INFORMATION WITH FOREIGN INTELLIGENCE SERVICES

It is self-evident that good cooperation with foreign services is indispensable in some areas. The Standing Committee I is of the opinion, however, that the legal rules of such a cooperation must be defined in greater detail. The transfer of personal data to foreign services, in particular, must be explicitly defined. The bill defining the special intelligence methods would appear to provide an excellent opportunity.

---

100 Only when such foreign intelligence services resort to espionage or interference, is there at present a legal competence for State Security (Articles 7 and 8, of the Intelligence Services Act).

101 "*It would appear that most of Europe is a happy hunting ground for foreign secret services. While most of our member states have mechanisms to supervise the activities of their domestic intelligence agencies as well as the presence of foreign police officers on their territory, hardly any country, with the clear exception of Hungary, has any legal provisions to ensure an effective oversight over the activities of foreign security services on their territory*" (T. DAVIS, in Council of Europe, Speaking notes for the press conference on the report under Article 52 of the European Convention on Human Rights, 1 March 2005 (www.coe.int/t/e/com/files/events/2006-cia/speaking_notes%20_sg.asp)).

102 Report on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners, European Parliament, 2006/2200(INI), 30 January 2007 (among others 48, 188 and 204).

VIII.2. RECOMMENDATIONS WITH REGARD TO THE COORDINATION AND THE EFFICIENCY OF THE INTELLIGENCE SERVICES

VIII.2.1. A LEGAL REGULATION FOR SPECIAL INTELLIGENCE METHODS

The Standing Committee I repeats its request to grant the intelligence services those competencies they require to carry out their assignments. In particular, they can no longer be denied the interception of telecommunications. The Committee refers in this connection to its recommendations in Chapter III.2.

The Standing Committee I also emphasises the importance of the other recommendations that it has formulated in its opinion (the need for a detailed regulation of the standard intelligence methods, a better elaboration of the transfer of information to the judicial authorities, a clear regulation with regard to cooperation with and technical assistance to the judicial and administrative authorities, etc.).

VIII.2.2. COMPLIANCE WITH THE SCOPE OF COMPETENCE OF THE INTELLIGENCE SERVICES

During 2006, the Standing Committee I has found that in 3 dossiers, the intelligence services were requested to carry out assignments that do not fall within their legal scope of competence. Concretely this concerned two assignments for localisation of persons and the issues surrounding the CIA flights.

For the general public to place trust in an intelligence service, it is vital that the impression is not given that it can be turned to whenever another government authority fails to or cannot intervene. The Standing Committee I therefore recommends the intelligence services, in case of doubt regarding the legality of an assignment, to carry out an objective (legal) analysis and to officially announce this to the competent minister(s). In applicable cases, the service or the minister could consider obtaining the opinion of the Standing Committee I.

VIII.2.3. THE 'THIRD PARTY RULE'

Certain investigations strengthen the conviction of the Standing Committee I that the issues surrounding the 'third party rule' are still current. Even though the Standing Committee I is aware that the (foreign) intelligence services consider

this rule to be untouchable, it has frequently urged that application of this rule and the control thereof should be reconsidered.

VIII.2.4. THE PROTECTION OF THE SCIENTIFIC AND ECONOMIC POTENTIAL

The Standing Committee I has pointed out numerous times that State Security cannot properly execute the assignments it has been delegated by the Intelligence Services Act of 30 November 1998, especially with regard to the scientific and economic potential, if it is not provided with the appropriate legal, technical and personnel resources.

The Standing Committee I confirms that the personnel resources that are deployed for the protection of the scientific and economic potential are effectively insufficient. A lack of economic and financial experts at State Security explains the attitude of the service with regard to these subject matters. The Committee once again appeals to the necessity of expanding the personnel resources of State Security. At the very least, this service should have the possibility of enlisting the assistance of external experts in economics, IT, telecommunications, cryptography, financial analyses, etc.

With regard to the required legal definition of the scientific and economic potential, the Standing Committee I has learned that the Ministerial Committee for Intelligence and Security has recently given its approval to a proposal by State Security.[103] The Standing Committee I is pleased about this, and it is convinced that State Security will be able to fulfil its legal assignment with greater resoluteness from now on.

VIII.2.5. THE COOPERATION WITH THE IMMIGRATION SERVICE

The Standing Committee I recommends that an assessment be made of the possible synergies between State Security and the Immigration Service. Pursuant to Article 19 of the Intelligence Services Act, intelligence services may transfer information to, amongst others, administrative authorities. Pursuant to Article 20, §1, of the Intelligence Services Act, they must see to an as effective as possible mutual cooperation with those authorities, and pursuant to Article 20, §2 of the Intelligence Services Act, State Security can extend its cooperation to these authorities. However, neither the Intelligence Services Act nor the Aliens and

[103] This proposal was the result of a study by the Standing Committee I and a subsequent constructive consultation with State Security.

Immigration Act makes provisions about the special role that State Security plays in the application of this legislation. The Aliens and Immigration Act does, however, argue in an indirect way the usefulness of an exchange of information between State Security and the Immigration Service, especially in those cases where the Minister of the Interior adopts security measures against aliens, for reasons of public order or national security.[104]

As far as the Standing Committee I has been able to establish, no specific directive by the Ministerial Committee for Intelligence and Security exists with regard to the exchange of information between State Security and the Immigration Service. A liaison officer was appointed, however, for the purpose of simplifying the exchange of information between these services. The Standing Committee I therefore recommends that such a directive is drawn up.

VIII.2.6. THE COOPERATION WITH POLICE AUTHORITIES

The Standing Committee I recommends that special importance is assigned to the specific nature of the intelligence assignment. Furthermore, a clear definition is required of the conditions under which an operational cooperation between the intelligence services and the police services is to take place. This must occur at the level of the Ministerial Committee for Intelligence and Security and by way of a protocol between the intelligence services and the (federal) police.

VIII.3. RECOMMENDATIONS ABOUT THE EFFECTIVENESS OF THE REVIEW

VIII.3.1. PROVIDING INFORMATION TO THE INVESTIGATION SERVICE

Also in 2006, the Standing Committee I has established that the intelligence services were unable in the short term to deliver all information that was relevant for an investigation. All too frequently, the Investigation Service had to request additional documents when it got wind – by accident or after an analysis of previously submitted documents – of the existence of further information. With a view to an efficient control procedure and in order to avoid any misunderstandings, the Standing Committee I recommends that the intelligence services set up a system as soon as possible that will make it possible to almost immediately and completely inform the review body. The Standing Committee I is aware, however,

[104] These measures can in particular consist of the assignment of a place of residence, placing candidate refugees at the Government's Disposal and administrative detention.

that such a system will not be useful for every type of investigation (for instance for thematic investigations).

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

The Standing Committee I and both monitoring committees have already urged a number of times that the Committee be systematically provided with the directives of the Ministerial Committee for Intelligence and Security. This is still not the case. In practice this means, for instance, that the Standing Committee I is not informed about the contents of the directive relative to the protection of the scientific and economic potential, while the Committee is responsible for exercising control on the manner in which the intelligence services fulfil this assignment.

The reticence of the services in this matter is an enigma to the Standing Committee I. The Committee points out that it presently already disposes of a sufficient legal basis for receiving these documents. Article 33, §§1 and 2, of the Review Act of 18 July 1991 stipulates that the Standing Committee I has a right to all documents that regulate the manner in which the members of these services operate and that the Standing Committee I and the Investigation Service have the right to be provided with all texts which it deems necessary for the fulfilment of its assignment. The law contains no reservations with regard to the origin of the documents.

If the intelligence services continue to refuse the systematic transfer of directives, then it should be recommended that the legislative power obliges the Ministerial Committee itself to directly send its directives to the Standing Committee I.

VIII.3.3. BOUNDARIES OF THE REVIEW ASSIGNMENT OF THE STANDING COMMITTEE I

The Standing Committee I is sometimes confronted with questions by its principals which appear to exceed the boundaries of the legal assignment and the expertise of the Committee. As a consequence, the Standing Committee I cannot properly answer these questions, because its legal possibilities and its personnel resources are not appropriate for this task.

VIII.3.4. SUPERVISORY JURISDICTION OVER OTHER SERVICES THAN THE BELGIAN INTELLIGENCE SERVICES

In the context of the investigation into the CIA flights, the monitoring committee of the Senate formulated the proposal of expanding the scope of competence of the Standing Committee I, so that it can supervise all institutions that may provide useful intelligence on the operation of the Belgian intelligence services and of the foreign intelligence services on our territory.

With regard to the first aspect, the Standing Committee I can already direct all necessary questions to all services, without however being able to apply any pressure. The Standing Committee I is of the opinion, however, that this possibility is sufficient for fulfilling its review task.

With regard to the control of the activities of foreign intelligence services in Belgium, the Standing Committee I is of the opinion that this must become one of the core assignments of the two intelligence services (see VIII.1.2 *above*). The Standing Committee I can then supervise the manner in which State Security and the GISS fulfil this assignment within the framework of its normal scope of competence.

VIII.2.3. MISUSE OF CLASSIFICATION AND THE 'THIRD PARTY RULE'

An improper appeal by the Belgian intelligence services to classification or the third party rule sometimes stands in the way of a meaningful reporting of investigation results to the monitoring committees. The Standing Committee I therefore considers it desirable to provide a specific rectification system (e.g. declassification).

ACTIVITY REPORT 2007

TABLE OF CONTENTS OF THE COMPLETE ACTIVITY REPORT 2007

PREFACE

In the early months of 2008, the intelligence community was the subject of an unabated stream of news reports, not infrequently casting it in an unfavourable light. 2007 was a different story, however, a year that was remarkable for both the intelligence services and the Standing Committee I, albeit in different respects. For State Security and the General Intelligence and Security Service, on the one hand, because a bill on special intelligence methods was finally brought before Parliament. But also because it was the first year that these services were working within the framework of the Threat Assessment Act of 10 July 2006. For the Standing Committee I, on the other hand, 2007 was remarkable in the sense that the exceptional political situation and the resulting reduced interaction with Parliament provided the time to reactivate a number of investigations and to evaluate the internal operation of the committee.

The Standing Committee I therefore took advantage of the exceptional political situation to breathe new life into and – where possible – complete a number of investigations that had not been finalised due to circumstances. The initial results of that catching-up operation are contained in the second chapter of this activity report, together with the conclusions of a number of recent investigations. This chapter also shows that considerable capacity was devoted to other investigations during 2007.

Furthermore, the Standing Committee I built on this momentum to optimise its 'internal operating processes', which were due for revision after fifteen years. The results of this are not immediately visible to the outside world, but we hope that indirectly, they will be evident: this exercise – which is, incidentally, still ongoing – is intended to lead to even higher-quality investigations, and to sound recommendations with a view to more efficient operation of the two Belgian intelligence services, of the Coordination Unit for Threat Assessment and the supply of information by its supporting services.

2007 was also the first complete year of (co-)operation of the Coordination Unit for Threat Assessment and the so-called supporting services. In this context, the Standing Committee I made enquiries among the intelligence services about potential problems with the supply of information by their foreign counterparts. Furthermore, an initial report was drawn up – together with the Standing Committee P – about the start-up of the Coordination Unit. At the time of writing of this activity report, a second report regarding specific aspects of the coordination of the threat analysis was being completed.

In closing, a bill on special intelligence methods was brought before the Senate in March 2007, even though it was not brought to a vote in the end. The Standing Committee I has repeatedly recommended in the past that the intelligence services are provided with the necessary resources and methods, but in its opinion on the above-mentioned bill, it also emphasised the need for parliamentary supervision to keep pace with the new instruments. The Standing Committee I will maintain this position with regard to any new initiative on this subject.

Guy Rapaille,
Chairman of the Belgian Standing Intelligence
Agencies Review Committee

1 June 2008

CHAPTER II.
INVESTIGATIONS

Since it came into existence in 1993, the review mission of the Standing Committee I has been limited to the review of State Security and the General Intelligence and Security Service of the Armed Forces (GISS).[105] 2007 was the first year in which the Standing Committee I was able to initiate investigations into the operation of the Coordination Unit for Threat Assessment (CUTA) and its various supporting services.[106] Since the CUTA was still very much in its start-up phase in 2007 (and the main emphasis was therefore on implementation of the regulations and recruiting), it was decided not to initiate any specific investigations. However, pursuant to Article 35, §4, of the Review Act, both committees drew up a first comprehensive report to the House of Representatives and the Senate about that start-up phase and enquiries were made about the application of the 'third party rule' in the transfer of information to the CUTA.[107]

In 2007, the Standing Committee I initiated six investigations: five on its own initiative and one after a complaint made by a private individual.

The committee received a total of twenty complaints from private individuals. As stated, one complaint resulted in the initiation of an investigation. Seventeen complaints were not upheld, because – sometimes after rapid verification of a number of items of information – they were manifestly unfounded (Article 34 of the Review Act). The two remaining complaints also appeared manifestly unfounded after preliminary investigation. Three reasons led to these complaints being ruled unfounded: either the complaint had already been dealt with or rejected, or the complaint had no basis in fact, but usually it was not the Standing Committee I but another service (such as the Standing Committee P) which was competent. In these last cases, the complainant was referred to the competent authority.

---

105 Up to 1998, the Standing Committee I could also supervise any public service, which after the entry into force of the Review Act was specifically charged with the collection and processing of data about persons, groups and events, performed with a view to security. This clause was deleted from the Act.

106 If the investigation relates to the operation of the CUTA and of the supporting services which are not police services as defined by the Review Act, this investigation must be carried out together with the Standing Committee P that is responsible for the supervision of the Belgian police services.

107 See Chapter II.1.

In total, investigation procedures were initiated in seventeen different cases in 2007. In some other cases, no actual investigation activities took place, for example because they were suspended due to an ongoing judicial inquiry, or because the investigation was initiated at the end of the operating year.

Moreover, nine cases were completed in 2007. This chapter will first discuss the completed investigations (II.1 to II.9). Then follows a summary and a brief description of the investigations where significant investigative activities were carried out in the course of the operating year 2007 (II.10.1 to II.10.11), and the investigations started at the end of 2007 (II.10.12 to II.10.14).

For the sake of completeness, the Standing Committee I wishes to emphasise again that the decision to launch a investigation is often preceded by a brief preliminary investigation. This may take the form of a rapid enquiry of the intelligence services, a discussion or a briefing on a given theme, a literature study etc. For example, the committee inquired in 2007 about the so-called defence attachés, about the issue of theft of documents and about international treaties which include the 'third party rule'. However, these preliminary investigations, which sometimes require a considerable amount of work, do not always lead to the initiation of an actual investigation.

II.1. THE CUTA AND THE 'THIRD PARTY RULE'[108]

On 23 December 2006, former Senate President Lizin requested, on a proposal from MP Van Parys, that the Standing Committee I examine the compatibility between Article 12 of the Threat Assessment Act of 10 July 2006 on the one hand, and Article 15 of the implementation decree of 28 November 2006 on the other.

Article 12 of the Threat Assessment Act stipulates that intelligence supplied by the intelligence services but emanating from a foreign service which has expressly requested that it should not be passed on to any other services, must nevertheless be communicated to the Director of the CUTA. This information must also be included in the evaluation if it is indispensable to be able to take the necessary measures for the protection of persons.

---

[108] See more about the CUTA: DELEPIÈRE, J.-Cl., "Une approche commune et intégrée de l'analyse de la menace terroriste: la création de l'organe de coordination pour l'analyse de la menace" (A common and integrated approach of the terrorist threat assessment), in *Geheime diensten. A licence to kill*, MATTHIJS, H. (Ed.), Bruges, la Charte, 2007, 11–23; PIETERS, P., "Terrorisme en extremisme: coördinatie van de dreigingsanalyse" (terrorism and extremism: coordination of the threat assessment), *Panopticon*, 2007, n° 2, 68–75; SCHUERMANS, F., "Terrorisme en extremisme" (terrorism and extremism), *RABG*, 2007, n° 1, 60–62 et VAN LAETHEM, W., "L'Organe de coordination pour l'analyse de la menace: une analyse ponctuelle" (The Coordination Unit for Threat Assessment: a punctual analysis), *Vigiles*, 2007, n° 4, 109–127.

Article 15 of the Royal Decree of 28 November 2006 states that this information may only be included in the evaluation with the express consent of the source service concerning the form, content, dissemination and level of classification of its despatch.

The Standing Committee I decided not to examine the specific legal question, because it fell outside its mandate. The committee did consider, however, that the general issue underlying the question, i.e. the principle of the 'third party rule' and the principle of collaboration with foreign intelligence services, required further investigation. This decision was partly prompted by the fact that the Standing Committee I had sometimes received – occasionally contradictory – information from different domestic and foreign sources as to difficulties in the relationship with certain foreign services. This was a consequence of the regulations which are included in the Act of 10 July 2006 and oblige the intelligence services to pass on all intelligence to the CUTA.[109] According to these rumours, the information flow from the foreign services to their Belgian counterparts may have been influenced by this.

For that reason, the question arose within the Standing Committee I whether, and to what extent, the Belgian intelligence services were experiencing problems with their foreign counterparts as a result of the implementation of the Threat Assessment Act.

II.1.1. THE GENERAL INTELLIGENCE AND SECURITY SERVICE (GISS)

The GISS made the following statement about this:

- The service has not received any document or memorandum from foreign intelligence services with regard to the establishment of the CUTA. During international contacts at command level, no formal questions were put to those in charge of the GISS about the CUTA;
- Certain foreign services have expressed their concerns about the observance of the 'third party rule', and have spoken about this to Belgian agents with whom they were in contact;
- In relations on the ground, the GISS has not encountered any particular problems;
- No statistics are or have been kept about the amount of intelligence sent to or received from foreign services, either before or after the establishment of the CUTA;

[109] Members of staff who do not comply with this obligation render themselves liable to a penal sanction (Article 14, Threat Assessment Act).

– The quality of the relations between the Belgian and foreign services depends to a large extent on good interpersonal contacts. These have not suffered from the establishment of the CUTA. The GISS did point out that whenever there was a change in the legal or regulatory framework governing the intelligence services, certain foreign services expressed concern, which soon evaporated. This had been the case, among other occasions, on the establishment of the Standing Committee I and on the occasion of the adoption of the Intelligence Services Act of 30 November 1998;
– The GISS also draws attention to the fact that various communications have created or aggravated misunderstandings.

The GISS concluded that, based on its practical experiences before and after the establishment of the CUTA, there were no problems in relations with foreign services.

II.1.2. STATE SECURITY

State Security made the following statements:

– The draft law had already raised questions and concerns from foreign services;
– At the end of 2006/early 2007, more detailed explanation was requested by certain foreign services;
– Detailed explanation about the Threat Assessment Act was drawn up and distributed to foreign services. In this presentation, it was expressly stated that there is no incompatibility between the Act of 10 July 2006 and the Royal Decree of 28 November 2006 on implementation of that law. It was also made clear that the CUTA is the successor to the Mixed Anti-Terrorist Group (ATG) – which nobody had ever complained about – and that the CUTA is based on the British Joint Terrorism Analysis Centre (JTAC), which has been in operation for a number of years;
– The collaboration between the Belgian and foreign services has never suffered from particular difficulties connected with the establishment of the CUTA;
– The embargo procedure enshrined in the Act of 10 July 2006 and in its implementation decree, complies with the guarantees requested by the foreign services.

State Security also pointed out that the 'third party rule' implies that neither the source, nor the service of origin may be divulged, but that these elements are not relevant to the threat analysis, which is the essential mission of the CUTA. This

service also drew attention to the fact that undoubtedly, hasty misunderstandings have grown from an incorrect perception of the objectives and the modalities of the transfer of intelligence. State Security argued that the problems that existed with foreign services were ironed out as a consequence of the explanation given about the operation of the CUTA, and that practice had shown this at the time of the inquiry by the committee.

II.1.3. CONCLUSION

Based on the information provided by the Belgian intelligence services, the Standing Committee I could conclude that certain foreign services did ask questions relating to the establishment of the CUTA, but that they evidently received a satisfactory answer. The two Belgian services have not experienced any particular difficulties in their relations with foreign services. This observation was confirmed by the fact that the Standing Committee I has since then not received any more indications that might give rise to a presumption to the contrary.

II.2. MONITORING OF RADICAL ISLAMISM BY THE INTELLIGENCE SERVICES[110]

In the activity report on the operating year 2001,[111] the Standing Committee I devoted attention to the way in which State Security monitored extremist and terrorist 'Islamist' activities. While 'Islamic' relates to the religion and culture of Islam, 'Islamist/Islamism' are defined as an ideology which makes Islam and fundamentalist observance of the *sharia* a political, economic and social alternative to democracy and liberalism.

The committee came to the following conclusions in this respect:

- State Security does not supervise Muslims as such, nor the practice of Islamic religion;
- The service gives absolute priority to terrorism;
- Although an intelligence service can be expected to act mainly preventively, in these matters, State Security acts mainly reactively;
- Particularly since the attacks of 11 September 2001, the service appears to have collaborated effectively in the context of judicial inquiries. But already

[110] The complete report may be consulted on the website of the Standing Committee I (www.comiteri.be).

[111] STANDING COMMITTEE I, *Activity report 2001*, 89–150.

during the 1990s, State Security collaborated in the dismantling of various terrorist cells established in Belgium;
– State Security investigates how specific Islamist tendencies are attempting to impose their political-religious views on society by being active within some immigrant communities in our country and within the institutional Islamic bodies in Belgium;
– State Security also investigates extremist activities in mosques and provides information in this regard to the political authorities who are responsible for the financing of the religious services;
– The extra personnel resources that have been deployed since 11 September 2001 in the context of radical Islamism, have been recruited from other services, who evidently also have important tasks to carry out;
– State Security has not yet carried out any in-depth analysis of the development of the Islamists' long-term strategy.

The Standing Committee I has carried out other investigations in recent years in connection with the monitoring of extremist and terrorist Islamist activities.[112] From this, it could be deduced that:

– The activities carried out by the intelligence services with regard to certain persons came within their legal powers;
– The collaboration between the civil and military intelligence services in 2002 and 2003 revealed a substantial number of deficiencies. In this context, it also emerged that State Security challenged the powers of the GISS to monitor radical Islamism in Belgium. The Standing Committee I considered that monitoring of this phenomenon did indeed fall within the powers and responsibilities of the GISS, but only to the extent that military security in the broad sense was threatened, not just in Belgium but abroad as well;
– The information flow between the intelligence services, police services, the ministers concerned and the judicial and administrative authorities left room for improvement, and genuine coordination of the intelligence at the highest level was recommended;
– There was a need for extra personnel, technical and legal resources for the intelligence services;

112 Investigation into the way in which the intelligence services cooperated in the surveillance of a person suspected of supporting terrorist activities in Belgium (*Activity Report 2004*, 84–108); investigation of the role of the intelligence and security services concerning a Belgian foundation with possible links with an organisation appearing on the list of terrorist organisations of the European Union and the United States (*Activity Report 2004*, 36–43) and joint investigation by the Standing Committees P and I concerning the coordination between the various intelligence and police services in the fight against terrorism (*Activity Report 2005*, 45–46).

– More detailed legislation was required about the way in which the intelligence services can collaborate with the judicial authorities.

By means of this follow-up, the Standing Committee I attempted to examine whether, and to what extent, the conclusions from those previous investigations were still relevant, and whether new observations could be made. At the same time, the investigation was extended in every respect to the military intelligence service.

For this evaluation, the government's *Action Plan Radicalism* was used as a guideline. This plan, which provides for proactive, preventive and repressive measures to combat the causes of Islamist radicalism and terrorism among others, was approved in 2005 by the Ministerial Committee for Intelligence and Security (MCI&S). It divides the tasks between various administrative, police and judicial authorities. Of course, State Security has an important role to play, and has to manage a number of projects. The military intelligence service is also a stakeholder. The original action plan consisted of six key areas: radical internet sites, radio and television broadcasts, extremist imams and preachers, cultural centres and non-profit organisations, radical groups and, finally, propaganda centres.[113] Subsequently, the pillar 'prisons' was added.

II.2.1. MONITORING OF RADICAL ISLAMISM BY STATE SECURITY

II.2.1.1. General considerations

The approach to radical Islamism by State Security is partly thematic, partly geostrategic. This latter angle is put into practice by the distribution of the analytical work across several departments, which are each responsible for a specific geographical area.[114] If necessary, various departments make joint

[113] By way of an exception, the Prime Minister sent the Standing Committee I the *Action Plan Radicalism* approved by the Ministerial Committee for Intelligence and Security. The Prime Minister wanted at the very least to set a precedent in response to the requests from the Standing Committee I to be notified of other documents emanating from the Ministerial Committee which are relevant to its supervisory mission. See Chapters I.3 (not included in this report) and VIII.3.1 about this subject. The original action plan has been amended in the meantime, in that the six or seven intervention areas have been re-grouped into a number of action plans.

[114] Each of those departments decides where it will place its emphasis. The department responsible for North Africa, the Near East and Middle East, for example, is one of the departments most involved in this subject area. It studies the evolution of radical Islamism and associated terrorism at international level. This department also studies the interference of certain governments in affairs of institutional Islam in Belgium. The Europe and Asia Minor

analyses about movements and persons who are present in various countries. Above departmental level, there is a coordination unit, which ensures that cases are assigned to the correct department, depending on their evolution.

The analytical work of State Security is carried out in the spirit of the *Alliance of Civilisations* initiative launched by the Secretary-General of the United Nations in 2005.[115]

The analyses by State Security are mainly intended for the Prime Minister, the Minister of Justice, the Minister of Foreign Affairs (and the diplomatic posts abroad) and the Minister of the Interior. In addition, the federal prosecutor's office, some public prosecutors and examining magistrates, the Federal Police, the CUTA, the Governmental Coordination and Crisis Centre, the Counter Terrorism Group (CTG)[116] and the EU Joint Situation Centre (SITCEN)[117] are standard addressees.

Building on the planning made earlier, and in implementation of the *Action Plan Radicalism* mentioned previously, State Security drew up its own *Action Plan Radicalism 2006/2007*. In this plan, the service emphasises the importance of both operational and more ad hoc analyses (case-by-case approach) and strategic analysis (long-term vision) dealing with certain phenomena or themes.

A large proportion of the analytical capacity goes into ad hoc analyses; strategic analyses remain exceptional. The investigation also showed that State Security (but the GISS as well) had not yet carried out a quantitative evaluation of Islamist radicalisation in our country. As they are faced with urgent tasks in the short term, constantly changing threats and a permanent staff shortage, the services apparently find it difficult to elaborate deeper insights into the development of radical Islamism in Belgium.

The ad hoc analyses are usually focussed on the fight against terrorism. The role of State Security in that fight – supporting the police services and the judicial authorities – is mainly repressive, although the preventive aspect is undeniable.

---

department, on the other hand, investigates the evolution of radical Islamism in Turkey, the Balkans and Chechnya and its consequences for the communities living in our country.

115 This 'alliance' endeavours "*to improve understanding and cooperative relations among nations and peoples across cultures and religions and, in the process, to help counter the forces that fuel polarisation and extremism. It aims to contribute to a global movement of conciliation which, in accordance with the wishes of the vast majority, rejects extremism in every society*". The alliance attempts to counter "*mutual suspicion, fear and misunderstanding between Islamic and Western societies*" by creating "*a model of mutual respect between civilisations and cultures*" (see www.unaoc.org).

116 The Counter Terrorism Group is a forum of intelligence services mainly responsible for the prevention of and the fight against terrorism in the countries of the European Union. This group was set up on 20 September 2001 as a result of the decisions of the Council (Justice and Home Affairs) of the European Union. It is expected mainly to gather knowledge and experience about the problem of the Iraqi *filières*.

117 The *SITCEN* of the European Union monitors international events and evaluates them on a permanent basis. One of the key areas on which it focuses is terrorism, of course.

When State Security acts preventively, this is mainly with regard to its mission in relation to extremism. In that regard, the core mission of the service is to gather information and provide objective information to the competent authorities about radical tendencies, about extremist activities and entities in our country, about any links with organisations or movements abroad and about their strategies in relation to Belgian institutions or population groups in Belgium. Unlike the GISS, State Security does not investigate the political, cultural, social and sociological causes of violent radicalisation.[118] It argues that such analyses do not fall within its remit. The Standing Committee I does not share this view.

In 2004, the then Director-General of State Security attributed the limited sphere of action of his service (the issue of Islamism could only be approached selectively) mainly to a lack of operational resources and manpower. It was expected, however, that the gradual supplementing of the staff and the associated reforms would lead to a more structured approach to the issue of Islamist extremism, resulting in wider-ranging studies.

Meanwhile, considerable efforts have gone into broadening the staff training in the service.

The new training of agents assigned to field operations will focus on knowledge of foreign languages. State Security has specialised staff with a command of several languages among its ranks, but only a very limited number who can speak classical Arabic.

The recruitment of agents with an excellent knowledge of certain languages (e.g. classical Arabic, Farsi, Urdu) is no easy task. Only a few people with this kind of knowledge apply for recruitment. Furthermore, candidates of foreign origin, who sometimes do speak one of these languages, do not always have a sufficient level of education in French or Dutch to pass the selection tests. The selection criteria must be tailored for this purpose, and attention must be paid to the issue of security checks for people who have lived abroad.

II.2.1.2. The various domains

Under this heading, various topics are discussed that are monitored by State Security.

It is important to emphasise that the service does not supervise Muslims as such, nor the practice of Islamic religion. As a (legally recognised) religion, Islam is not a matter for surveillance. State Security does not wish to be drawn into social debates such as about the prescriptions on how Muslims should dress (e.g. wearing headscarves). Only when practice of Islam leads to certain actions which threaten public security and the continuation of the democratic and constitutional

[118] This implies, for example, that the GISS does investigate the phenomenon of 'withdrawal into one's own community', while State security does not (see II.2.2.2.3).

order, or in the event of attempts to influence certain decision processes via clandestine or unauthorised means, may this service turn its attention to the practice of Islam. State Security therefore takes an interest in demonstrations within the Muslim community which, whether in theory or practice, conflict with the fundamental principles and the workings of the democratic constitutional state. In other words, State Security takes an interest in 'Islamism', as well as its (neo-)fundamentalist, salafist[119] and terrorist derivatives.

II.2.1.2.1. Monitoring of radical Islamist tendencies and groups

State Security declares that since the 1980s – as one of the first European intelligence services to do so – it devoted attention to the development of potential terrorist cells, as well as non-violent extremist networks. The Standing Committee I was able to observe that State Security has good theoretical knowledge both of Islamic ideology and its development through the course of history, and of the evolution of radical Islamism.

According to the service, the planting of Islamic extremists and terrorists in Europe is rather of an exogenous nature. Both phenomena were brought to Europe from North Africa and the Middle East, without the initial support of the local Muslim communities. The first extremist groups which established themselves in Belgium were working more for a national cause rather than for the Islamisation of Belgian society. Their prime aim was to bring down the established order in their country of origin.

At the end of the nineties, the membership of most of these groups was in continual decline. From then on, supranational groups such as the Muslim brotherhood or the salafistic movement had great success. They consider Belgium less as an operating base for bringing about changes abroad. Now they are trying to carry out their plans in our country, and make their mark on the development of a 'European Islam'. The radicalisation of a minority of groups of young Muslims, including a number of Belgian converts, is therefore a rather recent development in Belgium. Islamic extremists often band together in small groups based on their ethnic origin. Their objectives and methods differ from one group to another. Only a few groups have well-developed networks. However, State Security has observed over the last few years that there are specific actions to recruit and train young Muslims. Through lobbying work, some groups try to convey certain views or present themselves as the preferred partners of the authorities. These groups try to gain a degree of credibility by concealing their Islamist views. Their interpretation of Islam leads them to condemn the democratic rule of law and the

[119] Salafism goes hand in hand with individualisation and therefore a loss of social control, with greater radicalisation as a result. State Security states that it is particularly difficult to monitor this radical tendency, due to its fragmentation.

socio-judicial achievements relating to Western values. One only has to think of the principle of non-discrimination on grounds of race, gender, sexual orientation or inclination. According to State Security, this phenomenon is limited in scale at present, but will certainly become more important over the next few years.

Today, State Security is closely monitoring various radical tendencies and movements. What they have in common is that they consider the Koran as the only law which governs life in all its facets. These tendencies and movements appear on a list of subjects which are monitored continuously by the service. Summary memoranda are drawn up for each of the movements appearing on the list. They describe the history, ideology and structure of the movement in Belgium and abroad. These documents also contain a summary of the activities of the movement, any ties that it has with terrorist organisations and, finally, a justification of the fact that they are being monitored by State Security.

State Security has also drawn up a general summary of extremist Islamist tendencies in Europe. This document is intended, among other purposes, for the political authorities and police services.

II.2.1.2.2. Monitoring of imams and mosques spreading extremist ideas

In 2001, the Standing Committee I observed that, of the approximately three hundred mosques established in Belgium, there are around thirty that deserved to be labelled 'extremist', based on the criteria laid down by State Security (see below). About fifteen of them are said to have salafistic leanings. Most of the mosques for which the Muslim Executive of Belgium has requested recognition at that time, were well known to State Security because of their radical course and/or because they were financed by a third country.

In the additional investigation carried out in 2002, no major change was observed in this matter. However, State Security did not rule out (further) radicalisation of some Islamic institutions in the near future.

In view of the freedom of religious worship granted by the Constitution, State Security does not supervise imams as such. It only intervenes when a person attracts attention because of possible extremist activities. The service is definitely particularly vigilant – in application of the *Action Plan Radicalism* – concerning foreign preachers who openly attack democratic values or incite violence or hatred. For foreign preachers, there is also a special residence permit procedure. The Immigration Service makes sure that these imams are recognised by their own national governments and have a moderate profile. A new imam is only allowed into Belgium once his predecessor has left the country. This obligation is also checked by the Immigration Service. The Minister of the Interior has declared, moreover, that in these cases, the opinion of State Security is always sought

beforehand.[120] However, State Security states that it is rarely consulted by the Immigration Service. The Standing Committee I regrets this, and recommends that a protocol agreement settle this issue.[121]

The same method of action applies for the mosques. State Security does not monitor the activities within mosques as such, but observes any extremist activities that may develop there. In order to assess the 'level of radicalism' of a mosque, State Security takes account of various criteria, such as the ideological profile of the imams who preach there, the profile of the members of the mosque committee, any ties with groups recognised as radical, and the activities in which all these players engage. If State Security becomes aware of the dissemination of extremist ideas, it informs the political, administrative, police and judicial authorities, so that appropriate measures can be taken. Since 2004, there has been a cooperation agreement between the Minister of Justice and the Regions. This agreement provides for a prior recommendation from State Security before the recognition of mosques.

However, supervision of radical places of worship is no easy matter. State Security states that the most dangerous movements often meet in private homes, cellars, garages or other places, without leaving any official traces. The strategy of salafist militants is said to be to gain control of mosques by means of 'entryism',[122] after which radical preaching occurs behind closed doors. State Security states that this hampers its observation activities to an increasing extent.

II.2.1.2.3. Monitoring of the infiltration by extremists into institutional Islam

Successive Ministers of Justice have assigned State Security the mission of monitoring the procedure for recognition of a representative body for Islamic service.[123]

In 2002 and 2003, State Security notified the Minister of Justice that radical Islamist elements were continuing their strategy of infiltration and take-over of power within the representative bodies for Islamic service. Their purpose was to appropriate the subsidies granted to this religion. For this purpose, they maintained contacts with Belgian political circles. According to State Security,

120 Question from Jansegers to the Minister of the Interior about 'Muslim extremism – Imams – Illegal immigration' (*Q&A,* Senate, 2006–2007, 7 December 2004, no. 29, 1965, Q. no. 1528).

121 In this protocol agreement, the possibilities offered by the Act of 3 May 2005 that amended the Classification Act, allowing requests for security advice in connection with legislation on aliens and immigration, should be put into practice.

122 This is a strategy where like-minded people enter a given organisation, so that after a period of time, those persons can exert influence on the direction taken by the organisation.

123 Since the amendment of the Classification Act by the Act of 3 May 2005, candidates for membership of the Muslim Executive have been subject to a security check.

such a seizure of power would lead to a confrontation with the Belgian authorities, and to a loss of trust among moderate Muslims.

In recent years, State Security has also paid attention to the interference of some foreign governments in the activities of the Muslim Executive. In this regard, various reports were sent to the Minister of Justice. In 2005, State Security also informed the Minister of the fact that some extremists opposed elections to appoint new members to the Muslim Executive.

II.2.1.2.4. Monitoring of the teaching of the Islamic religion

The *Action Plan Radicalism* does not provide, as such, for supervision of radical indoctrination in certain religious schools. However, State Security does monitor this subject. Most Islamic organisations pay a great deal of attention to the instruction and education of youngsters. Almost all mosques organise teaching of the Koran. Since the 1990s, private schools for Islamic education have also been in existence. This does not pose any problem whatsoever if the lessons are given by moderate teachers or imams. However, State Security is concerned about possible cases where the instruction may have an extremist character.

In the past, the service therefore devoted attention to a specific institute. State Security was of the opinion that the strict, religious education of young Turkish girls from all over Europe was an example of fanatical indoctrination. In 2004 and 2005, State Security sent various reports to the authorities in which it described the power struggle raging between radical and moderate elements within the governing body of that institute. According to State Security, the radical movement seemed to have taken over at the expense of a moderate and tolerant line that had previously been followed by the governing body.

In various memoranda sent by State Security in 2004 and 2005 to the authorities, this service also expressed concerns about other initiatives in the field of Islamic religious education. For example, steps were taken to have a number of institutions recognised by a Community government in order to obtain subsidies for those institutions. The Standing Committee I is of the opinion that State Security rightly monitors this issue.[124]

II.2.1.2.5. Monitoring of extremist websites

Pursuant to the *Action Plan Radicalism*, the Federal Police is the lead service for monitoring extremist websites. State Security participates in the working group which exchanges intelligence on this subject.

---

[124] Here too, in certain cases, the possibilities offered by the amendment to the Classification Act by the Act of 3 May 2005 could be used.

Memoranda sent in 2005 and 2006 to various authorities provide evidence of the activities carried out by State Security in this field. In these memoranda, the attention of the political and judicial authorities is drawn to a number of specific websites.

II.2.1.2.6. Monitoring of 'propaganda centres'

One of the key areas of the *Action Plan Radicalism* is the monitoring of bookshops and propaganda centres which disseminate extremist literature. This task is effectively carried out by State Security.

II.2.1.2.7. Monitoring of Islamist conversion campaigns in prisons

In 2001, the Standing Committee I wrote that State Security was worried about the 'conversion zeal' shown by some Islamist organisations in prisons.[125] The service complained about the fact that penal institutions had still not developed the habit of notifying information on this subject spontaneously. In order to overcome this problem, work had been under way for some years to draw up concrete agreements. These were only settled in 2006, when State Security and the prison administration signed a protocol agreement within the framework of the updated *Action Plan Radicalism*. The aim is to facilitate and promote the exchange of information, to determine the practical implementation arrangements for collaboration, and to intensify the exchange of ideas and analyses. The protocol also provides that within this framework, State Security can contribute to the training of staff of penal institutions.

Another aspect of this problem could be the Islamist proselitism in Moroccan prisons, to which Moroccans convicted in Belgium but serving their sentence in Morocco may be subject. On their return to Belgium, these persons may cause problems.

II.2.1.2.8. Monitoring of a few specific events

Any national or international events that could have an impact on the Belgian Muslim community, are monitored and analysed by State Security. For example, this was the case following the desecration of the Koran at the Guantánamo Bay prison camp (2005), the publication in Denmark of caricatures of the prophet

[125] According to a report by an intern at State Security, the radicalisation of young Muslims in the prisons in 2005 had not yet assumed major proportions. However, the risk associated with excessive zeal to make converts cannot be underestimated. Both the prison guard, who is the prime representative of the State and Western society as far as the prisoner is concerned, and the Muslim counsellor, who can form a counter-balance against radical ideas spread by some extremist prisoners, have an important role to play in this respect.

Mohammed (2006) and the conflict between Israel and *Hezbollah* in Lebanon (2006).

II.2.1.2.9. Monitoring of the Islamist terrorist threat

The counter-terrorism action of State Security is both preventive and repressive in nature. The emphasis is on the latter aspect, which is the continuation of the information gathering about extremism and its financing.

State Security informs the federal prosecutor's office systematically whether, and to what extent, certain extremist groups are moving towards terrorist activities. The service was behind the majority of prosecutions in Belgium against terrorist networks, such as the one against the Belgian cell of the *Groupe islamique combattant marocain* (GICM).

The information exchange, collaboration, cooperation and technical assistance which State Security – and the GISS – can offer the judicial authorities are laid down in Articles 19 and 20 of the Intelligence Services Act. The implementation arrangements for these were explained in two circular letters.[126] As far as the committee can ascertain, not all of these aspects are governed by a protocol between the competent ministers or a directive from the Ministerial Committee for Intelligence and Security.

State Security makes no periodic analyses of the status of the terrorist threat in or against Belgium. According to this service, this was and continues to be the task of the CUTA and of its predecessor, the ATG. However, over the past few years, State Security was repeatedly consulted about the possible existence of a terrorist threat on Belgian soil, or offshoots in Belgium of foreign terrorist networks. Various domestic and foreign bodies have received thorough analyses about this from State Security.[127]

II.2.1.2.10. Monitoring of the recruitment of volunteers for *jihad* and travel from and to sensitive regions

In 2005, the European Council formulated a recommendation to identify and monitor travel to conflict zones, in order to prevent people being able to undergo terrorist training. It is widely known that this phenomenon has applied in Belgium

126 Col 9/2005 of 15 July 2005 on the judicial approach to terrorism and Col 12/2005 of 5 October 2005 concerning the collaboration between the judicial authorities, State Security and the GISS.

127 Specifically, State Security mentions an analysis about the dismantling in 2006 of a major terrorist cell in Morocco, which according to certain information, had offshoots in Belgium (according to State Security, this appeared to be incorrect), and an analysis of the evolution of Algerian terrorist networks in Belgium.

as well. So far, four Belgians have been identified with certainty as being directly involved in suicide attacks abroad.[128]

The issue raised by the European Council was nothing new for State Security. The problem had already arisen at the time of the crisis in Afghanistan. At that time, many armed fighters, the so-called *Mujahadin*, went to Afghanistan to undergo training and take part in the fighting. In 2001, the attention of State Security was drawn to the problem of the Iraqi *filières*. Since the beginning of the Iraq crisis, some countries have observed that the number of trips and the level of travel to and from this country had increased sharply. State Security states that it was one of the first to draw attention to this issue. The service states that it has informed a large number of foreign contacts about this phenomenon. In 2005–2006, these *filières* were one of the priorities of State Security.

Concerning the recruitment of *jihadis*, State Security focuses its attention on those radical networks in Belgium that have contacts with terrorist organisations abroad. State Security has no evidence that young Muslims in Belgian mosques are being recruited for *jihad*. There are also other important places that need to be monitored in the context of this recruitment process. Besides the general monitoring of certain places, State Security also keeps a close eye on persons who could be involved in recruitment networks. On several occasions, the service has provided the federal prosecutor's office with information in this regard that has (contributed or) led to law enforcement or judicial inquiries.

Monitoring of travel to sensitive regions is no easy task, for various reasons. Travel to Iraq does not necessarily involve direct flights, a multiplicity of routes could be used, and it is easy to cross EU internal borders. It should also be borne in mind that the networks are informal in nature, and persons involved in these *filières* almost systematically use different passports or identity papers. According to State Security, systematic controls are illusory. Sometimes, the service also seems to lack relevant information.

After having undergone training and/or fought in Afghanistan or Pakistan, some of these 'Afghan Arabs' returned to Europe where they set up networks, organised *filières*, and recruited other people. Although comparisons with Iraq are not fully applicable, it cannot be ruled out that some of these *Mujahadin* may decide to follow the same path on their return home.

Despite the difficulties in monitoring recruitment, travel and possible return home, State Security has regularly been able to provide useful intelligence to the competent authorities. In 2005, for example, State Security provided the judicial authorities with details of a number of Muslim fundamentalists who were known to have travelled to Pakistan to undergo religious education, but probably paramilitary training as well. Also in 2005, in connection with the issue of the

128 Rachid El Ouaer and Dahmane Abd al Sattar (Afghanistan, September 2001); Issam Goris and Muriel Degauque (Iraq, November 2005).

Iraqi *filières*, attention was focused on various individuals. Furthermore, the issue of the Iraqi *Mujahadin* was repeatedly raised with the Minister responsible, and in 2005 and 2006, various specific memoranda were written. At the end of 2005, State Security sent two analytical memoranda about the suicide attack by Murielle Degauque to the SITCEN.

II.2.2. MONITORING OF RADICAL ISLAMISM BY THE GISS

II.2.2.1. General considerations

Since 2001, the subjects and groups that are to be monitored by the GISS are laid down in an *Intelligence Steering Plan*[129] and a *Security Intelligence Steering Plan*. Both documents, approved by the Army Chief of Defence and the Minister of Defence, consider radical Islamism and terrorism to be absolute priorities for the military intelligence service.

In 2002, the GISS did not conduct any comprehensive investigation into radical Islamism. The service restricted itself to gathering specific data. In 2005, however, the GISS was assigned a role under the *Action Plan Radicalism*. The GISS thus became more closely involved with this phenomenon, although under the Intelligence Services Act of 30 November 1998, that task is only assigned to them if there is a military threat or a threat to our military interests. The GISS is now collaborating with State Security and other services on the implementation of this action plan. Furthermore, the GISS is sometimes brought in as an expert in judicial inquiries.[130]

Two departments of the GISS are concerned with extremism and Islamist terrorism. One department deals with the cross-border phenomena that could form a threat to the security of the armed forces abroad (e.g. the Balkans, Afghanistan or Lebanon). The other department pays specific attention to threats (such as terrorism, as well as subversive activities and espionage) against the armed forces in Belgium.

Unlike State Security, the GISS carries out studies that the service deems useful for the perception and understanding of sociological phenomena that could cause societal problems in the medium and long-term. For example, the service has organised a process of reflection about the headscarves issue. In doing this, the GISS wishes to break taboos and eliminate prejudices that might arise from inadequate knowledge of this issue. Generally speaking, the GISS has

129 This plan is drawn up on a regular basis, depending on the priorities of the missions of the Belgian army abroad.

130 As already stated, the Standing Committee I has no knowledge of any protocol on the subject that, pursuant to Article 20, § 2, of the Intelligence Services Act, has been approved by the ministers concerned (and therefore also by the Minister of Defence).

repeatedly advocated a policy of long-term investigations. Although the service cannot carry out this task itself due to lack of time, other priorities and staff shortage, which it regrets, it describes this as an important mission for intelligence services. The Standing Committee I applauds this intellectual curiosity of the GISS concerning these societal issues. However, the committee is of the opinion that such an attitude would be more appropriate to State Security than for the GISS, whose actions must mainly be focused on threats in a military context.

The GISS has analysts among its ranks who are familiar with the Arabic language, enabling the service to supply and analyse reasonably targeted information about Islamist tendencies present in Belgium.

Since the events of 11 September 2001, the GISS has made considerable efforts to recruit informants.

At the same time, an urgent necessity has emerged: to be able to guarantee the anonymity of some members of the GISS who were threatened because of their work.

II.2.2.2. The various domains

In the following section, we explain among other things the phenomenon of monitoring radical Islamism abroad, Islamist NGOs, 'withdrawal into one's own community' and the terrorist threat or radical Islamist groups in Belgium. Pursuant to the *Action Plan Radicalism*, the GISS plays a key role in the monitoring of radical radio and television broadcasts. The military intelligence service is also closely involved in the implementation of the other pillars of the *Action Plan Radicalism*.

II.2.2.2.1. Monitoring of radical Islamism abroad

The GISS devotes attention to Islamist activism in countries where Belgian troops are involved in peacekeeping missions. Although for a long time, attention was focused on Bosnia, Kosovo and the Balkans in general, nowadays, the GISS is more focused on Afghanistan, Lebanon and sub-tropical Africa.

The GISS is monitoring the Al Qaeda movement in particular, and activities that could be related to it. In Afghanistan, the GISS is devoting attention to the Taliban, as well as the *Hizb Al Islami Gulbudin* movement, which has carried out murderous attacks against soldiers of the international NATO force. As far as Lebanon is concerned, the GISS is monitoring the salafist and jihadist movements.

II.2.2.2.2. Monitoring of Islamic NGOs

The activities of certain NGOs are not just limited to a humanitarian role. Some organisations attempt primarily to spread Islam in the regions where they operate, and support local radical Islamists for this purpose. Various Arab and Muslim countries support and finance these activities. In view of the military presence in the Balkans, Lebanon and Afghanistan, the GISS is particularly alert to this situation.

The GISS provides its analyses regularly to various Belgian and foreign military authorities, as well as the judicial authorities, the CUTA and State Security.

II.2.2.2.3. The phenomenon of 'withdrawal into one's own community'

The *Security Intelligence Steering Plan* prescribes the study and analysis of the political and sociological context within which the threats to be monitored arise. In that context, the GISS also deals with factors of the so-called 'withdrawal into one's own community'.[131] This withdrawal implies the rejection of the values of Western society, and can lead to radicalisation. The individualisation of radicalisation processes makes it necessary to increase the efforts to detect and identify such risk groups and individuals.

II.2.2.2.4. Monitoring of radical imams and radical Islamist groups in Belgium

Pursuant to the *Action Plan Radicalism*, the GISS believes that today, it can use its specific competencies, in particular to detect preaching by imams who could influence the Arab and Muslim population in Belgium in a radical direction.[132] 'Radical influence' is deemed by the GISS to mean any incitement to hatred and xenophobia or any justification of and call to violence.

Of course, the GISS also devotes attention to radical Islamist groups. Some of those are considered not as terrorist but rather as subversive and undermining authority. But they may function as a breeding ground for extremists, some of whom could go on to become terrorists.

II.2.2.2.5. Monitoring of a few specific events

Just like State Security, the GISS devotes attention to specific events like the reactions in Belgium to the publication in Denmark of caricatures of the prophet

131 The study of this phenomenon is not included in the *Action Plan Radicalism* and is – wrongly – not monitored by State Security.

132 The monitoring of this issue is also controlled by State Security.

Mohammed (2006), which the service describes as orchestrated reactions and disinformation. The GISS also made an analysis of the violence in French cities in 2005. The service provided detailed commentary on the attitude of a number of Muslim organisations in relation to these events.

II.2.2.2.6. Monitoring of the Islamist terrorist threat

The GISS takes on board the evaluations of the terrorist threat by the CUTA and comments on them. This does not prevent the GISS from regularly making its own analyses and evaluations of threats to Belgium, foreign countries and military installations. These evaluations are passed on to the CUTA and to State Security. In 2005, for example, the GISS stated that the dismantling of a terrorist cell in Morocco, with one Belgian member, could have consequences in Belgium. Still in 2005, the GISS was working on the Iraqi *filières*. The service was of the opinion that it posed no direct or imminent threat to military installations in Belgium. The presence and the activities of Islamist networks in Belgium did increase the risk of a potential attack in our country. At the beginning of 2006, the GISS did not see any short-term threat to military interests in Belgium. Nevertheless, the GISS considered that the risk of terrorist action was not zero; therefore, the service called for vigilance.

II.2.2.2.7. Monitoring of travel by persons to sensitive regions

The GISS states that it does not devote particular attention to travel in itself, due to a lack of personnel and input. The service does not exercise any systematic checks, but does receive information from abroad from time to time.

In general, the GISS does suspect that in the Pakistani and Afghan communities in Belgium, there are persons present who provide logistic support to extremist Islamist movements in their country of origin. In some cases, this could concern terrorist movements. The GISS does not yet have sufficient evidence for these assertions. According to the service, there is also a threat from extremist members of the Maghrebian community.

II.2.2.2.8. Monitoring of radical radio and television broadcasts

Pursuant to the *Action Plan Radicalism*, the GISS chairs the group studying the monitoring of radical radio and television broadcasts. In this context too, it collaborates with State Security.

The monitoring is intended to detect broadcasts that could have a radicalising influence on the Arab and Muslim communities in Belgium. The relevant information on this subject must be communicated immediately to other services

involved in the *Action Plan Radicalism*, such as the police services, State Security[133] and the CUTA.

From two summary memoranda concerning a number of private radio stations from the Brussels area, it appears that there is nothing to indicate that these radio stations are being used for radical purposes. One report does state that various radio stations should be monitored more closely, and others listened to *at random*, to evaluate the influences, financing, programme markers, etc. and investigate whether they are spreading radical propaganda.

The GISS also devotes attention to the programmes of Arab broadcasters based abroad that are watched in Belgium by digital receivers or satellite dishes.

Of course, substantial technical and translation capacities are required for monitoring radio and TV programmes in foreign languages. At present, these are lacking. Therefore, radio and TV programmes are watched and listened to selectively, e.g. with reference to specific events. However, extra technical resources and manpower has been requested (specifically freelance translators) to be able to select and monitor interesting broadcasts more effectively.

II.2.3. COLLABORATION BETWEEN THE VARIOUS COMPETENT SERVICES

II.2.3.1. Collaboration between the GISS and State Security

Despite the fact that the management of both services described the application of the existing cooperation agreement dating from 1997 as satisfactory, targeted investigations in 2001 pointed to deficient collaboration. In 2002, the Standing Committee I was compelled to observe that the cooperation agreement was even no longer being applied in the field of extremist Islamism. State Security was still of the opinion that general monitoring of Islamist extremism was not one of the legal powers of the GISS. The GISS was apparently aware of this sensitivity.

On 12 November 2004, a new protocol agreement was signed. This agreement met the recurring concern of the Standing Committee I to improve exchange of information between the intelligence services.

The current collaboration between the GISS and State Security is part of the implementation of the *Action Plan Radicalism*, where the two services take it in turns to manage the project or cooperate in its implementation. Both services have provided the committee with documents, reports, analyses and internal

[133] State Security also monitors this phenomenon. On 16 January 2007, the Brussels correctional court convicted two presenters from an Islamist radio station for incitement to racial discrimination and racial hatred. State Security had already drawn the attention of the authorities to this radio station in 2002.

memoranda, showing that in 2005 and 2006, they exchanged intelligence intensively, and carried out joint analyses.

II.2.3.2. Collaboration between the intelligence services and the Federal Police

Collaboration between the intelligence services and the Federal Police occurs within a *task force* charged with the coordination and task allocation in the judicial sphere between the various services, under the authority of the federal prosecutor's office.

At the time when the committee was making its enquiries, the Federal Police considered collaboration with the intelligence services in relation to monitoring of Islamist extremism as positive. For example, the Terrorism and Sects service of the Federal Police received various reports from State Security referring to radicalisation of preaching in some mosques or by certain imams. The Federal Police examines whether, based on information received, a (proactive or reactive) investigation can be initiated. If terrorism is involved, the federal prosecutor is informed. If it emerges that the information which State Security provides does not contain any elements that could give rise to the initiation of a judicial case, the Federal Police will continue to use it in the context of the exercise of its administrative policing mandate.

In this context, the Standing Committee I is compelled to observe again that the protocol agreement between the Federal Police and State Security, which was announced a long time ago, has still not been finalised. With a view to better exchange of certain intelligence, this is essential.

II.2.3.3. Collaboration between the intelligence services and the CUTA

Numerous memoranda and reports which the intelligence services supplied to the Standing Committee I, provide evidence of intensive information exchange between these services on the one hand and the CUTA and its predecessor ATG on the other.

The Standing Committee I will continue to evaluate the collaboration between the intelligence services and the CUTA with regard to other investigations and cases.

II.2.3.4. Collaboration between the Belgian and foreign intelligence services

Article 20 of the Intelligence Services Act provides that the intelligence services are responsible for collaboration with their foreign counterparts. The European Commission also urged more intensive collaboration between the intelligence services of the Member States, with regard to operations, intelligence and

strategies. The Commission also recommended that the services should share their *best practices* and their expertise concerning violent radicalisation within European organisations such as Europol or the SITCEN.

In this context, it can be stated that the work of State Security clearly has an international dimension (bilateral and multilateral), both at the operational and analytical level. The service is part of the *Counter Terrorism Group (CTG).* Within this group, it states that it was the co-initiator of an integrated European approach to the 'Iraqi *filières*'.

Exchange of information between the police and the security services of various countries is a necessity, which is being given increasing prominence by international conventions and treaties. On the other hand, international collaboration between intelligence services is subject to the 'third party rule', which makes certain investigations by the Standing Committee I *de facto* more difficult.

II.2.4. CONCLUSIONS

This follow-up investigation has shown that the following findings from previous investigations are still applicable, and moreover, are also (partially) applicable to the military intelligence service:

- The two services do not monitor Muslims or the practice of the Islamic religion as such;
- They both give absolute priority to fighting terrorism;
- State Security regularly provides assistance to judicial inquiries. Its contribution in this respect is appreciated. The GISS is less prominent in this respect, but this is entirely consistent with its legal powers and responsibilities, which situate its work in the military sphere;
- State Security rightly still investigates how specific Islamist tendencies are attempting to impose their political-religious views on society by being active within some immigrant communities in our country and within the organs of institutional Islam in Belgium;
- State Security still conducts investigations into extremist activities in mosques, and provides information to the competent authorities. The GISS has also been assigned a role in this regard;
- Now that the dispute about the powers and responsibilities of the GISS to monitor radical Islamism in Belgium seems to have been settled, the collaboration between both intelligence services in the fight against radical Islamism seems to have been greatly improved. Likewise for the exchange of

information between the intelligence services, police services, the ministers concerned and the judicial and administrative authorities.

On the other hand, a number of problem areas still remain:

- The extra personnel resources which has been attracted in recent years do not appear sufficient to cover all aspects of the missions to be carried out in this context;
- State Security has not yet carried out any in-depth analysis of the development of the Islamists' long-term strategy. But the GISS is experiencing difficulties in developing insight into the development of radical Islamism in Belgium, both in-depth, and in the long term;
- The extra technical and legal resources for the intelligence services have not yet been made available;
- Likewise for the more detailed legislation about the way in which the intelligence services can collaborate with the judicial authorities.

Finally, this follow-up investigation enables us to formulate a number of additional conclusions:

- The intelligence services appear to analyse the information they obtain with care and moderation. This is also apparent from the fact that both intelligence services usually agree about the essential points of their analyses;
- The intelligence services are faced with the difficulty of recruiting personnel with sufficient knowledge of foreign languages and cultures, so that an urgent review of certain statutory recruitment conditions is required;
- The GISS carries out sociological studies based on open sources about certain phenomena, in order to make a medium and long-term threat analysis possible. State Security is reluctant about the idea of investigating the political, cultural, social and sociological causes of violent radicalisation in greater depth. It argues that such analyses do not fall within its remit. The Standing Committee I does not share this view entirely. The committee can but applaud the intellectual curiosity of the GISS about these societal issues. However, the Standing Committee I feels that such an attitude would be more appropriate for State Security rather than for the GISS, whose powers must be focused on threats against the armed forces. The committee does recognise that such studies can also be very useful for the perception and understanding of sociological phenomena that could cause political and military problems in the medium and long term;
- The Standing Committee I remains of the opinion that monitoring of radical Islamism is part of the powers and responsibilities of the GISS, to the extent

that military security in the broad sense in Belgium and abroad is under threat.

With reference to subsequent investigations, the Standing Committee I will continue to devote attention to the various important findings which came to light during the course of this thematic investigation.

II.3. THE INFORMATION PROCESSES AT STATE SECURITY

Following a comprehensive audit, the Standing Committee I observed various deficiencies in the management of information by State Security in 2002 and 2003.[134] With a view to improving the situation, the Standing Committee I formulated various recommendations at that time.

Nevertheless, with regard to subsequent investigations, the committee observed that the same complaints came to light again. For that reason, an investigation was started in 2006 with the aim of obtaining insight into the way in which the information flow, processing, decision-making and reporting of the information occurs at State Security. Since the service was, and still is, setting up a new, integrated IT system, it was impossible to already complete the investigation. This can only be done usefully after that implementation.

The Standing Committee I did consider it opportune to issue an intermediary report containing a number of recommendations about problems not directly connected with the new IT structure. Specifically, this concerns the deficient in-house ICT personnel policy (structure and management of the IT unit could certainly be optimised), the absence of an information strategy (State Security had no information manager), and the lack of government directives about improving the usability and quality of the information. These recommendations are given in detail in the final chapter of this annual report.[135]

II.4. THE ROLE OF THE GISS IN THE CONTEXT OF MILITARY SECURITY

Following the discovery of arms traffic where weapons were on sale that came from a military storage depot, the Standing Committee I launched a investigation

134 The findings of this audit were published in the activity reports for the years 2002 and 2003. In the present investigation, it is only the conclusions of the third phase that are important. These are contained in the *Activity Report 2003,* 152–163.

135 See Chapter VIII.2.1 and VIII.2.2.

in 2004 into the way in which the GISS acted in this matter, both with regard to intelligence gathering (Article 11, §1, 1°, of the Intelligence Services Act) and with regard to military security (Article 11, §1, 2°, of the Intelligence Services Act).

The investigation was concluded in mid-2007, and did not reveal any dysfunction on the part of the military intelligence service.

Even before the theft of the weapons was discovered, the GISS had already carried out an inspection at the military quarters concerned. The service came to the conclusion that there were serious deficiencies in the security of the weapons storage.

It is important to emphasise that the role of the GISS in the context of security of military bases is limited to auditing and advising. The GISS does not have any coercive measures at its disposal in such matters.[136] The implementation of security standards, directives and regulations is the sole responsibility of the military hierarchy at the barracks. The GISS can only observe deficiencies and make proposals to rectify them. Of course, the authority of the GISS would be enhanced if it could associate binding consequences with its interventions. In principle, this does not concern the effectiveness of the GISS, but instead that of the military internal security policy, so that the Standing Committee I did not feel competent to formulate any recommendation in this regard.

II.5. COMPLAINT ABOUT A PROMOTION PROCEDURE WITHIN STATE SECURITY

In 2002, a State Security agent complained to the Standing Committee I about the attitude of his then hierarchical superiors towards him with regard to his possible promotion. The negative recommendation of his superiors was said to have contained falsehoods and defamatory allegations. The complainant appealed to the State Security Advisory Board. The Board concluded that the complainant did indeed have the necessary qualities to hold a higher position. Consequently, the Board issued a favourable opinion, and the agent concerned was promoted. Since then, the complainant claims to have been the victim of harassment, unfairness and mismanagement.

The Standing Committee I came to the conclusion that the complaint by this official lacked any foundation. As far as his promotion is concerned, it appeared

136 Article 11, § 1, 2°, of the Intelligence Services Act assigns the GISS the mission of ensuring maintenance of military security of military installations. In the Explanatory Statement, this task is explained as follows: "*The GISS ensures that military security is guaranteed. It is its responsibility to draw up directives, to ensure that they are disseminated within the Armed Forces, and investigate compliance, in particular via investigations into security incidents relating to the Armed Forces.*" (Official documents of the House of Representatives, 1995–1996, 638/1) [free translation].

that he could use the appropriate appeals procedure, and that he was given the opportunity to put forward arguments. Ultimately, he was promoted and therefore did not suffer any prejudice. With regard to the alleged harassment and unfairness, the Standing Committee I could not point to any fact that suggested that his hierarchy had done anything wrong.

In relation to this investigation, however, the Standing Committee I was faced with another question. The then management of State Security had expressed its dissatisfaction about this investigation, among other things because it asserted that any disputes concerning promotion should be a matter for the Council of State and not to the Standing Committee I. The committee did not share this opinion. It was (and remains) of the opinion that its Investigation Service is empowered to launch an inquiry into grievances of a staff member of State Security against his/her hierarchy. The Investigation Service I has been assigned this power by Article 40, §2, of the Review Act. The Standing Committee I does not have the intention of interfering with purely personnel problems or personal conflicts within the intelligence services, but neither can it accept that its overall powers are diminished, or a person is denied the right to make a complaint. Such complaints may in fact point to a dysfunction within a service, and thus have a direct impact on the effectiveness of State Security.

II.6. COMPLAINT BY A STAFF MEMBER OF STATE SECURITY

At the beginning of 2006, an investigation was launched into a complaint by a staff member of State Security. He also claimed to be subject to harassment by his hierarchy. In addition, he contested the way in which his performance had been appraised.

Although the staff regulations of State personnel – which also applied to the complainant – provide for administrative procedures with hearing of evidence from all parties so that unfavourable appraisals can be contested, and although failure to comply with these rules can be challenged before the Council of State, the Standing Committee I considered that it fell within its scope of competence to consider the case. Like the previous investigation, the complaint related both to the rights of the person concerned and to the effectiveness of the service to which he belonged.

Within the framework of this investigation, it emerged that the member of staff had been involved in two security incidents. The committee observed that the way in which State Security management had dealt with these incidents was inadequate: there was hesitation, various hierarchical levels adopted contradictory attitudes and no appropriate decision was taken. In the second incident,

management even left it to another body to take the decision. It was therefore hardly surprising that the relationship between the complainant and his hierarchy deteriorated, and that the complainant felt that he had been subject to harassment.

Moreover, the facts of the case were of such a nature that *prima facie* they would have justified the launching of disciplinary proceedings or even criminal proceedings. Neither happened. Nevertheless, such procedures have the additional advantage that the person concerned can have disclosure of the evidence in the case, and put forward a defence efficiently. The incidents should also have led to immediate withdrawal of the agent's security clearance. That was not done either. The Standing Committee I was therefore of the opinion that the way in which the incidents were treated showed a deficient personnel and security policy.

II.7. COLLISION WITH A STATE SECURITY PRIORITY VEHICLE

In 2004, the Standing Committee I initiated a investigation following a complaint in connection with a traffic accident. What happened? When the complainant drove across a junction when the traffic light was green, she collided with a State Security service vehicle, which shot a red light. The two occupants – inspectors from State Security – argued that they were driving a 'priority vehicle', and that both the blue flashing light and the siren of their vehicle were operating. According to Article 37.4. of the Royal Decree of 1 December 1975,[137] they are allowed to drive through the red light – after having stopped and on condition that this caused no danger to other road users – and those other road users must give way in these circumstances. According to the complainant, only the flashing light was in operation. In that case, the State Security vehicle would have been obliged to stop for the red light.

The investigation by the Standing Committee I bore no relation to the possible criminal[138] or civil liability. This is outside the remit of the Standing Committee I. The committee not only investigated the legitimacy and the way in which State

137 Royal Decree of 1 December 1975 on general road traffic rules for the police and use of the public highway.

138 The criminal investigation was dismissed by the prosecutor's office.
Even though the Standing Committee I does not intend of interfering with the criminal aspect of the case, it would have been better for the investigation, had the police findings (and if necessary the court ruling) been involved in the assessment. In this respect, the question arises as to what extent Article 38 of the Review Act is applicable to traffic offences. Such traffic offences are sometimes treated as infringements and on other occasions as offences. Article 38 of the Review Act however, is restricted to offences and crimes. Extending its scope to include infringements (possible only those committed in the exercise of the functions) would remove any ambiguity and create a legal basis for notification and cognizance.

Security operates priority vehicles, both in general and in this specific case, without being able to determine whether the siren was operating or not. State Security has an individualised ministerial authorisation for each vehicle in its fleet to carry a removable flashing blue light and a permanently fitted siren throughout its general and special missions.[139] These vehicles are therefore 'priority vehicles' as defined by the Royal Decree of 1 December 1975. The authorisation prescribes that the use of this equipment must occur in accordance with the provisions of that Royal Decree. This implies that the blue flashing light may be used for any assignment, and that it must be used for urgent assignments. Use of the siren, on the other hand, is only allowed for urgent assignments.

In practice, this means that the inspectors concerned – who were on a protection assignment as provided for by Article 7, 3°, of the Intelligence Services Act – had the necessary ministerial authorisation and a legitimate reason for using the flashing light. But was it an 'urgent assignment' and could or should they therefore have used the siren as well?

The protection unit concerned was on its way to an ambassador, whose security they had to guarantee when he was travelling. Due to factors beyond their control, the two inspectors were late leaving for their assignment. To meet up with the ambassador in time, they were compelled to use their flashing light and siren. The question remains whether this can be regarded as an urgent assignment as defined by the Royal Decree. Many factors come into play in assessing this: human, social, professional, protocol, etc. Those factors may justify various choices, depending on the person taking the decision. Both inspectors stated that in practice, the decision was left entirely to the people on the ground. They stated that there were no specific instructions or directives.

II.8. INVESTIGATION OF THE WAY IN WHICH STATE SECURITY COOPERATED WITH A JUDICIAL INQUIRY

Over the course of 2002, the Investigation Service I received a reporting from a State Security staff member. The person concerned suspected his hierarchy of not having provided to the judicial authorities all the documents at its disposal in connection with an investigation.

In 2003, the Standing Committee I initiated an investigation into this case. It was examined which documents State Security had handed over to the judicial

[139] Pursuant to Articles 28, § 2, c, 1°, 4, and 43, § 2, 3°, Royal Decree of 15 March 1968, these authorisations are issued by the Minister of Mobility and Transport.

authorities in connection with this investigation. These documents were compared with those held by the service.

The Standing Committee I came to the conclusion that all relevant documents had indeed been handed to the judicial authorities. No indication was found of information having been withheld. State Security even handed over various original documents, without keeping a copy for its own use.

It did appear that the then management of State Security had given instructions, once it was notified of the judicial inquiry, to suspend any form of analysis and information gathering concerning the person who was the subject of the judicial inquiry. This was done to "*prevent parallel and contradictory initiatives*". This decision gave rise to resentment among some staff of State Security. In their opinion, this person was of interest in the context of the legally-imposed missions of the service. The Standing Committee I did not understand either why the then management took such a decision. Although it is true that State Security cannot interfere with an ongoing judicial inquiry, in this case, there was no reason whatsoever not to at least continue using and analysing the documents which the service already had available.[140]

II.9. COMPLAINT ABOUT AN INCORRECT MENTION IN A SECRET STUDY

In 2003, the name of a diamond importer was linked in a newspaper to *Hezbollah* and to an attempt to obtain a diamond concession in Namibia to circumvent existing embargos. The Israeli intelligence service *Mossad* was also said to be interested in the activities of the importer. The newspaper sourced its information from a report published on the Internet by the London-based NGO *Global Witness*. This NGO in turn was said to have based its report on the findings of a secret study by the Belgian military intelligence service.

The diamond importer, outraged at these allegations, filed a complaint with the Standing Committee I.

The committee was able to confirm that the GISS had indeed written a study about the Belgian aspect of world-wide diamond smuggling. This study was classified 'SECRET' pursuant to the Classification Act of 11 December 1998.[141] In the preface of this study – which again stated that it was prohibited to divulge the

---

140 In the past, the Standing Committee I had already pointed out that an ongoing judicial investigation should not stand in the way of further intelligence work (*Activity Report 2003,* 191 and 232 and *Activity Report 2004,* 124).

141 Since leaking of classified documents is a crime, the GISS filed a complaint with the prosecutor's office at that time. The complaint was later dismissed due to 'unknown perpetrator'. The Standing Committee I had no indications that the leak came from within the GISS, or that negligence or carelessness were attributable to this service.

content without prior consent – the GISS pointed out explicitly that the service was not relying on proven facts, but indications that might require further investigation. The study itself indeed contained a name that matches that of the diamond importer, yet without the Standing Committee I being able to ascertain that the complainant and the (legal) person mentioned in the study were one and the same person. In addition, the name was only mentioned incidentally, and in extremely guarded terms; in no way were actual allegations made about connections to *Hezbollah*, nor was there any mention in the study about an attempt to acquire a diamond concession in Namibia, or about alleged interest that *Mossad* might have shown in the importer afterwards.

The Standing Committee I was of the opinion that the GISS had acted in a circumspect, professional manner in the reporting of the contested study. The service made every effort to point out, where necessary, the hypothetical and entirely unproven character of its material and ideas.

CHAPTER VIII.
RECOMMENDATIONS

Based on the investigations completed in 2007 and the initial enquiries of the CUTA, the Standing Committee I wishes to present the following recommendations relating to the protection of the rights conferred on individuals by the Constitution and the law (VIII.1), the coordination and efficiency of the intelligence services, the CUTA and the supporting services (VIII.2), and – finally – the optimisation of the options open to the Standing Committee I to carry out its role to review these services (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. COMPLIANCE WITH THE OBLIGATIONS ARISING FROM ARTICLES 19 AND 20 OF THE INTELLIGENCE SERVICES ACT

Article 20 of the Intelligence Services Act assigns the following missions to the competent ministers and the Ministerial Committee for Intelligence and Security (MCI&S):

- The conditions for communication of information by the intelligence services to administrative and judicial authorities and police services are to be laid down by the MCI&S (Article 19, §1, and Article 20, §3, of the Intelligence Services Act);[142]
- The conditions for the most efficient collaboration possible between the intelligence services, the police services and the administrative and judicial authorities are to be laid down by the MCI&S (Article 20, §§1 and 3, of the Intelligence Services Act);

[142] Information flows in the opposite direction – particularly from the judicial authorities and public services to the intelligence services – can occur on the basis of agreements and the rules laid down by the responsible authority (Article 14, of the Intelligence Services Act).

– The conditions for collaboration with foreign intelligence services are to be laid down by the MCI&S (Article 20, §§1 and 3, of the Intelligence Services Act);
– The limits of cooperation and technical assistance to judicial and administrative authorities must be apparent from a protocol approved by the competent ministers (Article 20, §2, of the Intelligence Services Act).

First of all, the Standing Committee I wishes to underline the complexity of these arrangements in various respects. The initiative to elaborate the law, for example, has to emanate from the competent ministers the one time and from the MCI&S the other. In addition, the terms used are unclear (what is meant by 'technical assistance'?) and appear to overlap (e.g. the terms 'collaboration' and 'cooperation' cannot be easily distinguished).

Partly for these reasons, the Standing Committee I is of the opinion that the legislator should urgently clarify these passages of the law and the terms used therein. The same applies to the collaboration with foreign intelligence services. What does this mean *in concreto*? Does this refer to the exchange of analyses or personal data? Is there scope for collaboration at an operational level? Does this mean that foreign services may be allowed to carry out operations on Belgian soil?

The necessity for intervention by the legislator in this matter is also prompted by the observation that the executive power has not yet covered all aspects of this subject area (in an adequate way). The committee has no knowledge, for example, of any directives governing collaboration with foreign intelligence services. However, the committee does know about the existence of directives from the MCI&S relating to the exchange of information with administrative authorities. But these directives basically state that all relevant data must be handed over. No 'conditions' are laid down in this way. Furthermore, a number of protocols exist on certain aspects of collaboration in the broadest sense of the term, but these agreements do not always emanate from the MCI&S or the competent ministers. For example, the committee is unaware whether the Minister of Defence has approved the way in which the GISS can cooperate with and provide technical assistance to the courts.

The bill setting out the special intelligence methods seems like an excellent opportunity to put this right.

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

VIII.2.1. A SOUND PERSONNEL POLICY IN THE FIELD OF IT MANAGEMENT

State Security must define clearly the expertise and the framework required to provide the necessary support in terms of information technology. Any measures necessary must then be taken to prevent staff shortages or partial unavailability of personnel in the IT unit from jeopardising the continuity of service provision, or from leading to excessive technical dependence on external experts.

For an intelligence service, particular and timely attention to human resources in the field of IT is a real necessity, particularly as a possible extension of the scope of competence of the service in the field of investigation in data processing environments has already been on the political agenda for some time.

VIII.2.2. THE FUNCTION OF INFORMATION MANAGER

State Security needs to have a specific function of information manager, whose responsibilities would include outlining an information strategy. The importance of having internal information management for this service has the following reasons: the permanent dependence on information, both from the organisation and in its set-up; the need for a fully-fledged interlocutor as a counter-balance to the ICT department – which may or may not be outsourced; and the optimisation of the understanding of and the organisation of the specific information processes.

VIII.2.3. INFORMATION GATHERING AND STRATEGIC ANALYSES WITH REGARD TO RADICAL ISLAMISM

The Standing Committee I again emphasises the necessity for – in addition to efficient information gathering – in-depth, long-term analyses of the strategy of Islamic extremists. Sociological studies about certain phenomena (such as withdrawal into one's own community) may be very valuable in this respect. Both intelligence services must devote the time and the resources to produce such studies and analyses – each within the framework of their powers and

responsibilities. The fact that strategic analyses about extremism and terrorism must (or should) also be carried out by the CUTA, does not alter this essential mission for the intelligence services.

The Standing Committee I is also of the opinion that any form of contribution to the dissemination of Islamist ideology and of direct or indirect support to terrorist groups – for example by means of pseudo-charity NGOs – deserve the sustained attention of both State Security and the GISS, once again within the framework of their respective powers and responsibilities.

VIII.2.4. RECRUITMENT OF PERSONNEL WITH KNOWLEDGE OF SPECIFIC LANGUAGES

In order to monitor radical Islamism effectively, the intelligence services must have sufficient knowledge of languages including Arab languages. In order to achieve this goal, effort must first be put into ensuring that people who possess such knowledge actually apply for recruitment competitions.[143] Furthermore, the tests for these persons must be tailored to the extent that any deficiencies in knowledge of our national languages does not rule them out *a priori*. Finally, attention must be paid to the way in which security investigations are carried out on people who have lived abroad.

VIII.2.5. REQUESTING SECURITY ADVICE

The Standing Committee I recommends that with regard to residence permits for foreigners, and with regard to the derogation from the nationality condition for teachers, use should be made of the possibilities offered by the Act of 3 May 2005 amending the Act of 11 December 1998 on classification and security clearances, certificates and advice. Among other things, this law introduced the system of security advice. In the Explanatory Statement of the original bill, these two areas were explicitly mentioned. This system requires a well-founded decision by the competent authority to request a security advice and run security verifications before granting a particular permit or authorisation (Article 22*quinquies*, of the Intelligence Services Act).

---

143 Recently, the GISS made a move in that direction by publishing vacancies for commissioner-analysts emphasising the following: "*We wish to particularly encourage applications from candidates with extensive knowledge in the field of certain geo-political regions and an extensive knowledge of European as well as non-European languages, such as Arab and Oriental languages, and who hold the necessary qualifications.*" [free translation].

VIII.2.6. PROTECTION OF THE IDENTITY OF AGENTS OF THE SECURITY SERVICES

In the past, threats have been made against intelligence agents who were actively involved in the fight against extremism and terrorism. The Standing Committee I is of the opinion that it must be examined how the anonymity of these persons can be guaranteed, especially when they are called to testify in court. Of course, a balance needs to be struck with the rights of the defence, and the principles of *fair trial* must be observed.

VIII.2.7. COOPERATION AGREEMENT WITH THE POLICE SERVICES

The Standing Committee I has already pressed in the past for the creation of a cooperation agreement between the intelligence and police services. It repeats this recommendation now that it has become apparent that the actual implementation of the *Action Plan Radicalism* of the Ministerial Committee for Intelligence and Security requires optimal information exchange between the intelligence services and the Federal Police. But the local police are also important partners because they may have a better view of the phenomenon of 'withdrawal into one's own community', and the radicalisation of certain communities.

VIII.2.8. APPROPRIATE RESPONSE TO SECURITY INCIDENTS

The intelligence services must venture to respond appropriately to incidents involving members of their own personnel. If the incident raises questions in connection with the guarantees that the person has to give in relation to confidentiality, loyalty and integrity, their security clearance must be withdrawn immediately. Otherwise, the *raison d'être* of these clearances would be undermined. The Standing Committee I is aware of the pernicious consequences that such a decision could have on the (career of the) person concerned, but wishes to point out at the same time that there is a possibility of appeal to the independent appeal body on security clearances, security certificates and advice.

VIII.2.9. STAFF REGULATIONS FOR THE CUTA

Since personnel seconded to the CUTA from the various supporting services keep their own statutes, the management committee of this body has to contend with fourteen different sets of statutes. This makes personnel management particularly complex. A regulatory initiative to overcome this problem would be useful and desirable.

VIII.2.10. A SECURE COMMUNICATION NETWORK FOR THE CUTA

The Standing Committee I emphasises the necessity of urgent installation of an efficient, secure communications network between the CUTA, its suppliers and its customers, due to the nature and the content of the information exchanged. Besides the obvious security risk if such information becomes known, Belgium and the services also risk considerable damage to their image if certain data should get lost or fall into the wrong hands.

VIII.3. RECOMMENDATIONS ABOUT THE EFFECTIVENESS OF THE REVIEW

VIII.3.1. DIRECTIVES FROM THE MINISTERIAL COMMITTEE FOR INTELLIGENCE AND SECURITY

The Standing Committee I cannot exercise its legal mandate fully if it has no knowledge of the directives from the Ministerial Committee for Intelligence and Security that relate to or are relevant to the operation of the intelligence services and the CUTA.[144] Although the Standing Committee I is of the opinion that the current wording of Article 33 of the Review Act gives it sufficiently explicit right to have cognizance of these directives, this view appears not to be universally shared. Given the years of deadlock, the Standing Committee I recommends introducing even clearer rules on this subject in the Act of 18 July 1991 governing the review of police forces and intelligence services and of the Coordination Unit for Threat Assessment. It will suffice to amend Articles 9, §2,[145] and 33, §2, by

144 The Standing Committee P also experienced difficulties in this regard in its supervision of the CUTA.

145 This clause must also be amended to allow the Standing Committee P to obtain instructions or directives concerning the CUTA.

inserting the following words after the words "*all documents that govern the manner in which the members of these services operate*": "*even if these documents do not emanate from those services*".

VIII.3.2. OFFENCES COMMITTED BY MEMBERS OF INTELLIGENCE SERVICES

Article 38 of the Review Act provides for a three-pronged possibility or obligation for the courts to inform the Standing Committee I if members of the intelligence services and the CUTA are prosecuted or convicted for 'crimes' or 'offences'. 'Infringements' are outside the scope. For example, traffic offences can be 'hidden' from the Standing Committee I since these are sometimes treated as 'infringements' and on other occasions as 'offences'. But infringements can also be indicative of a dysfunction. By extending the scope of Article 38 of the Review Act to include infringements, this would remove any ambiguity and create a clear legal basis for notification and cognizance.[146] At the same time, Article 50 of the Review Act – which provides for an obligation for the police to submit an informative report on any offence or crime committed by a member of an intelligence service to the Investigation Service I – should be supplemented along the same lines.

[146] In its *Activity Report 2005* (p. XV), the committee already advocated extending the scope of Article 38 of the Review Act, but with regard to relevant information relating to subjects that the intelligence services deal with, and which is contained in judicial files when the members of these services are summoned as witnesses, experts or even as the victim of offences in the exercise of their functions.

ANNEX

18 JULY 1991
ACT GOVERNING REVIEW OF THE POLICE AND INTELLIGENCE SERVICES AND OF THE COORDINATION UNIT FOR THREAT ASSESSMENT

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.