COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

REVIEW REPORT

on

investigative activities of GISS on social media

CTIVD NO. 39

[16 July 2014]

REVIEW COMMITTEE
for the
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 39

REVIEW REPORT

On investigative activities of GISS on social media

Table of contents

REVIEW COMMITTEE
for the
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 39

DEFINITIONS

For the purposes of the review report on investigative activities of GISS on social media

The following list contains definitions of a number of terms as used in this review report. It was not the Committee´s aim to make the descriptions exhaustive, but rather to try and give readers a concrete idea of the meaning of the terms included in the list.

Acquiring or supporting department	The department at GISS which is involved in acquiring the data – by technical means or otherwise – when a special power is deployed . This is not the same department as the one that conducts the operational investigation in the context of which a special power is deployed.
Agent	A person specifically deployed by the service to gather data (article 21 ISS Act 2002). Agents operate under the direction and the supervision of the service.
Approval	Permission to exercise a special power (e.g. the services require the minister´s approval for telephone tapping).
Cable-bound communication	Communication via a cable (e.g. fibre optic or copper cables).
Case manager	Service employee who maintains the contacts with human sources (informers and agents).
Computerised device or system	A device or system used for recording, processing and transmitting data by electronic means (e.g. a computer, a computer network, a mobile phone or a server).
Cyber	All things relating to the digital or virtual world, including the internet.
Data collection	A collection of data. A data collection may have been compiled by GISS, but GISS can also obtain data collections from open sources or external parties, or by exercising (special) powers.
Data processing	Collecting, recording, arranging, storing, updating, altering, demanding access to, consulting or using data, providing data by forwarding, dissemination or any other means of making data available, assembling or combining data, and protecting, deleting or destroying data (article 1(f) ISS Act 2002). The mere act of *gathering* data is also referred to as data acquisition.

Director (GISS)	Officer at GISS positioned in the organisation's hierarchy as follows: head, *director*, unit head, team head.
Evaluated data	Data which has been assessed for relevance.
Fictitious identity	The whole set of personal characteristics used by a person to present himself as another, non-existent person. Also known as 'assumed identity' within the meaning of article 21 ISS Act 2002.
General power	The power of GISS to collect data (articles 12 and 17 ISS Act 2002). GISS may exercise this power for all the tasks mentioned in article 6. A distinction should be made between the general power and the special powers (see below).
Hacking	Gaining access to a computerised device or system with the aim of acquiring data (article 24 ISS Act 2002). The service can hack from a distance (remote hacking e.g. over the internet) or it can hack a device that is in its physical possession (e.g. by decoding the password of a laptop in the possession of the service).
Head (GISS)	Officer who is in charge of GISS. The head occupies the following position in the organisational hierarchy at GISS: *head*, director, unit head, team head.
Human source	An informer or agent.
Informer	A person or body who/which the services can approach to collect data (article 17 ISS Act 2002). An informer is not controlled and is deemed to be able to provide information on the basis of his/its usual activities.
Intelligence task (GISS)	Investigating other countries (see article 6(2)(d) ISS Act 2002).
IP address	Every individual computer which communicates with other computers via IP has a unique address, the IP address. The IP address identifies the connection of the computer to the internet, similar to a telephone number.
Mandate Decision	GISS Special Powers Mandate Decision 2009, adopted by the head of GISS. The Decision has not been published.
Metadata	Data about a communication session. The metadata of a telephone call, for example, comprises the telephone numbers involved, the starting and ending times of the call and the data of the mobile phone masts involved.
Network analysis	Identifying , combining and finding links between data relating to persons and organisations in order to gain insight into the relationships between them, for example by providing insight (e.g. based on a technical characteristic such as a telephone number) into the contacts of a target with other persons and subsequently into the contacts of the latter with yet other persons.
Nickname	A name stated by an internet user (e.g. on social media), under which he or she presents himself or herself to others.

Operational process	Combining data that has been acquired with other data that is already available, following which the data is interpreted and analysed for the purpose of preparing reports which may, if required, be provided to the responsible authorities.
Operational team	A team which investigates one of the areas of attention of GISS. For example: a team investigating terrorism.
Personal data	Data relating to an identifiable or identified individual natural person (e.g. a name or a photograph).
Platform	A specific form or application of social media.
Processer	An employee whose tasks include assessing new data, and on the basis thereof setting the first step towards intelligence products, towards the course to be taken by the team and towards the exercise of powers, if necessary.
Raw data	Data obtained by the exercise of (special) powers which have not yet been assessed for relevance. Also called *unevaluated* data.
Search request	Request for a focused (targeted) search addressed to a provider or foreign service having access to a social media data collection.
Security screening	Security clearing check pursuant to article 7 of the Security Screening Act regarding a person who holds or is to hold a position of confidentiality in which he or she may harm national security.
Security service	A service that investigates persons and organisations who or which may constitute a danger to the continued existence of the democratic legal system, or to the security or other vital interests of the state, or to the security and the readiness of the armed forces.
Security task (GISS)	Task aimed at identifying dangers to the continued existence of the democratic legal order or to the security or other vital interests of the state (article 6(2)(a) ISS Act 2002.
Select before you collect	The basic principle that GISS will only acquire data collections if the service has capacity to effectively process them.
Special power	A power conferred on the service which entails a specific infringement of privacy. Special powers are usually exercised in secret. The special powers and the conditions under which they may be exercised are laid down in articles 20-30 ISS Act 2002 (e.g. wiretapping or hacking).
Stored telecommunications data	Telecommunications data stored in a computerised device or system (e.g. a computer, a mobile phone or a server).
Streaming telecommunication /transmission phase	Streaming telecommunication is communication being transmitted from sender to receiver. Such communication is in the *transmission* phase. Streaming telecommunication can e.g. be intercepted by means of tapping.

Support team	A team which does not carry out (substantive) investigations into one of the areas of attention of GISS, but which exercises special powers or gives advice thereon, usually at the request of operational teams. An operational team may e.g. request a support team to carry out a hack with respect to a specific target, because the support team has the expert knowledge for doing so. The support team does not itself use the data obtained by the hack.
Targeted interception	Interception where the person, organisation or technical characteristic at whom/which the data acquisition is targeted can be specified in advance.
Team head (GISS)	Officer at GISS who occupies the following position in the organisational hierarchy at GISS: head, director, unit head, *team head*.
Telecommunication	Communication at a distance by electronic means (e.g. telephone, radio, telefax or the internet).
Traffic data	Data relating to a user (user data, e.g. name, address, city, number), to the persons or organisations with whom/which the user is or was connected or tried to make a connection, or who/which tried to make a connection with the user (name, address, city, telephone number), data relating to the connection itself (metadata, e.g. starting time, ending time, terminal equipment location data, terminal equipment numbers), and data relating to the subscription (the type of service the user is using or has used, the data of the party paying the bill) (article 28 ISS Act 2002).
Unit head (GISS)	Officer at GISS who occupies the following position in the organisational hierarchy at GISS: head, director, *unit head*, team head.
Untargeted interception	Interception where the person, organisation or technical characteristic at whom/which the interception is targeted cannot be specified in advance.
User data	Also called subscription data. These are name, address, city and number of a user and the type of service used. (article 29 ISS Act 2002).
Web forum	Digital discussion pages on the internet. Some forums require visitors to register in order to obtain access to the site. Usually, visitors can also exchange messages via these sites.

REVIEW COMMITTEE
for the
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 39

Summary

Of the review report
on investigative activities of GISS on social media

Social media nowadays play a significant role in society. This is one of the reasons why social media have become an important intelligence source for GISS. Because of the volume of communications on social media and the low threshold for participation, messages cannot always be interpreted instantly: is a threat tweet a desperate cry from an angry teenager or a serious sign of extreme radicalisation? Society can expect GISS to respond adequately to developments on social media when performing its tasks. In the present investigation the Committee reviewed whether GISS carries out these activities lawfully.

It is important, given the task GISS has to perform, that it remains secret who exactly are being monitored and how. This secrecy gives rise to speculation, especially since 2013 when information was disclosed about the activities of a number of foreign services. As far as GISS was concerned the media and public discussions centred for the most part on the following questions:

- How does GISS use social media?
- what is GISS permitted to do in the context of social media and does GISS keep within the boundaries of the law?
- what does GISS do with the data it gathers on social media?
- How does GISS cooperate with foreign services in this field?

Based on its fact-finding and file examination at GISS and on the legal frameworks defined by the Intelligence and Security Services Act (ISS Act 2002), the Committee has included the above questions in the present investigation. It covers the period from 1 January 2011 to 1 January 2014.

When the ISS Act 2002 was drafted, the internet was not yet as important as it presently is and social media were still developing. The deployment of 'conventional' powers in this 'new' digital context, for example the use of agents and surveillance on the internet, compels GISS to think about how national security is to be safeguarded in relation to the protection of privacy and the legal safeguards of the right to privacy. The obligation of the service to perform its task in strict accordance with the law means among other things that any and every infringement of privacy must have a basis in the law and that privacy may only be infringed when it is necessary to do so. The infringement must be reasonably proportional to the purpose served and lighter means must not be available. While developing new techniques, GISS must continually keep these requirements in mind and fundamental issues must be acknowledged in time.

The Committee has established that for most issues the ISS Act 2002 provides an adequate framework for assessing whether the use made of social media is lawful. The Committee further points out that GISS has been making considerable efforts to keep up with technical developments in the field of social media. However, on some points the service's policies ensuring the safeguards for the protection of privacy have lagged behind these developments. In particular the substantiation for deploying powers and the reporting on the operations (instructions, results) fall short of what can be expected from a service operating in accordance with the law. The Committee appreciates that in the pioneering phase it was not immediately clear how these essential safeguards should be given a firm place in the procedures, but GISS has by now moved beyond the pioneering phase and the methods applied may now be expected to have been embedded in established procedures.

Interactions between users of social media take place partly in the public domain. Just as everybody else GISS, too, may follow these interactions. GISS may collect this data on the basis of its *general power.* An important limit on collecting such data follows from the degree to which it infringes privacy. As soon as an activity entails privacy infringement, it must have a specific basis in the law. The activity must, moreover, be surrounded by increasingly stringent safeguards in proportion to the seriousness of the infringement. The Committee has not found any unlawful activities in the course of its investigation of data collecting by GISS on the basis of its general powers.

On account of the seriousness of the resulting privacy infringement, this investigation devoted particular attention to a number of secret *special powers*, including the deployment of agents. Communications on social media include communications that are relevant for the task performance by GISS. The service responds to this fact by deploying agents on these media, who may use a fictitious identity for their activities. Subject to strict conditions, moreover, agents may commit criminal offences, among other things to avoid standing out in the groups where they operate.

The Committee has examined several agent operations. The Committee holds the opinion that in the case of *external* agents GISS acts with due care and deliberation. As far as its *own* employees are concerned, however, the operations are regularly deficient in the matter of reporting. The reporting deficiency in five agent operations in which GISS employees were deployed on social media under a virtual identity, was such that the Committee considers that in this respect those operations were carried out unlawfully. Documentation is of vital importance for the safety of agents, internal accountability and the external oversight by the Committee. The lack of adequate documentation also occurs in operations where permission had been given to commit criminal offences. The Committee holds the opinion that as a result the permissions, too, were implemented unlawfully. Because of the deficient reporting it is impossible to verify whether the agents complied with their instructions and to what extent they were given sufficient direction. However, GISS has recently identified a number of problems in the guidance and support given to employees operating online and has started an improvement programme.

Providers of social media often store metadata or communication content in data collections. The same is done with respect to web forums. Various methods are available to GISS for doing focused (targeted) searches in such data collections. GISS may also try to acquire an entire data collection if this is necessary for its task performance and satisfies the requirements of proportionality and subsidiarity. It can do so in different ways, for instance via a human source, a hack or a foreign service. The more general the nature of the data

collection, the less targeted the nature of the acquisition will be. In the Committee's opinion stricter requirements apply in that case regarding prior substantiation, namely a more stringent proportionality assessment. The reason for this is that in those cases GISS will also collect data of persons who are not relevant to the performance of its task.

The Committee holds the opinion that the reasons given for the acquisition of a large number of web forums were deficient. With regard to five agent operations in which web forums were acquired the Committee holds the opinion that the reasons stated for deploying these agents were so inadequate that permission was given unlawfully in all of these cases. The Committee is convinced, though, that in most cases acquiring the web forum was necessary and fell within the tasks of the service. However, in four cases (not the same as the aforementioned ones) the Committee considers the acquisition of certain web forums not proportional and holds that for this reason the acquisitions were made unlawfully. The web forums in question were rather large and the infringement of the privacy of the web forum users who were not targets of the ongoing investigations was out of proportion to the results to be expected.

Data collected by GISS on behalf of its security or intelligence task by means of exercising special powers, may also be used by GISS for other tasks, such as security screenings. The Committee holds the opinion that this applies only to *evaluated* data: data which following (metadata) analysis has actually been found to be relevant to an operational investigation. It considers making *unevaluated* (raw) data from web forums accessible for security screening purposes to be unlawful. The law does not provide an adequate basis for doing this.

As the Committee already observed in an earlier review report, the law does not set a maximum storage period for unevaluated (raw) data. The Committee recommends that GISS itself set maximum storage periods, in anticipation of a possible amendment of the law. As part of the present investigation the Committee examined whether the acquired web forums were kept in storage on good grounds. The Committee holds the opinion that it was lawful for GISS to store those of the web forums that had been lawfully acquired.

Because communication using social media is virtually unhindered by national borders, the investigative activities of GISS involving social media often affect the interests and legal order of other countries. On the one hand the targets of the service usually operate internationally. On the other hand operating in an online context, for example by an agent of GISS, often entails the collection of data which (also) has relevance to other countries. The mutual interest in cooperation can hardly be overestimated. Web forums sometimes comprise very large amounts of data that is not only important for the Netherlands. The Committee emphasizes the importance of sound agreements with foreign services in order to reduce the risk of relevant data being overlooked.

The Committee has found no evidence that GISS has been sidestepping its own powers when cooperating with foreign services. Moreover, the Committee has not established any unlawful activities in the course of operations carried out by GISS in cooperation with foreign services. The service generally proceeds with care and deliberation, keeping adequate written records.

Finally, the Committee devoted special attention to the sharing of web forums acquired by GISS with foreign services. In practically all the cases examined GISS acted lawfully. The Committee found the following exceptions to this overall picture. GISS acquired a number of

web forums at the request of specific foreign services. If a web forum is acquired for a foreign service while the forum has no relevance to any ongoing investigation of GISS, this constitutes giving support to the foreign service. In this case the law requires the service to obtain the permission of the minister before acquiring the data. The Committee holds the opinion that in four cases GISS acted unlawfully since the minister's permission was absent. In a fifth case GISS shared a web forum with a foreign service, while the Committee holds that the acquisition of this forum by GISS was not proportional. Consequently, both the acquisition and the subsequent sharing of this forum were unlawful.

REVIEW COMMITTEE
for the
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 39

REVIEW REPORT

On investigative activities of GISS on social media

1. Introduction

The General Intelligence and Security Service (GISS) gathers data from a variety of sources in the context of its intelligence and security tasks. Over the past decade the internet has made significant gains as an important source of information. People meet on the internet, just as they do in the non-virtual world. They have discussions, exchange ideas and make new contacts. This may take place in the digital equivalent of the public domain or in more private environments. The online platforms on which individuals can communicate, either in private groups or in the digital public domain, are referred to collectively as social media. There are several ways in which GISS can gather relevant data on social media. The service can exercise the powers of tapping and hacking, but it can also gather data without using technical means.

In its review report on the assessment processes of GISS with respect to Mohammed B. the Committee observed that in 2004 GISS did not yet have an adequate information position on the internet. The Committee further stated "that an intelligence and security service may be expected to closely follow and (quickly) respond to developments of new communication means."[1] The successive annual reports since 2004 show that since then GISS has heavily invested in internet-related investigation, including social media. The service has repeatedly drawn attention to the threat of jihadism on the web in single-issue reports.[2]

In the present in-depth investigation the Committee examined whether the efforts made in the field of social media are lawful.

The Committee conducted this investigation pursuant to the oversight task which article 64 of the Intelligence and Security Services Act 2002 (ISS Act 2002) assigns to it. A preliminary investigation was started on 1 May 2013. On 2 October 2013 the Committee announced its

[1] CTIVD review report no. 17 on assessment processes of GISS with respect to Mohammed B., *Parliamentary Papers II* 2007/08, 29 854, no. 22 (appendix), section 7.4. All review reports of the Committee are available on: www.ctivd.nl. This report is not available in English.

[2] GISS devotes attention to the issue in both annual reports and single-issue reports: Violent jihad in the Netherlands – current trends in the Islamic-terrorist threat [*De gewelddadige jihad in Nederland – Actuele trends in de islamitische-terroristische dreiging* (2006)], The jihadist Internet – breeding ground for the current jihad [*Het jihadistisch internet – Kraamkamer van de hedendaagse jihad*] (2012) and The transformation of jihadism in the Netherlands - Swarm dynamics and new strength [*Transformatie van het jihadisme in Nederland – Zwermdynamiek en nieuwe slagkracht* (2014). The latter report is available in English on: www.aivd.nl

intended investigation to the minister of the Interior and Kingdom Relations and to the presidents of both chambers of Parliament.

The Committee completed its investigation on 5 March 2014 and adopted the review report on 18 March 2014. In conformity with article 79 ISS Act 2002 the minister of the Interior and Kingdom Relations was given the opportunity to react to the findings set out in the review report. The Committee received the minister's reaction on 28 April 2014. The reaction to the review report induced the Committee to further investigate several points, before finally adopting the report. Furthermore, it held an additional interview with an employee of GISS. All this resulted in some modifications to the review report. The Committee notes that some time elapsed between the minister's reaction and the final adoption of the review report on 16 July 2014, which was partly due to the additional investigative activities.

2. Organisation of the investigation

Since mid-2013 there has been a sharp increase in public interest concerning how the intelligence services operate in general. When organising this investigation the Committee took account of the concerns entertained in society. The Committee understands that the main questions in regard to social media are the following:

- how does GISS use social media?
- what does the law permit GISS to do in connection with social media and does GISS keep within the boundaries of the law?
- what does GISS do with the data gathered on social media?
- how does GISS cooperate with foreign services in this field?

In connection with the public debate the Committee in March 2014 issued a review report on the processing of telecommunications data.[3] In this report the Committee made a commitment to further investigate specific procedures at GISS, namely hacking by human sources, hacking of web forums and the storage and exchange of web forums. The Committee also pointed out in the report that new technical possibilities and the digitalisation of society have had the result that existing powers can be deployed in ways not yet foreseen when the law was drafted. With the present investigation the Committee fulfils its commitment, examining in particular whether the way in which GISS conducted investigations on social media in concrete operations is in line with the protection of privacy.

With this in-depth investigation the Committee wished to gain a broad picture of the activities undertaken by the service in the field of social media. For this purpose the relevant policy documents and the activities of two operational teams working in this field were scrutinised. One of the teams had already been conducting intensive investigations on social media for quite a long time, while for the other team social media were only one among many sources from which the team gathered data.[4] The Committee also examined the activities of the support team, focused among other things on the acquisition of web forums.

---

[3] CTIVD review report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Papers II* 2013/14, 29 924, no. 105 appendix). Further cited as: CTIVD review report no. 38. This report is available in English on www.ctivd.nl.

[4] In order to protect sources and the current level of knowledge of GISS this review report does not mention the areas of attention on which these operational teams focus their activities. GISS reports publicly on the activities of these teams in its annual reports.

For the above purposes the Committee thoroughly examined the files of several dozen operations and held a number of interviews with thirteen employees holding key positions. This set-up enabled the Committee to form a representative picture of the operational use of social media by GISS.

Gathering data on social media can be done in several ways. This in-depth investigation focused on the human dimension of data collection on social media. The use of technical means, such as wiretapping and the selection of sigint, has already been or is being investigated by the Committee in other in-depth investigations.[5] The present investigation included examination of the power of article 24 to gain access to a computerised device or system (hacking) wherever this power was used to acquire data collections of social media. This means that the particular focus was on the acquisition and processing of web forums.

The file examination covered the period 1 January 2011–1 January 2014. This period was chosen to enable the Committee to issue a report within a reasonable period, but also because it was found that in recent years developments in the field of (investigation on) social media followed each other in rapid succession. Conclusions relating to earlier periods would have limited value for current practice at GISS. The Committee notes that some of the web forums included in the investigation involved large data collections. By sampling and searches in the documentation systems of GISS the Committee has sought to form as complete a picture as possible of these data collections.

This report has the following structure. Section 3 deals briefly with the definition of social media and how they work. Section 4 sets out the legal framework. In this section the Committee further elaborates, with a focus on social media, the framework set out by the Committee in review report no. 38 and the legal appendix attached to it. Section 5 discusses the existing methods for collecting data on social media and sets out the Committee's findings regarding concrete operations. To this end the Committee particularly examined the extent to which fundamental rights were infringed and the justification for doing so, as well as a number of aspects of operational implementation, such as reporting, control and security. Section 6, finally, contains the conclusions and recommendations of the Committee.

This report has a secret appendix. In this appendix the Committee does not draw any conclusions regarding the procedures established to be unlawful that are not also mentioned in the public part of this report. Furthermore, the public part has an appendix containing a brief synopsis of the assessment framework.

3. The concept of social media

There are many definitions of the phenomenon of social media. At GISS, the following definition applies, which will also be used for the purposes of this review report:

> "Social media is an umbrella name for applications that use the internet and have the objective of allowing individual users to enter intentionally and/or unintentionally into interactions

[5] CTIVD follow-up investigations on the use by GISS of the power to tap/intercept and the power to select Sigint: review report no. 31 covering the period September 2010 through August 2011, *Parliamentary Papers II* 2012/13, 29 924, no. 86 (appendix), available in English on www.ctivd.nl; review report no. 35 covering the period September 2011 through August 2012, *Parliamentary Papers II* 2013/14, 29 924, no. 101 (appendix), not available in English; ongoing investigation covering the period September 2012 through August 2013: expected to be published in September 2014.

with other users of those applications by means of a mix of different media (text, photo, video)."

It is important to point out the difference between the public part and the private part of social media. Much of what is happening on social media is accessible to all internet users and easy to find by using search machines like Google. Users and providers can, however, protect communications to varying degrees, for instance by restricting access to members as the provider LinkedIn does, or by users determining who can see what. For example: a Facebook user can limit the information that is visible to the world at large, and web forums can have coexisting public and private discussion groups. Many platforms, moreover, have a feature for sending messages directly to another user, which is comparable with e-mailing or texting.

While it is a characteristic element of social media that the content is shaped by individual users, the companies and institutions that develop and provide social media usually store both content and metadata of the communications. This means that (large) data collections exist in connection with social media.

This review report uses the expression investigation *on* social media when GISS mingles, as it were, with the individual users on social media and in some cases actively participates. The term investigation *of* social media data is used when GISS investigates data collections in the possession of the providers of the various platforms. These investigation methods are also known collectively as *social media intelligence* (socmint).[6]

4. Legal framework

In the legal appendix to its recent review report on the processing of telecommunications data the Committee presented a detailed explanation of the legal frameworks within which GISS and the Military Intelligence and Security Service (DISS) must operate.[7] The Committee therefore decided that in the present report it would only further elaborate on the legal framework where this would be significant or where the framework has a specific interpretation in the context of social media. The appendix to the present review report contains an overview of the assessment framework applying to the investigative methods used by the service on social media.

4.1 Human-rights framework

An individual who is active on social media enjoys protection on the basis of several fundamental rights. This subsection will discuss the fundamental rights enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). In a social media context the right to respect for privacy (article 8 ECHR) is the most prominent human right, but the fundamental rights to freedom of religion (article 9 ECHR), of expression (article 10 ECHR) and of association (article 11 ECHR) can also play a role in connection with social media. Because the conditions under which infringements of these fundamental rights are permitted are all based on the same system, the Committee will confine itself here to a discussion of the right to respect for privacy.

[6] Taken from: D. Omand, J. Bartlett and C. Miller, #*Intelligence*. London: Demos, 2012.
[7] CTIVD review report no. 38.

When GISS infringes the right to privacy in performing its tasks, such infringement must satisfy the requirements arising from article 8 of the ECHR. This means that the infringement must be in accordance with the law and necessary in a democratic society. The infringement must be necessary on the grounds of one of the interests mentioned in article 8, which include the interest of national security. Legislation must be formulated with sufficient precision, in order that individuals can attune their conduct to it and can also foresee the consequences that may result from any specific conduct. The infringement must also satisfy the requirements of proportionality and subsidiarity.

A large part of the information that can be gathered via social media is unprotected information in the public domain, sometimes expressly disclosed by the persons in question to a broad public.[8] Examples are public profiles, online speeches or pictures placed on a freely accessible website. This information can be gathered by employees of GISS or via the service's agents without using special methods.

The question arises when the gathering of such publicly accessible data constitutes privacy infringement. The case law of the European Court of Human rights (ECtHR) provides guidance regarding the scope of the protection of privacy in the public sphere. In particular the case law relating to monitoring persons in the public domain, developed in the context of camera surveillance and public demonstrations, contains relevant considerations for deciding whether or not the right to privacy has been infringed.

An example that is very suitable for application in the social media context is a decision of the European Commission for Human Rights on the police taking photographs at public demonstrations. The Commission discussed the scope of the term privacy.

> "In the present case, the Commission has noted the following elements: first, there was no intrusion into the "inner circle" of the applicant's private life in the sense that the authorities entered his home and took the photographs there; secondly, the photographs related to a public incident, namely a manifestation of several persons in a public space, in which the applicant was voluntarily taking part; and thirdly, they were solely taken for the purposes, on 17 February 1988, of recording the character of the manifestation and the actual situation at the place in question, e.g. the sanitary conditions, and, on 19 February 1988, of recording the conduct of the participants in the manifestation in view of ensuing investigation proceedings for offences against the Road Traffic Regulations."[9]

The Commission further attached weight to the fact that no names were noted down with the photographs, and that no action was taken to identify the persons. On the above grounds the Commission found that the photographs that had been taken did not fall within the scope of the term private life so that there was no infringement of privacy.
The European Court of Human rights (referred to below as: ECtHR) further developed this case law in relation to camera surveillance:

> "Article 8 also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world […]. There is also a

[8] Such information can also be characterized as 'open source intelligence' (osint). GISS holds that osint includes information that is available at commercial businesses and only accessible after payment.
[9] European Commission for Human Rights, 19 May 1994, *Friedl v Austria*, 15225/89, paragraph 49.
The Commission ruled similarly in: *Herbecq et al. v Belgium* , 14 January 1998, 32200/96, paragraph 3.

> zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".
>
> There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks on the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar nature. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by the security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method."[10]

In a subsequent decision the Court repeated its ruling in a different wording:

> "The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life. […] On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations. Accordingly, in both Rotaru and Amann […] the compilation of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with the applicants' private lives."[11]

The finding of infringement therefore depends partly on the justified expectations of an individual regarding his privacy. The mere examination by the authorities of data in the public domain concerning a specific individual does not as such constitute infringement of that person´s privacy.[12] The Court will quite readily find infringement, however, if the personal data is subsequently stored (whether or not systematically). Targeted gathering of data on a specific person by security services also constitutes infringement. In addition, the use of secret or concealed methods is a circumstance that will more readily lead to the finding of infringement. The mere fact that technical means are used – inherently linked to internet investigations – does not automatically result in the finding of infringement.

So far the Court has not given any direct ruling on the application of the rights arising from the ECHR to social media. Based on the case law mentioned above, however, the Committee arrives at the following principles.

The relevant factors in establishing the extent to which gathering intelligence from the public domain infringes the right to privacy are: the intention, the methods and the product of the intelligence work. Infringement will be found more readily if the gathering is *intended* to collect information on a specific individual, if very intrusive or secret *methods* are used, if the *storage* of information is actually targeted at a specific individual. By contrast, it may be assumed that the analysis of data from open sources without using secret methods and without targeting a specific individual will usually not constitute infringement of the privacy

[10] ECtHR, 25 September 2001, *P.G. and J.H. v the United Kingdom*, 44787/98, paragraphs 56-57.
[11] ECtHR, 28 January 2003, *Peck v the United Kingdom,* 44647/98, paragraph 59.
[12] The Court did not need many words to find that targeted monitoring of the entire internet traffic of a specific person constituted infringement of the right to privacy. ECtHR, 3 April 2007, *Copland v the United Kingdom*, 62617/00, paragraph 43.

of the persons concerned. The more a search is targeted at an individual or the more intrusive the method used, the sooner infringement of privacy will be found to exist. In that case an adequate legal basis for and justification of the infringement will be required.

4.2 ISS Act 2002

In addition to the general power to gather data the law contains an exhaustive list of special powers available to GISS. The special powers that are particularly important in the context of this in-depth investigation are the power to conduct surveillance (article 20), the power to deploy agents (article 21) and the power to gain access to a computerised device or system, also known as hacking (article 24).

GISS may only exercise a special power if doing so is necessary for investigative activities in the performance of its security task or foreign intelligence task (article 18 in conjunction with article 6). Permission to exercise a power must be granted by the competent authority (article 19) and the power must be exercised in accordance with the principles of proportionality and subsidiarity (articles 31 and 32). Moreover, the service must report in writing on the exercise of special powers (article 33). With respect to several special powers the law requires that the reasons why using this means is deemed necessary must be laid down in writing in the application for permission to exercise the power. The Committee holds the opinion that it follows from the law that the reasons for deploying agents and for hacking must be laid down in writing, too. This will make the exercise of these powers transparent and verifiable for the purposes of internal accountability and external oversight. The internal policies at GISS are indeed consistent with this opinion and require that applications for permission to exercise these special powers must also state why this is deemed necessary.

It should be noted that when the bill containing the ISS Act 2002 was discussed in parliament, the subject of gathering data on social media was not mentioned separately. In parliamentary history the internet is only mentioned in connection with the special powers in the field of interception and hacking.[13]

4.2.1 General power

Acquiring intelligence from social media is a form of data processing within the meaning of article 1(f) of the ISS Act 2002. The general power of GISS to process data is embodied in article 12. It includes processing of personal data as well as other data. Data processing is only permitted for a specific purpose and insofar as necessary for the proper performance of tasks (article 12(2)). In addition, data processing must be done with proper and due care (article 12(3)). Moreover, processing personal data is only permitted of personal data relating to persons listed in article 13.[14] Data relating to other persons, further referred to below as other users, is only permitted if it is necessary for or supports the proper performance of tasks by GISS.

---

[13] With regard to hacking: *Parliamentary Papers II*, 1999/2000, 25 877, no. 8 (NV), p. 64, and with regard to tapping electronic messaging: *Parliamentary Papers II*, 1997/98, 25 877, no. 3 (Expl.M.), p. 41.

[14] In the following the term 'targets' will be used to refer to the persons mentioned in article 13(1)(a) and (c). In this review report this term includes the groups and organisations to which these persons belong.

Article 17 confers power on GISS to apply to administrative bodies, persons and institutions which or who process data (informers) in performing or in support of performing its task. These may include companies which process data in connection with social media. GISS may, for instance, ask such a company to provide the IP address from which a specific user has logged in. The requested company is not required to provide the information; it does so on a voluntary basis. GISS may only ask for data to the extent necessary for a specific purpose and for the performance of its statutory tasks. In general, furthermore, the Committee holds the opinion that GISS may only apply to an informer insofar as the informer's normal activities include taking cognizance of the requested data or providing the data to third parties. If this goes beyond the activities of the human source in his normal capacity, he or she should be considered an agent.

In the Committee's opinion the general power of article 17 does not provide a sufficient basis for any further infringement of privacy, as results e.g. from the acquisition of content of non-public communications, e.g. of private messages on social media. The latter entails such a far-reaching infringement of privacy that it is only permitted subject to supplementary safeguards. These include requirements relating to the level at which permission must be obtained, substantiation, reporting and the use to be made of the acquired data. The law attaches such safeguards to the exercise of special powers. Since article 17 does not include such safeguards, the general power under this article does not suffice to permit the acquisition of content of private messages.

The Committee further notes that its opinion on this issue applies only to the deployment of human sources to acquire content of non-public communications. Such data enjoys a higher level of protection than e.g. financial data, which may be acquired under the power of article 17.[15]

The third paragraph of article 17 declares that any other provisions of law applying to the provision of data are not applicable if the data is provided to GISS pursuant to this article. Often, privacy legislation will prohibit the provision of personal data to third parties. Pursuant to article 17(3) a company is permitted to provide the data to GISS notwithstanding the prohibition.

4.2.2 Surveillance

One of the special powers which can be relevant in relation to social media is the power of surveillance pursuant to article 20(1) of the ISS Act 2002. It concerns the power of conducting surveillance of and monitoring a natural person and on this basis recording this person's behaviour. The question arises in which cases activities of GISS on social media constitute surveillance within the meaning of the law. In the parliamentary debate on the bill containing the ISS Act 2002 the exercise of this power in an internet environment met with the same lack of attention as did the special power to deploy agents discussed above.

The Committee has previously expressed an opinion on the interpretation of the power of surveillance in general terms:

[15] See for example: CTIVD review report no. 20 on financial and economic investigations by GISS, *Parliamentary Papers II* 2009/10, 29 924, no. 50 (appendix), section 3.3.1. This report is not available in English.

> "It is not explained in the legislative history of the ISS ACT 2002 what the term surveillance must be understood to mean. […] The Committee considers that the decisive factor in interpreting the term is not the objective but the intrusiveness of the surveillance. When deciding when there is systematic surveillance, the criteria applying in criminal law can provide guidance. These are: the duration of the surveillance, the location, the intensity, the frequency or the use of a technical means providing more than merely reinforcement of the senses."[16]

In the opinion of the Committee, the activities of GISS on social media constitute surveillance, which requires permission pursuant to article 20 ISS Act 2002, if e.g. the duration or intensity of the surveillance produces a more or less full picture of certain aspects of a person's life. An example in a social media context is the systematic monitoring on social media of the public messages of a specific person.[17]

Mandate
Article 3(1) of the GISS Special Powers Mandate Decision 2009 (further referred to as: the Mandate Decision) mandates the director, unit heads and team heads to give permission for surveillance. Article 3(2) requires GISS to apply to the minister for permission if the surveillance includes examination by a technical means of 'any form of conversation, telecommunication or data transfer by means of a computerised device or system'. The explanatory note to this article clarifies that in those cases surveillance is no different from tapping, a special power for which pursuant to article 25 ISS Act 2002 only the minister has authority to grant permission.

The Mandate Decision further provides for an exception in situations in which "considerations of principle play a role or if there are special circumstances". Article 14(1) provides that in those cases the submandate is not applicable, or that the power to give permission must be exercised at a higher level. By way of example of such a special circumstance the explanatory notes to the Mandate Decision mention the situation in which the exercise of the power entails a great public risk. The mandatary himself must assess whether this situation occurs.

4.2.3 Deployment of agents

The first power entering the picture in investigative activities on social media is the power to deploy a natural person pursuant to article 21 ISS Act 2002. This concerns a natural person who gathers information on the internet on the instructions and under the supervision of

---

[16] CTIVD review report no. 4 on the lawfulness of the investigation by GISS into developments within the Moluccan community in the Netherlands, *Annual Report 2004/05*, section 2.2.2. This report is not available in English.

[17] Compare: Explanatory Memorandum to the bill introducing article 126g Dutch Criminal Code (*Parliamentary Papers II*, 1996/97, 25 403, no. 3, pp. 26-27):

> "Systematic surveillance of persons means, as stated above, those forms of surveillance that may result in obtaining a more or less full picture of certain aspects of a person's life, for instance his contacts with a criminal. A number of factors are important for deciding where such a form of surveillance occurs: the duration, the location, the intensity or frequency and whether or not a technical means is used which does more than merely reinforce the senses. Each of these factors separately, but particularly in combination with each other, is decisive for answering the question whether a more or less full picture of certain aspects of a person's life will be obtained."

GISS. This can also be an employee of GISS who is active on the internet under an assumed identity.

In previous review reports the Committee already gave detailed descriptions of the legal framework for deploying agents.[18] The Committee refers in particular to the review report on a number of long-term agent operations. The safeguards and conditions applying to all agent operations also apply to agents operating on social media. For example: the deployment of an agent always requires prior permission from a director or unit head, which permission must be renewed by the team head every three months. The applications must include a substantiation of the deployment including an assessment whether the deployment of the agent satisfies the requirements of necessity, proportionality and subsidiarity. When agents are deployed on social media, the following aspects of the legal framework assume special significance.

It does not follow clearly from either the legal text or the legislative history when deployment of an employee of GISS constitutes deployment of an agent within the meaning of the law. It is evident that an employee of GISS may gather information in the public domain, e.g. by attending public demonstrations or meetings. He may also do so on the social media. An employee can e.g. follow a speech or visit a web forum. On social media, as in the public domain of the street, the GISS employee will not wish to be immediately recognizable as such and will therefore use an alias. Many average internet users are likewise not active on social media under their real names.[19]

The question arises when the use of such an alias by a GISS employee constitutes deployment of an agent operating under an assumed identity pursuant to article 21. This seems not be the case until the employee actually sets up a fictitious identity or capacity, which goes further than the mere use of an alias. If, however, the employee intends building a virtual identity from the start, then the mere creation of a nickname already forms part of using the assumed identity. Furthermore, when an employee participates in a conversation using a fictitious identity this also constitutes operating under an assumed identity.[20]

Another aspect of the participation of employees and agents of GISS on social media is the prohibition on instigation, laid down in article 21 van de ISS Act 2002. An agent is not permitted to instigate a person to perform other acts concerning devising or committing an offence than those he was already intending to perform.

---

[18] Inter alia: CTIVD review report no. 8b on the deployment by GISS of informers and agents, more in particular abroad. Annual report 2006/07, p. 72. And: CTIVD review report no. 37 on a number of long-term agent operations by GI**S**S, *Parliamentary Papers II* 2013/14, 29 924, no. 108 (appendix). This report is available in English on www.ctivd.nl.

[19] The Committee is referring to persons who do not use their real name, e.g. when creating an e-mail address, profile page or username. In this way online identities are created which offer a certain degree of anonymity to users of the internet.

[20] In a criminal investigation context active participation in communications is used as a distinctive criterion to distinguish systematic data collection (article 126j Dutch Criminal Code) from the powers of the police under its general tasks under the law (article 3 Police Act 2012): *Parliamentary Papers II* 1998/99, 26 671, no. 3, p. 36. In professional literature, too, such a distinction between active participation and passive monitoring is applied to intelligence gathering on social media: I. Cameron, 'Foreseeability and safeguards in the area of security: some comments on ECHR case law', in: Vast Comité I, *Inzicht in toezicht*, Antwerp: Intersentia 2013, p. 167.

When an agent is deployed on social media it can happen that he or she actively approaches the target environment. In assessing such operations, special attention will have to be paid to the prohibition of instigation and the case law of the ECtHR regarding *agents provocateurs*, developed in the context of article 6 ECHR. Time and again the Court's case law emphasizes the importance of clear limits and safeguards, as well as supervision of undercover operations.[21] The ECtHR does, however, attach weight to the environment in which the agent operates. If there are strong indications that a digital network is being used for criminal offences, the agent will be more free to approach the users of the network about such acts.[22]

Even though the agents of GISS do not operate for criminal investigation purposes and it is only in exceptional situations that their observations come to play a role in criminal proceedings, for example via an official message to the Public Prosecution Service, incitement should be prevented, since the fundamental principle remains that authorities may not themselves generate offences.[23] Moreover, the activities of an agent of GISS will not always become known to or be reviewed by the courts in concrete criminal proceedings, particularly not in the international context of social media. This means that very high standards must apply to the transparency and verifiability of agent deployment.

Finally, an agent deployed on the internet may also be instructed to take measures (article 21(1)(a)(2°). The agent may e.g. deliberately disseminate 'disinformation' or frustrate targets' actions. In principle, it is easy to apply such measures in an online context. The legislator considered that an agent may only be so deployed if the measures cannot be achieved by any other means (e.g. by administrative measures).[24] Moreover, if an agent is to conduct a hack for the purpose of such measures, separate permission for the hack must be obtained as well.

Mandate
Article 4(1) of the Mandate Decision mandates the director and unit heads to grant permission to deploy an agent. Subsequent renewals of the permission may also be given by a team head. Article 4(2) provides for derogation from this rule in cases in which the person to be deployed belongs to a special category, for instance a doctor or a journalist. In those cases permission must be given at a higher level, consistent with the position of the person concerned.

The aforementioned exception also applies in case of fundamental considerations or special circumstances. In case of such considerations or circumstances permission must be obtained at a higher decision level.

[21] Inter alia: ECtHR, 5 February 2008, *Ramanauskas v Lithuania,* 74420/01, paragraphs 53-55; *Bannikova v Russia*, 4 November 2010, no. 18757/06, paragraphs 34-50.
[22] ECtHR, 7 September 2004, *Eurofinacom v France*, 58753/00, pp. 14-15 (English translation).
[23] CTIVD review report no. 7 on the execution of a counterterrorism operation by GISS, *Parliamentary Papers II* 2005/06, 29 944, no. 10 (appendix), section 4.3. This report is available in English on www.ctivd.nl.
[24] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 61 (NV).

4.2.4 *Hacking*

Briefly stated, article 24 of the ISS Act 2002 confers power on GISS to hack and e.g. acquire the stored or processed data.[25] The service may hack a device that is in its possession, but may also do this from a distance, for instance via the internet. By means of a hack GISS can try to gain access to the device used by a person to be active on social media. In many cases providers of social media also store user data or communication content in a data collection. GISS can try to hack and thus gain access to such a data collection. It is clarified in the legislative history that GISS may not only hack stand-alone computers but also computer networks.[26] The Committee holds the opinion that the power to hack must include the power to gain access to a server as well.

Mandate
Insofar as relevant here, the Mandate Decision mandates the director and unit heads to give permission for hacking. Only the director is mandated to give permission for remote hacking (article 7(2)). Just as in the case of the power of surveillance, only the minister has authority to grant permission to hack if a hack is highly similar to tapping (article 7(3)). Furthermore, the aforementioned exception to the mandate in case of fundamental considerations or special circumstances applies here as well (article 14).

4.2.5 *Data collections*

The requirements set by law on the processing of data collections are discussed in the legal appendix to the review report on the processing of telecommunications data.[27] In brief, this legal framework does not include specific rules on processing (large) data collections but permits such processing on the basis of the general power to process data. The service may use the data collections for analysis purposes. The service may also acquire data collections (partly) for the benefit of a foreign service. However, the minister's permission for acquisition is required if the data does not contribute directly to an ongoing investigation of GISS (article 59(5)).[28]

Targeting and proportionality
Targeting is a concept used in the legislation to regulate the powers to intercept communications.[29] The articles referred to make a distinction between targeted interception and untargeted interception; in the case of targeted interception the approval document must clearly specify the party concerned. For interception purposes targeting means that it is determined beforehand to which person, organisation, frequency, telephone number or IP address the data to be gathered relate.[30] The proportion between the total number of users

[25] In describing the power under article 24 ISS Act 2002 the legislator closely followed the wording of article 138ab of the Criminal Code. *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 39 (Expl. M.). The definition of a computerised device or system is indeed interpreted in accordance with article 80sexies of this Code: "a device or system used for recording, processing and transmitting data by electronic means".
[26] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 63 (NV).
[27] CTIVD review report no. 38, section IV.2 of the Legal Appendix.
[28] CTIVD review report no. 22a on the cooperation of GISS with foreign intelligence and/or security services *Parliamentary Papers II* 2009/10, 29 924, no. 50 (appendix), section 8.2. This report is available in English on www.ctivd.nl.
[29] Targeted interception is defined in article 25 ISS Act 2002, untargeted interception in article 27 ISS Act 2002.
[30] See also CTIVD review report no. 38, sections II.2.2 and V.2.2 of the legal appendix.

and the number of users investigated by GISS in the performance of its tasks (targets) is an indicator of the degree to which acquisition of the data collection is targeted.

The Committee is faced with the question whether the concept of targeting must also be accorded restrictive meaning in regard to powers other than interception. The fact is that GISS can also acquire 'untargeted' data collections of social media, such as web forums, by deploying an agent or by hacking. The question that needs to be answered is whether the law permits such acquisitions.

On the following grounds the Committee holds the opinion that though it is true that the concept of targeting plays an important role in determining whether the exercise of a power is proportional, it cannot be said in advance that all powers are required to be exercised with the same degree of targeting as the power of targeted interception. In the first place the legislator has provided for the possibility that the services process data of persons who are not themselves legitimate investigation targets of the services if this is necessary to support the proper performance of tasks (article 13(e)). In the second place the law, in article 17, provides a sufficiently precise basis for acquiring large data collections on a voluntary basis, for instance from commercial providers. When debating the bill proposing the post-Madrid measures, cabinet and parliament also expressly proceeded on the assumption that the services already had the power to acquire data collections.[31] Finally, it can be pointed out that with respect to many powers the law requires that it must be expressly stated in advance against whom the power will be exercised.[32] It does not do so with respect to the powers of articles 20 (surveillance), 21 (deployment of agents) and 24 (hacking).

While the Committee does not in principle preclude the possibility of acquiring untargeted data collections, it does hold that a stricter proportionality test applies to such acquisitions. With regard to data collections from social media the Committee points out that the nature of such collections varies considerably. There are platforms, such as social network sites, which are used by a very large public. At the other end of the scale there are web forums of highly radical persuasions, on which only like-minded people are active or whose founders pursue objectives justifying the attention of GISS. The more general the nature of a platform, the more serious the infringement of the privacy of the other users, with the result that increasingly stricter requirements will apply to its acquisition and further processing. When the acquisition of a data collection does not pass the tests of necessity, proportionality and subsidiary, GISS must abandon the idea of acquiring the data collection in its entirety.[33] In that case GISS is still permitted to do targeted searches. On the basis of this criterion GISS will e.g. only be permitted to acquire the data collection of a general social network site in its entirety in special circumstances and subject to additional requirements.

Storage periods and use of the data

There is no general statutory rule on storage periods for data collections. The law only prescribes a maximum storage period for raw data obtained by untargeted interception of non-cablebound communication (article 27(9) ISS Act 2002). On the other hand, the law does provide that the service must delete data as soon as it has become meaningless for the purpose for which it was collected (article 43). In its review report on the processing of

[31] *Parliamentary Papers II* 2005/2006, 30 553, no. 3, p. 13 ff.

[32] See articles 20(4) (surveillance in a dwelling), 23 (opening correspondence), 25 (tapping), 27 (selection of sigint), and 28 (demanding access to traffic data) of the ISS Act 2002.

[33] This applies regardless of the method of acquisition: hacking, deployment of human sources or received from abroad .

telecommunications data the Committee already observed that the law does not prescribe maximum storage periods for raw, unevaluated data. It recommended in that report that the legislator should regulate this issue by law.[34]

In the same review report the Committee also found that unevaluated data collected by exercising special powers may only be used for the purpose of the investigation in the context of which the data was acquired or for the purpose of another ongoing investigation falling within the scope of the security or intelligence task.[35] This is consistent with the statutory restriction that special powers may only be exercised for the purposes of the intelligence and security tasks of the service. It is only after the data has been evaluated, i.e. after GISS has found it to be relevant to an ongoing investigation, that it may be used in performing other tasks of the service. This means that data collections containing both evaluated data and unevaluated data may not be made available in their entirety for e.g. security screenings.

5. Social media in the intelligence process

5.1 Organisational embedding

As stated in the introduction, the Committee had previously established that GISS did not yet have a good information position on the internet in 2004.[36] The service had noticed the use of the internet by young people undergoing radicalisation and in the Hofstad investigation it had since 2000 gained its first experiences with investigation on the internet.[37]

Subsequently, internet investigation and particularly the investigation of the jihadist internet gained momentum. In Annual Report 2005 the service extensively discussed the role of the internet in violent jihad, especially as a result of its investigations of Mohammed B.[38] At the time GISS considered the internet to be "one of the principal boosters of the processes of independent radicalisation and recruitment". In 2006 a specialist internet team was established to respond to this development. The Committee has found that by now all operational teams collect data from social media to a greater or lesser extent.

This section describes the different methods and the actual procedures applied by GISS when conducting investigations on social media.

For a clear understanding it is necessary to briefly outline which departments of GISS have practical involvement with the investigations on social media. In the first place there are the operational teams that conduct investigations in the context of their a-task (security task) and d-task (foreign intelligence task). Based on specific investigation assignments the operational teams collect the necessary data. In the case of operations that serve a broad area of interest or more than one of GISS' areas of attention, however, the acquisition of data may be

[34] Article 27(9). See also: CTIVD review report no. 38, section 6 (under 4.1).
[35] CTIVD review report no. 38, sections 4.3 and 6 (under 4.2).
[36] CTIVD review report no. 17 on assessment processes of GISS with respect to Mohammed B., *Parliamentary Papers II* 2007/08, 29 854, no. 22 (appendix), section 7.4. This report is not available in English.
[37] GISS, *Annual Report* 2004, pp. 20 and 36.
[38] GISS, *Annual Report* 2005, pp. 17, 25 and 27.

assigned to one of the support teams. In organisational terms these support teams, each of which has a task emphasis of its own, now fall under the Joint Sigint Cyber Unit (JSCU). This joint unit of GISS and MIVD serves both organisations. In the review period for this investigation the support teams still worked for GISS only.

5.2 Passive investigation on social media

5.2.1 Practice

For several years now, authorised employees of GISS have been conducting operational investigations on the internet. Like anyone else, GISS can thus do searches on the internet, e.g. search for the e-mail address of a target on Google, visit the website of an extremist organisation or read tweets of a person who is participating in violent jihad abroad. This form of investigation using open sources can be defined as passive investigation, because the employees do not actively try to make contact or use an assumed identity. When practising this passive form of investigation the service restricts itself to gathering data from the internet to the extent it is an 'open source'. This is in fact a form of *open source intelligence* (osint).

Because the internet is 'open' in many different degrees, the question arises which part of the internet GISS may consider 'open sources'. The Committee's answer to this question goes further than the interpretation given to the term open source by GISS:

> "A source is 'open' when the distributor (the medium) has made the information accessible to the public. It is irrelevant whether or not one must login or pay for the information. So if the distributor allows everyone to pay or set up a login account, the information is accessible to the public."

According to this definition, websites and social media requiring one to login fall under the term 'open source' provided that any other person can become a member, too. Because, just as on the street, an employee will not wish to be immediately recognized, he or she may use a fictitious login name (nickname).

Investigation on the internet has increasingly come to form an integral part of operational investigations, with the service striving to improve its use of open source information. In addition to manual searches on the internet, automated devices exist for analysing messages on social media.

Increasing the effective use of open sources is also important in the interest of lawfulness. The consultation of open sources will usually entail only very limited privacy infringement. The principle that GISS must first consult open sources before deploying special powers has in fact been laid down in the law (article 31). This article provides that special powers may only be exercised if the data cannot be obtained or cannot be obtained in time by consulting publicly accessible sources of information or sources of information which the service is authorized to examine. Article 32 requires, moreover, that the exercise of a special power must be terminated if a less far-reaching means will suffice. This means that GISS must continuously ask itself whether, from the perspective of privacy protection, the method it is using in its efforts to gather data is in fact the appropriate method. On grounds of the principle of subsidiarity the Committee considers it proper that GISS should integrate the use of open sources in its operational processes as far as possible.

A considerable number of the employees of the teams studied by the Committee have authorisation to do operational searches on the internet. This includes logging in on certain social media. It has proved far from simple to gain a clear picture of the extent to which data is obtained from social media by passive investigation, because the sources from which data has been acquired are not always mentioned nor the fact *that* data has been acquired from the internet.

5.2.2 Findings

The activities defined above as passive investigation on social media take place on the basis of GISS' general power to process (and acquire) data (article 12). Based on its interviews, the Committee has established that only a limited volume of data is collected on social media by direct access to the internet. The operational teams generally collect data from social media by other means than by searching the internet for data themselves. The few results thus obtained had been acquired amply within the limits of the general power to collect data and had been processed with due care. The results do not point to investigations via the internet of such intensity or long duration as to require additional approval. There is no evidence either that the searches done entailed more than slight infringement of privacy and should thus have come to fall under the power of surveillance.

Because this is an investigation method that is still being developed and because further-reaching techniques may emerge in the near future, the Committee considers it appropriate to discuss a number of safeguards in greater detail.

Firstly, attention must be drawn to the line between the general power to collect data and the special power of surveillance of article 20 ISS Act 2002. It is clear that even passive investigation may involve highly targeted monitoring of a person on social media. In light of the case law of the ECtHR, the latter constitutes infringement of privacy.[39] If this happens systematically or more intrusively, it constitutes more than minor infringement. Furthermore, a lot more data can be gathered by investigation on the internet than is noticeable to an individual himself, this data can be stored, and automatic data comparison may enter the picture. Under certain circumstances this constitutes surveillance of a person (article 20).[40] In those cases the service will have to assess the necessity, proportionality and subsidiarity of the procedure and apply for permission. There are currently no guidelines within the service on the basis of which it can determine whether it must apply for surveillance permission for a more intrusive or more prolonged internet investigation. The Committee recommends establishing a clear criterion.

Secondly, the dividing line with the deployment of agents under article 21 ISS Act 2002 should be monitored. Employees of GISS are permitted to login on social media using a fictitious identity. The Committee considers it permissible for an employee of GISS to use a false name on the internet when investigating under the general power of GISS. A line is crossed, however, if the employee becomes actively involved and enters into interactions with other users, even if he only does so to prevent being conspicuous. In this case he is

[39] See section 4.1.

[40] Cf.: B-J. Koops et al., *Juridische scan openbrononderzoek*, Tilburg University and TNO 2012, pp. 37-38 and 53. This study examines the protection of privacy in surveillance programmes on the internet. The authors distinguish between non-targeted internet surveillance, which entails only very slight privacy infringement, and the more serious infringement resulting from surveillance.

operating under an assumed identity pursuant to article 21 and exercising a special power, with the result that the safeguards of permission, substantiation and reporting apply (section 4.2.3). The Committee has established that in the present situation there are insufficient safeguards guaranteeing that the distinction between using the general power and using the power to deploy agents will be observed.

Thirdly, the Committee notes that the use of the internet for operational investigations raises the question how the results should be recorded. The Committee considers it undesirable and impracticable to record all observations made on the internet, but relevant results should be documented.[41] The requirement of adequate documentation follows from the obligation to process data with due care (article 12(3) and to indicate the reliability of the data source (article 12(4)). The importance of adequate records is connected with the fact that investigation results are used to substantiate approval applications, intelligence reports and official messages. If results are insufficiently documented, they cannot be consulted by other employees of the service, and the products of GISS become less verifiable. On top of all this, the internet is fickle and data that can be found today may have disappeared tomorrow. Proper records also contribute to guarding that the borderline between passive investigation on social media and surveillance or deployment of agents is not crossed.

The Committee recommends that GISS clarify its existing policies on the operational use of the internet and on the recording of results. The above safeguards should be included in the policies. Among other things, investigation on the internet on the basis of the general power must be clearly defined and distinguished from the more infringing special powers, and unambiguous rules for recording results should be laid down. The Committee is aware that GISS is working on a revision of the internal rules on the registration of results.

The Committee makes the following observation with regard to the automated systems for gathering data from the internet. Other sectors of society have shown a continuous rapid increase in possibilities in this field. Nowadays, various tools exist for social network analysis and monitoring events.[42] The Committee recommends that GISS seek knowledge in the field of (privacy) safeguards from other sectors and science and apply this knowledge when developing new investigation methods. This will help ensure that new systems meet all the statutory requirements from the moment they are put into operation.

5.3 Active investigation by agents on social media

5.3.1 Practice

Just as in the material world, GISS can deploy agents in the digital world for the purpose of gathering data. Pursuant to article 21 ISS Act 2002 both employees of GISS and non-employees may be deployed as agents on social media. An agent may be active under his

[41] The need for accurate reporting also became clear to the Committee in a recent complaint procedure. GISS was no longer able to indicate whether certain data had been gathered on the public or the private part of the internet.

[42] The possibilities made available by this kind of tools and the safeguards that must be observed have already been described in detail elsewhere. See e.g.: J. Bartlett and C. Miller, *The state of the art: a literature review of social media intelligence capabilities for counter-terrorism.* London: Demos, 2013, p. 15. OVSE, *OSCE Online Expert Forum Series on Terrorist Use of the internet: Threats, Responses and Potential Future Endeavours – Final Report*. Vienna: OVSE, 2013.

own identity or use a fictitious identity. Practically everything agents may be instructed to do in the non-virtual world is also possible in the virtual world. To give some examples: establishing friendships (on Facebook), visiting meetings of a target group (on a web forum) or following open publications (blogs). In some agent operations the agent operates exclusively on the internet, in other operations this is only part of his deployment.

In the investigations examined by the Committee, various agents were deployed on social media to gather data. The objectives of the operations varied widely. Some agents were deployed in particular to pick up general signals of radicalisation or threats on specific social media. They supplied the team with comments on sentiments in a specific community and followed the (online) discussions taking place. Although these agents operated under an assumed identity, the infringement of fundamental rights of persons concerned was relatively limited insofar as the social media were concerned, because these agents adopted a predominantly passive attitude. In other agent operations that were examined, the agents adopted a more active attitude. A number of these agents had in fact been given permission to commit criminal offences. The permission enabled the agent e.g. to express himself on social media in such a manner as to avoid being conspicuous.

In 2006, supplementary to the general framework applying to agent operations, GISS prepared a legal framework for its *own* employees who operate online as agents. This framework provides among other things that the assumed identity under which the agent operates, his virtual identity, must be recorded and kept up to date. GISS employees usually operate as agents on the internet in addition to their main activities for the operational teams to which they belong. The employee himself is responsible for reporting on the operation. All this is different from the normal situation where an external agent is deployed and where the person managing the agent, the case manager, is responsible for directing and reporting on the operation.

In 2007 the service also prepared a guidance document setting out how employees of GISS should carry out agent operations on the internet with due care. The document prescribes among other things that employees must complete a specific course of training as a condition for being deployed as an agent. It also describes how agents must keep records of their activities and findings and of the directions given to them. The guide prescribes that a processer of the team must provide guidance to the agent. This is different from the procedure for normal agent operations, where an agent always has a case manager who provides guidance.

No specific policy has been adopted for the deployment of *external* persons as agents on the internet, but manuals and a training course have been developed for the case managers who provide guidance to these agents. These offer helpful instructions on how agent operations on the internet can be conducted carefully, safely, verifiably and effectively. They also describe various reporting and recording methods.

In addition to their activities for GISS, agents may also be active on social media in their private capacity. This can entail risks. The case managers recognise these risks and provide guidance to the agents. The case managers report on the deployment of external agents applying the usual forms of reporting. It is not always recorded in the files, however, what are the elements making up the fictitious identity of an agent, for example the nickname used.

A recent internal evaluation by GISS has identified various problem areas associated with the deployment of the service's own employees as agents on the internet. It was found that the guidance and support offered did not meet the needs of employees who operate online as agents. On the basis of this evaluation GISS is working to improve the conditions under which employees operate online. Improving their guidance is an important issue in this respect. GISS has also acknowledged the need to update its policies.

5.3.2 Findings

The Committee holds the opinion that the operations involving deployment of *external* agents are carried out with due care and deliberation. Adequate records are kept of the directions given to the agents and of the data collected by them. The Committee emphasises that the more intrusively an agent is deployed, the more meticulous the reporting methods must be.

The Committee found that the fact that no specific policies or legal framework exist for this type of agent operations does not in practice lead to problems. The general policy on deploying agents suffices. However, the Committee recommends paying greater attention to recording the online identities of the agents, whether fictitious or not. The files must clearly show which users on social media are agents of GISS. This is important to keep agents safe and operations verifiable.

The Committee has gained a more diffuse picture of the deployment of the service's *own* employees as agents on the internet. A framework policy exists for these operations which in actual practice, however, is insufficiently implemented. The Committee is in no doubt that the permissions for the operations examined were granted on good grounds and satisfied the requirements of necessity, proportionality and subsidiarity. Nevertheless, several formal defects and great reporting shortcomings were established.

In one case it seems that the deployment of the agent was not approved until months after the operation was started. In this case the permission for deploying the agent was not dated. The Committee holds the opinion that the absence of a date constitutes a lack of due care as a result of which it cannot be established whether the permission was present at the start of the operation.

The necessity of reporting is reflected in both statutory provisions and internal policies. The law provides e.g. that instructions to an agent must be recorded in writing (article 21(6)). The deployment of an agent must likewise be laid down in a written report (article 33). The Committee considers it necessary that the virtual identity under which an agent operates can be simply ascertained from the file on the agent operation. Pursuant to the internal policy rules of GISS virtual identities must be recorded in operational reports on the deployment of agents. The law imposes additional requirements on the instruction to commit a criminal offence (article 21(5)). In the operations examined by the Committee, the permission to commit offences was in each case given subject to the condition that reports on the operation be prepared regularly.

All the operations conducted by employees that were examined by the Committee were deficient in the matter of reporting. Insofar as operational reports had been prepared, it could not be properly ascertained from them what instructions were given to the agents. It was also practically impossible to verify which data the agents had gathered and what

statements they had expressed. Moreover, the assumed identities under which the agents operated were not recorded with sufficient clarity in their files, which is important for the safety of the agents and the verifiability of the operations. This situation complicated the Committee's investigation. The Committee noticed, moreover, that these deficiencies occurred in particular in the rather more intensive operations.

The Committee holds the opinion that in five cases the deficient reporting and recording of instructions was such as to make the agent's deployment unlawful. In these cases there were long periods in which no operational reports were prepared at all, or the reports that had been prepared provide absolutely insufficient insight into how agents were directed, instructed and deployed. This is not mitigated by the fact that some of the data gathered by these agents can be found in intelligence products. The Committee recommends that GISS without delay bring reporting on ongoing operations in line with the customary standards applying at the service. The results of the internal evaluation by GISS mentioned at the end of section 5.3.1 may contribute to improving the working processes in this respect. In the secret appendix the Committee will discuss these operations in greater detail.

The Committee has found that the absence of a case manager or other form of guidance contributed to the shortcomings it has established. It notes that in some cases in which a case manager came to be involved in the operation at a later stage, this resulted in clearly more attention being given to the careful execution of the operation. The Committee points out that GISS already has detailed guidelines in place for the execution of such operations, while the importance of reporting was also already emphasised in the aforementioned internal evaluation and the internal training course. The Committee recommends that GISS significantly improve the guidance provided to employee-agents on the internet, and at the same time address the question how the management and internal accountability of these operations can be improved. In its recent review report on a number of long-term agent operations the Committee deals in greater detail with the advisability of periodic evaluation of agent operations.[43]

5.3.3 Criminal offences in an online environment

The commitment of criminal offences by agents on the internet is a subject that requires separate attention.

Under strict conditions GISS may instruct an agent to commit criminal offences. This did in fact happen in some of the operations examined by the Committee. In order to make it possible for an agent to operate in a radical environment it may be necessary for the agent to make radical statements and thereby overstep the limits of criminal law. In the digital world this is no different from operations in the material world. A special aspect of operating on social media is that often a criminal offence does not only touch upon Dutch interests, but also on the interests and the legal order of other countries. There have been moments when agents of GISS did in fact attract the attention of foreign criminal investigation services.

In two cases an employee of GISS was deployed as an agent for several months while the head of the service had not given the required permission to commit criminal offences. In one case the application for permission to commit the criminal offences was not submitted to

[43] CTIVD review report no. 37 on a number of long-term agent operations by GISS, *Parliamentary Papers II* 2013/14, 29 924, no. 108 (appendix), sections 4.2.2 and 6. This report is not available in English.

the head of the service for a long time. When this was discovered six months later, the head of the service then signed the permission. In the other case the head of the service had likewise not signed the permission in time. After nearly a year the head of the service finally issued a (modified) permission. The Committee holds the opinion that these are serious formal shortcomings. In the Committee's opinion the permissions issued in retrospect did not repair the lack of due care. It notes, however, that there is no reason to suppose that permission, if applied for in time, would have been refused in these two cases.

With respect to another operation the Committee recommends that GISS consider whether it must apply for permission to commit criminal offences. The agent in question may be crossing the limits of what is permitted under criminal law with his statements on the internet. If permission is not applied for and granted, the agent must operate within the limits of Dutch criminal law and it must be ensured that he does so.

In the operations examined by the Committee, each of the permissions granted for committing criminal offences includes a number of safeguards, which are aimed at limiting the offences, achieving transparency and making verification possible. What is noticeable is that in all cases, with one exception, it was decided not to inform the National Public Prosecutor (LOvJ) of the permission to commit criminal offences. The Committee points out that according to internal policy the LOvJ must in principle be informed of any permission to commit criminal offences. In its review report on a number of long-term agent operations issued in June 2014 the Committee recommended that LOvJ should be informed of *all* permissions to commit criminal offences.[44] LOvJ can, after all, provide advice on assessing the proportionality of the permissible offences, preventing offences and formulating the permissible acts. In extreme cases LOvJ can play a role in protecting an agent from possible criminal prosecution.

In operations in which permission to commit criminal offences has not been given, agents must operate within the limits of criminal law. In the case of *external* agents the case manager will ensure that they do so. The Committee holds the opinion that in all operations it examined the case managers fulfilled this task adequately.

Because no case manager is involved in online operations by GISS' *own* employees, meticulous reporting is particularly important precisely in those cases. Adequate reporting is necessary for internal accountability and external oversight by the Committee. In the case of online agent operations it is, moreover, simple to work transparently because there are so many possibilities for having agents prepare (digital) reports. The Committee observes in this context that the deficient recording of instructions and lack of adequate reporting are felt particularly where permission to commit criminal offences has been given. A number of permissions expressly also include adequate reporting as a condition for the permission. The Committee once again refers to the case law of the ECtHR (see section 4.2.3) and the safeguards of proper direction, transparency and verification when deploying agents mentioned in therein.

In four of the agent operations by own employees that were already discussed in section 5.3.2 above, permission to commit criminal offences had been given. The deficient reporting

[44] In urgent cases LOvJ should be informed retrospectively. See CTIVD review report no. 37 on a number of long-term agent operations by GISS, *Parliamentary Papers II* 2013/14, 29 924, no. 108 (appendix), section 5.2.1. This report is not available in English.

on these operations also meant that nothing was recorded with regard to the commitment of criminal offences. This deficiency is so serious as to make the implementation of the permission to commit criminal offences unlawful. Because of the deficient reporting the Committee has been unable to assess whether these agents were given sufficient directions or whether compliance with the prohibition on incitement was sufficiently ensured.

In its review report on a number of long-term agent operations issued in June 2014 the Committee made recommendations regarding the procedures relating to the commitment of criminal offences by agents.[45] In the Committee's opinion, the issues described above confirm the need for GISS to implement these recommendations soon.

5.4 Investigation by acquiring data collections of social media

5.4.1 Practice

In addition to the methods for passively or actively gathering data *on* social media described above, the service also acquires data collections *of* social media. The latter comprise content and/or metadata of communications on social media. On account of the questions entertained in society, the Committee will in the following give separate attention to web forums.

GISS may conduct targeted searches at providers of social media, or try to acquire all or part of their data collections. The law provides various possibilities for doing this. The service may e.g. use hacks or human sources (informers under article 17 and agents under article 21). If a human source provides data collections such as web forums to GISS, this will usually fall outside the scope of his normal activities and the human source will then be considered an agent. GISS may also acquire data collections from a foreign service or conduct targeted searches via a foreign service.

In most cases these searches and acquisitions concern 'stored' data. This means that the data does not have the higher level of protection accorded by the Constitution to 'streaming' (real time) data. If 'streaming' data is concerned, it is the minister who must give permission to intercept the communication, just as is required for taps.[46] For hacks, this stricter regime is laid down in the Mandate Decision, and for the deployment of human sources it follows from recent internal policy rules at GISS.[47]

Data collections of social media can be important to more than one investigation of GISS, since e.g. a target in an investigation focused on extremism may happen to use the same social media platform as a target in a counterintelligence investigation. Since a data collection may be relevant to different investigations, it is the support team that carries out the tasks of searching, acquiring and making data collections accessible. Both on its own initiative and at the request of operational teams this team investigates the possibilities for gathering specific data or acquiring data collections in their entirety. This specific task of the support team does not preclude operational teams from acquiring a data collection themselves. This does in fact happen in a limited number of cases..

---

[45] CTIVD review report no. 37 on a number of long-term agent operations by GISS, *Parliamentary Papers II* 2013/14, 29 924, no. 108 (appendix), section 6. This report is not available in English.
[46] Article 13 of the Constitution.
[47] See further on this issue: CTIVD review report no. 38, section 6 (under 6.3.4 and 6.3.5).

Targeted searches of data collections using human sources are carried out by the case managers of the supporting team. The operational team supplies concrete questions concerning persons or organisations, which the case manager submits to the human source.

Web forums may be acquired in their entirety. In this case, no prior target-linked selection criterion is applied when acquiring the forum. All communication exchanges of all users (targets and other users) are copied and made searchable. As the Committee already established in its review report on the processing of telecommunications data, the procedure for managing the application in which this data is stored ensures careful implementation of the statutory requirement that access may only be given to employees in so far as this is necessary for the proper performance of the tasks assigned to the employee in question (article 35 ISS Act 2002).[48]

The service's internal policies on conducting security screenings, however, include a rule that for certain security screenings it must be checked whether data from web forums relating to the person concerned is available. The teams conducting security screenings do not themselves have direct access to this data, but they may submit targeted questions to specially authorised employees of the operational teams. Under certain circumstances the internal policies of the service thus allow security screeners to examine the content of the communications on a web forum of a person concerned in the security screening. The data thus examined may not only comprise data already used in an operational investigation of GISS, but also unevaluated (raw) data.

5.4.2 Findings

a) Acquisition by means of hacking
The examined hacks done by GISS to acquire web forums were all properly substantiated by reasons. Each of the hacked web forums was relevant in its entirety for the performance of tasks by GISS. Permission for the hack had generally been given at the competent decision level. The Committee considers it a lack of due care that in some cases permission for continuing a remote hack was given by a unit head. A remote hack means that GISS does not have direct physical access to the automated device or system to be hacked. Pursuant to internal policies and the Mandate Decision, only the director is authorised to give permission for starting or continuing a remote hack .[49]

b) Substantiation of the deployment of human sources
Most of the human sources (informers and/or agents) who acquire data collections or conduct focused (targeted) searches are deployed by the support team. It is therefore this team which prepares the reasoned applications in connection with these operations. The team does not itself use the acquired data in any investigation, since this is done by the operational teams. As a result the support team is not in an optimum position to assess the deployment of these human sources and its possible results. Since early 2013 the proportionality of deploying human sources is no longer assessed at all. No arrangements exist pursuant to which the operational teams are required to substantiate a deployment in writing. Moreover, it follows from several organisational documents that the responsibility

[48] CTIVD review report no. 38, section 4.3.
[49] This policy is presently being reviewed.

for the correct application of the rules applying to the deployment of agents by this team lies with the support team.

With regard to five *agent* operations the Committee holds the opinion that the substantiation of the deployment of the agents concerned was so deficient that the permission had been given unlawfully. In these five operations the agents also performed acts similar to hacking.[50] In the applications for initial deployment or for renewal, little attention was paid to the necessity of deploying the agent and to the principles of proportionality and subsidiarity. The applications merely stated general reasons, without mentioning which users were being investigated or to what extent the privacy of other users would be infringed. Neither was any attention given to the possibilities of limiting the privacy infringement of other users.

This resulted in several web forums being acquired without any careful prior assessment of necessity, proportionality and subsidiarity having been laid down in writing. Under *c)* the Committee will give more detailed consideration to the question whether the acquisition of these web forums satisfied the requirement of proportionality.

The Committee appreciates that in the early days of working with data collections it was not always clear on which legal basis the service was permitted to acquire the collections, and how the requirement of substantiation should be satisfied. But this pioneering phase is already some years behind us. In March 2013 an internal proposal was drafted to improve the substantiation of applications for approval. The implementation of this proposal was not taken in hand in the review period, however, so that the established substantiation deficiencies have continued to exist. GISS told the Committee that the procedures had recently been adjusted, though this still had to be translated into internal policy rules.[51] The Committee considers that the service could have been expected to show greater alertness in the matter.[52] The Committee recommends that the adjusted procedures be shortly embodied in written policies.

c) Proportionality and targeting

There is great variation in the degree to which the acquisition of data collections infringes privacy. In certain cases the infringement is very slight. Acquiring certain user data, for example, can in some cases best be compared to buying a telephone directory, which makes it possible to link users to IP addresses. Commercial providers sometimes have such data collections available ready-made and make them accessible for marketing purposes. At the other end of the scale the service may e.g. acquire both the public and private part of a web forum including message content from all users, which constitutes far-reaching infringement of the privacy of the persons concerned. The more far-reaching the infringement, the stricter the conditions that apply to the data acquisition and the more stringent the safeguards that must be observed in processing the data (see section 4.2.5 for more details on this issue). This

[50] The Committee already mentioned these operations in the report on the processing of telecommunications data, and has arrived at this opinion on the basis of further investigation. CTIVD review report no. 38, section 3.4.2.

[51] In its reaction to the draft of this report GISS stated that it was by then applying the new procedure. According to this procedure the operational team that wishes to exercise a power is responsible for substantiating its application.

[52] In a previous review report the Committee already recommended that GISS, when acquiring a web forum from a foreign service, should likewise lay down in writing an assessment to what extent its examination of the web forum's content will satisfy the requirements of necessity, proportionality and subsidiarity. CTIVD review report no. 38, section 3.5.5.

applies the more forcefully if there is also infringement of the privacy of other users who are not relevant to any operational investigation of the service.

The Committee has established that in 2011 the legal affairs department of GISS prepared a thorough policy memorandum on the acquisition of data collections, encompassing all relevant safeguards. GISS has not taken the implementation of the memorandum in hand, however. The failure to implement the policies makes itself felt in practice. As the Committee will describe below, there are four data collections which the Committee considers to have been acquired unlawfully. The Committee recommends that GISS shortly establish a binding policy on the acquisition of data collections (including web forums).

The Committee has examined the web forums acquired by GISS in the review period. It has found that in virtually all cases they were web forums whose acquisition was necessary for the performance of tasks by the service. They are web forums of predominantly radical or extremist persuasions, or the persons or organisations managing the web forums constitute a danger to national security or the democratic legal order. In those cases the virtual group of users and managers of the web forum qualifies as a target organisation, which – just as in the tangible world – can be a legitimate subject of investigation.

The Committee has established that in some cases, the acquired web forums or their managers do not show such radical or extremist persuasions. In those cases the web forums do not, in their entirety, qualify as a legitimate investigation target. A stricter proportionality test applies to such web forums. The fact that such a collection includes data of (many) other users who are not relevant to GISS carries great weight.[53] If the operational interest in acquiring the collection carries such great weight as to make its acquisition proportional, the infringement of the privacy of the other users must in all cases be limited to a minimum. The permission to acquire the web forum can give effect to this requirement by providing e.g. that after the acquisition the non-necessary data must be removed without delay.

The Committee holds the opinion that in four cases the acquisition of certain web forums did not pass the proportionality test and that they had been acquired unlawfully. These were large web forums where the infringement of the privacy of the other users was disproportionate in relation to the number of targets present on the forum and the results to be expected. Furthermore the Committee considers it a shortcoming that the acquisition of these web forums was continued for several years without its necessity and proportionality ever having demonstrably been a subject of discussion. The Committee will further specify this conclusion in the secret appendix to this report.

d) Permission level

In by far the larger part of the operations examined, permission for the operation or for its continuation was obtained at the required level. There are a few exceptions to this general picture.

The Constitution gives special protection to 'streaming' (real time) communication. Accordingly, where e.g. a hack will be used to acquire 'streaming' communication it is the minister who must give the permission. However, most of the data collections acquired by

[53] Pursuant to article 13(1)(e), ISS Act 2002 data of persons who are not targets may be processed if this is necessary to support proper task performance. The bill proposing the post-Madrid measures contained further rules on the processing of such "data files". *Parliamentary Papers II* 2005/06, 30 553, no. 3, Explanatory Memorandum, p. 26.

GISS relate to 'stored' communications that are not subject to a special permission regime.[54] In one case GISS gained 'live' access to a data collection and thus received 'streaming' communication. The Committee considers it evident that this activity should have been considered tapping and thus required permission from the minister. Since this permission had not been given, the Committee holds the opinion that this activity was unlawful.

The Mandate Decision restricts the mandate where special circumstances exist or where fundamental considerations play a role. The Committee holds the opinion that some operations involved fundamental considerations. In these cases the fundamental considerations arose from the nature and scope of the data collections that had been acquired and the resulting infringement of the privacy of large numbers of other users. As a consequence, the exception of the Mandate Decision applied. GISS can be expected to be alert in regard to this issue. In view of the infringing nature of the operations the obvious procedure would have been to apply for permission at a higher level. This was wrongfully not done and GISS thus acted with a lack of due care. The operations in question are also discussed elsewhere in this report.

e) Due care

One way of practising the required due care is to observe the basic principle that GISS will only acquire data collections if the service is capable of effectively processing them. In the aforementioned 2011 policy memorandum of GISS this is called the basic principle of *select before you collect*. In one specific case the Committee doubts whether GISS had sufficient capacity to effectively process the data acquired, either on its own or in cooperation with foreign services. The case is further explained in the secret appendix to this report. For the time being the Committee sees no reason to qualify the acquisition of this data as unlawful, but it emphasizes the need for careful consideration of this issue. In the context of the careful performance of tasks GISS must ensure that all possible threats are identified and investigated in time. Efficiency assessment plays a role in this, too. If GISS finds before or during an operation that it has insufficient capacity to process data, either on its own or in cooperation with foreign services, for instance due to a lack of translation capacity, it will have to give express consideration to other options such as issuing an official message. This will enable other public authorities to take measures.

f) Using the data

The Committee holds the opinion that the internal procedure which allows unevaluated data of web forums to be made available for the performance of other tasks than the a- or d-task of GISS (security or intelligence task) is an unlawful procedure. This regards the situation (described in section 5.4.1) in which an operational team provides unevaluated data, including communication content, for use in an ongoing security screening in performance of the b-task of GISS (security screenings). In this situation the privacy of the persons concerned in the security screening is infringed in a manner that has no adequate basis in law.

In general, there is nothing to prevent the internal provision of data from operational investigations for use in security screenings. But Article 18 of the ISS Act 2002 does not

[54] If, however, the pending amendment to the Constitution on this issue is adopted, this distinction between 'stored' and 'streaming' communication will be eliminated.

provide a basis for exercising special powers for other tasks than the a- or d-tasks of GISS. The Committee holds the opinion that it is not permitted to do checks in a system storing unevaluated data with respect to a person concerned in a security screening procedure who has not been linked in any way whatsoever to any operational investigation.[55] This is different if GISS has already investigated the person concerned in the context of its a- or d-task; in that case there is nothing to prevent taking further data into consideration for the purposes of a security screening procedure.

For a proper understanding of the matter the Committee further notes the following. GISS gathers data for ongoing investigations. After the data has been gathered and acquired, it is assessed for relevance ('processed'). In the case of data collections this may include a form of metadata analysis or file comparison. The results of such an analysis will as a rule be relevant to the operational investigation and will be further processed. That data is then called *evaluated* data. It has not been established (yet) at this stage to what extent the remaining data is relevant. For this reason the Committee holds the opinion that this data is *unevaluated* data. Unevaluated data may not be made available for other tasks than the a- or d-task of the service.

The Committee recommends that the procedure be revised accordingly and the possibility of providing data be limited to evaluated data. It recommends that the possibility for security screeners to do administrative checks in systems including unevaluated data be eliminated. The Committee notes, though, that it has the impression that the above procedure was used only very rarely.

g) Storage periods
When other special powers are exercised, e.g. tapping, the irrelevant results are removed and destroyed after the lapse of a certain period. In its review report on the processing of telecommunications data the Committee already observed that the law does not set maximum storage periods for unevaluated (raw) data, apart from the rules applying to sigint.[56] In the report it recommended that this issue would be addressed in the forthcoming amendment of the ISS Act 2002.

In addition to that recommendation the Committee notes the following. Even without further express legislation on the issue GISS is required to remove data that has lost its relevance (article 43). When acquiring data GISS can take this requirement into account by determining in advance how long the data to be acquired will be stored. This already happens where the power to tap is exercised, in implementation of the requirement of subsidiarity. In particular when data collections such as web forums are acquired, in the course of which GISS in some cases also acquires data relating to persons who are not relevant to any operational investigation, it is important that a maximum storage period is laid down in writing.

The Committee recommends the introduction of maximum storage periods for the unevaluated data of web forums, in anticipation of a possible amendment of the law. Since

[55] This is consistent with the Committee's opinion on the use of combined metadata for other tasks than the security or intelligence task, also having regard to article 35. CTIVD review report no. 38, sections 4.3 and 6 (under 4.2).
[56] It is only with respect to raw data acquired by untargeted interception of non-cablebound communication that the law sets a maximum storage period of one year (article 27(9)). CTIVD no. 38, section 6 (under 4.1).

so far no such storage periods were set at the time of acquisition, they should now be set in retrospect. Any unevaluated data that is no longer relevant to ongoing investigations should be removed as far as this is (technically) possible. The Committee also holds the opinion that the storage by GISS of the web forums that were examined by the Committee was permissible, with the exception of the web forums which the Committee in this review report found to have been acquired unlawfully.

h) Searching via human sources
If human sources are requested to conduct searches for the purpose of acquiring data from social media, this involves instructions within the meaning of this term as used in the law, so the Committee holds. This means that the instructions must be recorded in writing (article 21(6)). Recording what a human source is asked to do and subsequently what are the results, is a means to satisfy the requirement of stating sources. It also serves the internal accountability for, and the external oversight of the deployment of the agent. In a number of operations the searches agents were asked to do and the results were not recorded systematically over a long period. As a result, not all the files that were examined make it possible to verify the purpose for which the data was acquired. In 2013 the support team improved the procedure and by now all requests for searches are recorded.

The Committee recommends that GISS, when it instructs human sources to search data collections of social media, keep records of each separate search request. The Committee further recommends that GISS, when instructing a human source to gather data that can be compared with traffic and user data, follow the internal procedure applied with respect to requests under article 28 ISS Act 2002. This means that a reasoned application for permission must be submitted to the head of the service. In such cases there will be no need to separately record the search requests as instructions and prepare reports on them.

i) Restrictions arising from other legislation
In some of the operations examined by the Committee, human sources had told GISS that they needed clarity as to the lawfulness of their cooperation with GISS. The Personal Data Protection Act generally forbids these sources to provide personal data to third parties. With a view to this situation the ISS Act 2002 includes an exemption for informers, releasing them from other legal obligations when they provide data to GISS (article 17(3)). Contrary to the rules applying to informers, the law does not expressly make such provision for agents who provide data. Evidently, however, the considerations of the legislator underlying the exemption for informers also apply to the situation in which agents provide data.[57] The Committee therefore holds the opinion that this exemption also applies to human sources whom the services consider to be agents. This means that agents may provide data to GISS under the same conditions as informers, even if they would not normally be permitted to do so under applicable privacy legislation.

[57] *Parliamentary Papers II* 1997/98, 25 877, no. 3, Explanatory Memorandum, pp. 23-24. See also: *Parliamentary Papers I* 2007/08, 30 553, no. C, p. 4.

5.5 Cooperation with foreign services

5.5.1 Practice

It is a characteristic of social media that its communications are not hampered by national borders and that the communications do in fact often take place simultaneously between persons in several countries. This has several consequences for the investigative activities of GISS on social media.

On the one hand the persons investigated by the service are usually scattered across borders and active in several countries. As the annual reports of GISS have shown, many of the threats investigated by the service are linked to international networks and organisations. This was also the case in the operations examined in the context of this investigation. At the same time it is not always possible to know in which part of the world a specific person on the internet is located and to what extent investigating this person is relevant for the tasks of the service.

On the other hand these investigative activities of GISS often touch on the interests and the legal order of other countries. The service also gathers data that has only minor importance for the Netherlands but which may be critical for another country. The reverse situation also occurs. In addition, when the service operates on social media using agents, the acts of these agents may have significance or consequences in other countries as well. Examples include remote hacking, where the hack is potentially aimed at a computer in another country.[58] Finally, many forms of social media are set up by foreign companies, making GISS dependent on the cooperation of foreign services for the acquisition of data.

The above situation does not only apply to GISS, but also to many foreign services. The investigations examined all showed evidence of strong mutual interest in cooperation with foreign services in the field of social media. These investigations also indicated an intensification of such international cooperation. The cooperation takes various forms, among others the exchange of personal data, including data collections such as web forums, and the coordination of operational investigations.

As was briefly mentioned above, social media providers are often established outside the Netherlands. This means that the data collections, too, are often located outside the Netherlands. This obviously limits the possibilities for GISS to conduct searches at these providers on its own. Like any user of social media, GISS knows in which country a specific provider of social media is established. In order to be able to successfully gather data GISS can make a request to the sister service in that country. As was already described for the situation in the Netherlands in section 5.4, foreign services likewise have several ways in

[58] This problem was also encountered in relation to the Cybercrime treaty. *Parliamentary Papers II* 2004-05, 30 036, no. 2, p. 9 and *Parliamentary Papers II* 2012/13, 28 684, no. 363.

which they can gather stored data. Moreover, a foreign service may have different powers.[59] As a rule GISS cannot know how the foreign service has gathered the requested data.

GISS regularly cooperates with foreign services in the context of agent operations on social media. Cooperation makes it possible for GISS, while conducting such operations, to take the interests of these countries into account and to get a clear picture of which service is investigating which persons. Moreover, cooperation will prevent a foreign service from needlessly devoting attention in its investigations to a person who eventually transpires to be an agent of GISS. In some cases the international nature of social media necessitates more extensive coordination with foreign services concerning the deployment of agents and their areas of attention.

In addition to specific focused (targeted) requests, GISS also exchanges data collections of social media on a limited scale. This happens in the first place in the form of cooperation regarding web forums. The practice was already discussed in general in the review report on the processing of telecommunications data.[60] Within the scope of the present investigation the Committee has taken a closer look at whether the web forums exchanged in the review period were exchanged lawfully.

5.5.2 Findings

The Committee is already conducting another in-depth investigation into the cooperation of GISS with foreign services across the full spectrum.[61] The present investigation therefore focused mainly on the exchange of data collections *of* social media and the coordination of operational investigations *on* social media. In addition, it addressed the question whether GISS used its cooperation with foreign services to sidestep its own legal restrictions.

The Committee has not found any evidence that when GISS submits requests for searches, it asks the foreign service to use methods which GISS itself is not permitted to use. As regards their nature and scope, the requested searches in the investigations which the Committee examined were in each case consistent with the own powers of GISS.

The Committee has not established any unlawful actions in operations carried out jointly by GISS and foreign services. In such operations GISS generally proceeds with due care and deliberation, and the reporting is adequate. In one case GISS disclosed the nicknames of agents to the foreign service. In general the Committee appreciates that it may be necessary to demonstrate a certain level of openness regarding the deployment of agents, especially in the case of deployment on social media. In this particular case, however, it holds the opinion that there was no need to do so. The Committee recommends, also having regard to article 15, that GISS strictly adhere to the rule of source protection.

The Committee holds the opinion that in virtually all cases it investigated the sharing of web forums with foreign services was done lawfully. The only exception will be explained below. The Committee repeats the recommendation in its review report on the processing of

[59] In the review report on the processing of telecommunications data the Committee explained how GISS (and DISS) handle the differences in powers. CTIVD review report no. 38, section 5.1.
[60] Idem, section 5.6.
[61] Announced on 27 March 2013.

telecommunications data that GISS, when it acquires a web forum via a foreign service, record in writing why examination of the content of the web forum is legitimate.[62]

Precisely where social media are involved, the investigations of GISS in the context of performing its security task (its a-task) are strongly interconnected with the internal security of other countries. When GISS has a large volume of data in its possession with potential relevance to the security of other countries, seeking cooperation expresses due care. There is also a commitment to achieve careful and timely interpretation of the available data. This commitment is not only based on the own tasks of GISS but also on international and European law. The Netherlands has ratified many treaties and signed political statements by which it has committed itself to cooperate in the prevention of terrorism.[63]

The Committee makes the following comments. GISS cooperates with foreign services on a basis of equality, and each service has its own priorities in the cooperation. This implies that sharing web forums with a number of foreign services does not automatically mean that it may be assumed that the acquired data will thus be adequately analysed. The fact is that each service will only focus on the targets that are relevant to itself. If no clear arrangements have been made, the risk that relevant data will not be spotted and, in extreme cases, that a plotted attack will go unnoticed, will be insufficiently eliminated. The Committee recommends that GISS seek as much as possible to arrive at a division of tasks in its cooperation with foreign services.

Over a long period GISS kept insufficient records of which web forums it shared with which services. The law requires GISS to keep records of all provision of personal data (article 42). As a result of deficient reporting, moreover, the information furnished to the Committee for its investigation of the processing of telecommunications data[64] was incomplete in this respect. Five cases involving the provision of web forums were not included in the overview furnished by GISS at the time. Nevertheless, the Committee holds the opinion that GISS lawfully provided these five extremist web forums to the foreign services concerned. Consequently the absence of this information did not affect the substance or the conclusions of the investigation of the processing of telecommunications data.

The decisive factor in determining whether a special power is exercised for the benefit of the service's own tasks or for the benefit of a foreign service is, whether its exercise makes a direct contribution to an ongoing investigation.[65] In a number of cases the acquisition of certain web forums did not directly contribute to any ongoing investigation of GISS and the emphasis was on the interest of the foreign service. In these cases GISS gathered data concerning foreign extremist or terrorist organisations which the service was not currently investigating itself. Since the web forums were not acquired for use in GISS' own ongoing investigations, the acquisition of these web forums must be considered giving support to the

---

[62] CTIVD review report no. 38, section 6 (under 3.5).

[63] For example: Council of Europe Convention on the Prevention of Terrorism, *Treaty Series* 2006, 34. Council of Europe and the OSCE, *Decision 7/06 Countering the use of the internet for terrorist purposes*, 5 December 2006. Council of the European Union, *The EU Counter-terrorism strategy*, 30 November 2005 (14469/4/05, adopted on 15/16 December 2005) and subsequent conclusions of the Council.

[64] CTIVD review report no. 38.

[65] CTIVD review report no. 22a on the cooperation of GISS with foreign intelligence and/or security services. *Parliamentary Papers II* 2009/10, 29 924, no. 50 (appendix), section 8.2. This report is available in English on www.ctivd.nl.

foreign services in question. The Committee holds the opinion that at least in four cases GISS acted unlawfully because there was no permission from the minister as required pursuant to article 59(5). The Committee also notes that it does not have the impression that it was the service´s intention in these cases to circumvent the statutory permission rules. In the opinion of the Committee the unlawful nature of these procedures had its basis in an interpretation, incorrect in the Committee´s opinion, of the distinction between acquisition for the benefit of the service's *own* ongoing investigations and acquisition *in support of* a foreign service. In line with its previous review reports the Committee considers the strict application of this distinction to be important.

Finally, GISS acquired a web forum for a foreign service while the Committee is not convinced that acquiring this forum was proportional. In this case the foreign service did have some evidence against one of the forum managers, but the Committee considered this to constitute insufficient justification for infringing the privacy of the forum users. A significant element in the Committee's considerations here is the fact that the forum itself was not a forum of radical persuasions. No attention whatsoever was given to these aspects in the permission under which the forum was acquired. Consequently, the Committee holds that the acquisition and the subsequent provision of this forum to the foreign service was unlawful. The Committee will discuss this case in greater length in the secret appendix.

6. Conclusions and recommendations

In the past few years GISS has invested a great deal in investigation on social media. The Committee has found from its examination of files that the investments of GISS aimed at making adequate use of the internet in the performance of its tasks are bearing fruit and that investigation on social media is becoming part of the mix of instruments available to the service. Since developments in the area of social media are very dynamic, keeping up with them requires the service to make a sustained effort.

The Intelligence and Security Services Act 2002 was drafted at a time when social media did not yet play the role in society which they have come to play by now. In the general sense the Committee has established that investigation on social media is consistent with the present statutory framework. By European standards, too, the law provides adequate safeguards. However, the statutory framework needs to be complemented on a number of specific issues such as the maximum storage periods for raw data and metadata analysis, as the Committee already recommended in its review report on the processing of telecommunications data.[66]

The digital context in which the investigative activities of GISS take place does mean, though, that in various areas its internal policies need to be adjusted regularly in order to give more effective implementation to the safeguards guaranteeing the protection of privacy. The Committee has established the regular occurrence of new (technical) possibilities for which no policies have been formulated yet and which are not always comparable to other procedures. The employees directly involved in this pioneering in the field of new possibilities can be expected to be continuously on the alert. Fundamental issues must be acknowledged in time and be discussed at the appropriate level.

Organisational embedding (section 5.1)

6.1 GISS closely follows developments in the field of social media and responds to them proactively. (section 5.1)

Passive investigation on social media (section 5.2)

6.2 Large volumes of data on social media are freely accessible to everyone, and are to be characterised as open sources. (section 5.2.1)

6.3 The Committee has established that GISS collects only a limited volume of data on social media by direct access to the internet. The operational teams generally collect data from social media by other means than by searching the internet for data themselves. The few results thus obtained had been acquired amply within the limits of the general power to collect data and had been processed with due care. The results do not point to investigations via the internet of such intensity or long duration as to require additional approval. There is no evidence either that the searches done entailed more than slight infringement of privacy and should thus have come to fall under the power of surveillance. (section 5.2.2)

6.4 Under certain circumstances, however, investigation in open sources may entail a further-reaching infringement of the privacy of the persons concerned. In certain

[66] CTIVD review report no. 38, section 6 (under 3.3 and 4.1).

cases, for instance, doing systematic checks on a person in open sources constitutes surveillance. The Committee has found that there are currently no guidelines within the service on the basis of which it can determine whether it must apply for surveillance permission for a more intrusive or more prolonged internet investigation. (section 5.2.2)

6.5 **The Committee recommends establishing a clear criterion for determining whether GISS must apply for a surveillance permission for a more intrusive or more prolonged internet investigation.** (section 5.2.2)

6.6 The Committee considers it important that the dividing line between the general power to acquire data and the deployment of agents under article 21 ISS Act 2002 is monitored. This line is crossed if an employee of the service becomes actively involved and enters into interactions with other users, even if he only does so to prevent being conspicuous. In that case he is operating under an assumed identity pursuant to article 21. The Committee has established that current policies do not sufficiently guarantee the distinction between the general power to acquire data and the deployment of agents. (section 5.2.2)

6.7 The Committee considers it undesirable and impracticable for GISS to record all observations made on the internet, but holds that relevant results must be documented. If results are not adequately documented, they are not available to other employees of the service and the verifiability of the products of GISS will decrease. (section 5.2.2)

6.8 **The Committee recommends that the service clarify its existing policies on the operational use of the internet and on the recording of results. Investigative activities on the internet on the basis of the general power must be clearly defined and distinguished from the more infringing special powers, and unambiguous rules for recording investigation results should be laid down.** (section 5.2.2)

6.9 The Committee notes that other sectors of society have shown a continuous rapid increase in possibilities in the field of automated systems for gathering data on the internet. Nowadays, various tools exist for social network analysis and monitoring. (section 5.2.2)

6.10 **The Committee recommends that the service, when developing new investigation methods in the area of social media, will at an early stage use knowledge in the field of (privacy) safeguards from other sectors and science. This will help ensure that new systems meet all the statutory requirements from the moment they are put into operation.** (section 5.2.2)

Active investigation on social media (section 5.3)

6.11 GISS deploys agents on social media to gather data, both its own employees and persons not in the employment of GISS (external agents). (section 5.3.1)

6.12 GISS deploys *external* agents on social media with due care and deliberation. Adequate records are kept of the directions given to agents and the data collected by them. (section 5.3.2)

6.13 **The Committee recommends, however, that in each case the online identities of the agents be recorded carefully. This is important for the agents' safety and the verifiability of the operation.** (section 5.3.2)

6.14 The Committee is critical of the deployment of GISS´ *own* employees as agents on the internet. A strategic framework exists for these operations. In actual practice, however, it is insufficiently implemented. All the operations that were examined by the Committee were deficient in particular in the matter of effective reporting. In five cases the nature of the deficiency is such that the Committee holds it to be unlawful. In these operations few or even no operational reports had been prepared, thus compromising the transparency and verifiability of these operations. The Committee´s investigation was made more difficult by the absence of effective reporting. (section 5.3.2)

6.15 **The Committee recommends that GISS bring reporting on ongoing operations in line with the customary standards applying at the service without delay.** (section 5.3.2)

6.16 In one operation the permission to deploy an employee of GISS as an agent was undated. The Committee holds this to be a lack of due care as a result of which it cannot be established whether permission was present at the start of the operation. (section 5.3.2)

6.17 The Committee has found that the absence of a case manager or other form of guidance contributed to the shortcomings in the area of reporting established by the Committee. GISS had already identified the problem in an internal evaluation. (section 5.3.2)

6.18 **The Committee recommends that GISS significantly improve the guidance provided to employee-agents on the internet, also addressing the question how it can improve the management and internal accountability of these operations.** (section 5.3.2)

6.19 Under strict conditions GISS may instruct agents to commit criminal offences. This can be necessary in operations on the internet in order that an agent is not conspicuous. In some operations the agent was for this reason given permission to commit criminal offences. In two cases the application for permission was submitted for approval to the head of the service (far) too late. The Committee holds the opinion that these are formal shortcomings. In the Committee's opinion the permissions subsequently issued did not repair the lack of due care. (section 5.3.3)

6.20 **With respect to another operation the Committee recommends that GISS reconsider whether it must apply for permission to commit criminal offences. The agent in question may be crossing the limits of what is permitted under criminal law with his statements on the internet.** (section 5.3.3)

6.21 The Committee has established that in the operations it has examined, with one exception, it was decided not to inform the National Public Prosecutor (LOvJ) of the permission to commit criminal offences. The Committee points out that according to internal policy the LOvJ must in principle be informed of any permission to commit criminal offences. In its review report on a number of long-term agent operations

issued in June 2014 the Committee recommended that LOvJ be informed of *all* permissions to commit criminal offences. (section 5.3.3)

6.22 In operations in which permission to commit criminal offences has not been given, agents must operate within the limits of criminal law. In the case of *external* agents the case manager will ensure that they do so. The Committee holds the opinion that in all the operations it examined the case managers fulfilled this task adequately. (section 5.3.3)

6.23 In four of the five agent operations mentioned under 6.14, permission to commit criminal offences had been given. The deficient reporting on these operations also meant that nothing was recorded with regard to the commitment of criminal offences. This deficiency is so serious as to make the implementation of the permission to commit criminal offences unlawful. Because of the deficient reporting the Committee has been unable to assess whether these agents were given sufficient directions or whether compliance with the prohibition on incitement was sufficiently ensured. (section 5.3.3)

Investigation by acquiring data collections of social media (section 5.4)

6.24 Providers of social media often keep data collections in which they store user data and communication content. Via hacks, agents or foreign services GISS can try to gain access to all or part of such data collections. They can then conduct focused (targeted) searches in the data collections (e.g. a jihadist web forum).

6.25 The examined hacks done by GISS to acquire web forums were all properly substantiated by reasons. Each of the hacked web forums was relevant in its entirety for the performance of tasks by GISS and permission for the hack had generally been given at the competent decision level. In some cases permission for a remote hack was given by a unit head, while this should have been done at director level. The Committee considers this a lack of due care. (section 5.4.2, under a))

6.26 Most of the human sources (informers and/or agents) who acquire data collections or conduct focused (targeted) searches are deployed by the supporting team. Since early 2013 the proportionality of deploying human sources is no longer assessed at all. (section 5.4.2. under b))

6.27 With regard to five agent operations the Committee holds the opinion that the substantiation of the deployment of the agents concerned was so deficient that the permissions for them had been given unlawfully. This had the result that several web forums were acquired without any careful prior assessment of necessity, proportionality and subsidiarity having been laid down in writing. (section 5.4.2, under b))

6.28 In March 2013 the service drafted an internal proposal to improve the substantiation of applications for approval, but the implementation of this proposal was not taken in hand in the review period, so that the established substantiation deficiencies have continued to exist. GISS stated that the procedures had recently been adjusted, though this still had to be translated into internal policy rules. The Committee

considers that the service could have been expected to show greater alertness in the matter. (section 5.4.2, under b))

6.29 **The Committee recommends that GISS shortly lay down the adjusted procedures in written policies.** (section 5.4.2, under b))

6.30 The Committee has established that in 2011 the legal affairs department of GISS prepared a thorough policy memorandum on the acquisition of data collections, encompassing all relevant safeguards. GISS has not taken the implementation of the memorandum in hand, however. (section 5.4.2, under c))

6.31 **The Committee recommends that GISS shortly establish a binding policy on the acquisition of data collections (including web forums).** (section 5.4.2, under c))

6.32 The Committee has examined the acquisition of web forums in the review period. The Committee has found that in virtually all cases these were web forums whose acquisition was necessary for the performance of tasks by the service. (section 5.4.2, under c))

6.33 In four cases, however, the Committee holds the opinion that the acquisition of web forums did not pass the proportionality test and that they had been acquired unlawfully. These were large web forums where the infringement of the privacy of the other users was disproportionate in relation to the number of targets present on the forum and the results to be expected. Furthermore the Committee considers it a shortcoming that the acquisition of these web forums was continued for several years without its necessity and proportionality ever having demonstrably been a subject of discussion. (section 5.4.2, under c))

6.34 In by far the larger part of the operations examined, permission was obtained at the required level. There are a few exceptions to this general picture. In one case GISS received 'streaming' (real time) telecommunication, just as happens with a tap. In the absence of the minister's permission the Committee holds the opinion that this activity was unlawful. (section 5.4.2, under d))

6.35 The Committee further points out that the Mandate Decision provides that permission to exercise special powers must be obtained at a higher level if fundamental considerations play a role. The Committee holds the opinion that GISS wrongly failed to do so for the acquisition of some data collections since these required an assessment of fundamental considerations given the fact that the acquisition entailed infringement of the privacy of large numbers of other users. By failing to obtain permission at a higher level the service acted with a lack of due care. (section 5.4.2, under d))

6.36 Data or data collections of social media acquired by GISS must be processed with due care. This means among other things that GISS must consider, before acquiring data, whether the service is capable of effectively processing the data. (section 5.4.2, under e))

6.37 In one specific case the Committee doubts whether GISS had sufficient capacity to effectively process the data acquired, either on its own or in cooperation with foreign

services. For the time being the Committee sees no reason to qualify the acquisition of this data as unlawful, but it emphasizes the need for careful consideration of this issue. (section 5.4.2, under e))

6.38 GISS may use data which it has collected in behalf of its security or intelligence task by means of exercising special powers, for other tasks as well, e.g. security screenings. The Committee holds the opinion that this applies only to *evaluated* data. It holds the opinion that the internal procedure allowing employees to examine *unevaluated* data in behalf of the b-task of GISS (security screenings) is unlawful. The law does not provide an adequate basis for this. (section 5.4.2, under f))

6.39 The Committee recommends that the procedure be revised on this point and that the possibility of providing data be limited to evaluated data. It recommends that the possibility for security screeners to do administrative checks in systems including unevaluated data be eliminated. (section 5.4.2, under f))

6.40 As the Committee already observed in its review report on the processing of telecommunications data, the law does not set maximum storage periods for unevaluated (raw) data, apart from the rules applying to sigint. The Committee points out that even without further express legislation on the issue GISS is required to remove and destroy data if it has lost its relevance. (section 5.4.2, under g))

6.41 **The Committee recommends that GISS itself set maximum storage periods for unevaluated data of web forums, in anticipation of a possible amendment of the law. If unevaluated data is no longer relevant to ongoing investigations, it should be removed as far as this is (technically) possible.** (section 5.4.2, under g))

6.42 The Committee further holds the opinion that it was permissible for GISS to store the web forums examined by the Committee until now insofar as the Committee has not considered them to have been acquired unlawfully. (section 5.4.2, under g))

6.43 Over a long period no systematic records were kept of the focused (targeted) searches for data on social media which human sources were instructed to conduct. As a result, not all the files that were examined make it possible to verify which data was acquired for which purpose. (section 5.4.2, under h))

6.44 **The Committee recommends that GISS, when it instructs human sources to search data collections of social media, keep records of each separate search request.** (section 5.4.2, under h))

6.45 **The Committee recommends that GISS, when instructing a human source to gather data that are comparable to traffic and user data, follow the internal procedure for activities under article 28 ISS Act 2002 This means that a substantiated application for permission must be submitted to the head of the service.** (section 5.4.2, under h))

6.46 The ISS Act 2002 creates an exemption for informers, releasing them from other legal obligations when they provide data to GISS. Contrary to the rules applying to informers, the law does not expressly make such provision for agents who provide data. Since the considerations of the legislator underlying the exemption for informers evidently also apply to the situation in which agents provide data, the Committee holds the opinion that this exemption applies to agents as well. This

means that agents may provide data to GISS under the same conditions as informers. (section 5.4.2, under i))

Cooperation with foreign services (section 5.5)

6.47 The international context of social media compels GISS to cooperate with foreign services. The Committee has established great mutual interests in such cooperation. (section 5.5.1)

6.48 The Committee has not come across any evidence in this in-depth investigation that GISS has been sidestepping its own powers when making requests for searches on social media via foreign services. The service also acts with due care and deliberation when coordinating its own investigations in regard to social media with foreign services. (section 5.5.2)

6.49 **The Committee recommends, though, that GISS adhere strictly to the rule of source protection in the matter or sharing nicknames of its own agents with foreign services.** (section 5.5.2)

6.50 **The Committee recommends, as it already did in its review report on the processing of telecommunications, that GISS, when it acquires a web forum via a foreign services, record in writing why examination of the content of the web forum is justified.** (section 5.5.2)

6.51 When GISS has a large volume of data in its possession with potential relevance for the security of other countries, seeking cooperation expresses due care. There is also a commitment to achieve careful and timely interpretation of the available data. Sharing web forums with a number of foreign services does not automatically mean that it may be assumed that the acquired data will thus be adequately analysed. If no clear arrangements have been made, the risk that relevant data will not be spotted and, in extreme cases, that a plotted attack will go unnoticed, will be insufficiently eliminated. (section 5.5.2)

6.52 **The Committee recommends that GISS seek as much as possible to arrive at a division of tasks in its cooperation with foreign services.** (section 5.5.2)

6.53 GISS exchanges a number of web forums with foreign services. If such a web forum does not contribute directly to any ongoing investigation of GISS, the acquisition constitutes giving support to a foreign service. This means that the minister must give permission for acquiring such a forum. The Committee holds the opinion that in four cases GISS acted unlawfully because the minister's permission was absent. (section 5.5.2)

6.54 In one other case than those mentioned above the Committee holds the opinion that the acquisition did not satisfy the requirement of proportionality. The Committee holds the opinion that this forum was acquired unlawfully. (section 5.5.2)

Thus adopted at the meeting of the Committee held 16 July 2014.

REVIEW COMMITTEE
for the
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 39

APPENDIX

Overview of the assessment framework belonging to the review report on the investigations of GISS on social media

The various methods for investigating on social media are characterized below by reference to the relevant requirements set by the ISS Act 2002, so as to achieve a clear overview of the assessment framework in an accessible way. The methods mentioned are further elaborated in section 5. It should be pointed out that this overview is not exhaustive, but is intended to provide a concise summary of the assessment framework.

Passive investigation on social media

Requirement	*Elaboration*
Legal basis	Articles 6 and 12 ISS Act 2002
Definition	Investigating open sources
Permission	None
(Formal)requirements	- exercised for a specific purpose, only insofar as necessary (12) - proper and due care, mention of source or reliability (12)
Limits	- include data of third parties only if necessary (13) - more than minor infringement of fundamental rights, e.g. privacy, to be assessed inter alia on the basis of intention, nature of the methods and storage of data - systematic focused (targeted) investigation (20) - operating under an assumed identity (21)

Surveillance of persons on social media

Requirement	*Elaboration*
Legal basis	Article 20 ISS Act 2002
Definition	Investigation focused on an individual which by the criteria of duration, location, intensity, frequency or the means used constitutes systematic surveillance
Permission	By team head
(Formal)requirements	- exercised for a specific purpose, only insofar as necessary (12) - Proper and due care, mention of source or reliability (12) - substantiation (20) - reporting (33)
Limits	- include data of third parties only if necessary (13) - necessity, proportionality and subsidiarity (18, 31, 32)

Active investigation on social media by agents

Requirement	*Elaboration*
Legal basis	Article 21 ISS Act 2002

Definition	Operating on social media by agents, possibly using an assumed identity
Permission	By director or unit head, permission for continuation by team head
(Formal)requirements	- exercise for a specific purpose, only insofar as necessary (12) - proper and due care, mention of source or reliability (12) - substantiation - reporting (21(6), 33))
Limits	- necessity, proportionality and subsidiarity (18, 31, 32) - prohibition of instigation : 'Tallon criterion' (21(4)) - safety of agent (15) - criminal offences only if permission and instruction are available (21(3))

Acquisition of data collections of social media

Requirement	***Elaboration***
Legal basis	Articles 17, 21, 24, 59 ISS Act 2002
Definition	Gathering (parts of) data collections of social media
Permission	Depends on authorisation
(Formal)requirements	- exercise for a specific purpose, only insofar as necessary (12) - proper and due care, mention of source or reliability (12) - substantiation (21, 24) - reporting (33)
Limits	- include data of third persons only if necessary (13) - proportionality and subsidiarity (31, 32) - necessary for a-task or d-task, unless the legal basis is article 17 (18)

Making accessible and storing data collections of social media

Requirement	***Elaboration***
Legal basis	Articles 6 and 12 ISS Act 2002
Definition	Analysing, making accessible, storing data
(Formal)requirements	- exercise for a specific purpose, only insofar as necessary (12) - proper and due care, mention of source or reliability (12) - protection of data, among others against unauthorised processing (16) - authorization policy (16, 35) - remove and destroy when data is no longer relevant (43) - *previously, the Committee recommended introducing statutory rules on maximum storage periods of raw data as well as rules on processing metadata*
Limits	- include data of third parties only if necessary (13) - necessary for a-task or d-task unless the data was acquired pursuant to article 17 (18)

Exchanging data collections of social media

Requirement	***Elaboration***
Legal basis	Articles 36 *or* 59 ISS Act 2002
Definition	Providing data collection to a foreign service and/or receiving data collection from a foreign service
Permission	By team head or unit head (36) *or* minister (59)
(Formal)requirements	- exercise for a specific purpose, only insofar as necessary (12) - proper and due care, mention of source or reliability (12) - keeping records (42) - third-party rule (37)
Limits	- necessary for own task (36) *or* - in the interest served by the foreign service (59)

Requesting focused (targeted) searches of data collections of social media

Requirement	*Elaboration*
Legal basis	Articles 17, 21 and 59 ISS Act 2002
Definition	Focused (targeted) searching in data collections via human sources or foreign services
(Formal)requirements	- exercise for a specific purpose, only insofar as necessary (12) - proper and due care, mention of source or reliability (12) - records of instructions to agent (21(6)) - substantiation if equivalent to article 28
Limits	- proportionality and subsidiarity (31, 32) - necessary for a-task or d-task, unless legal basis is article 17 (18)