Toetsingscommissie
Inzet Bevoegdheden

Annual report 2018/2019

Binnenhof 19
2513 AA The Hague
www.tib-ivd.nl

Disclaimer: no rights may be derived from this translation and under all circumstances the official Dutch text of the *Jaarverslag 2018/2019* of the TIB prevails.

The TIB intended to include the total number of authorized requests of the AIVD and the MIVD in this annual report, per intelligence and security service. However, the Minister of the Interior and Kingdom Relations and the Minister of Defence are of the opinion that including these numbers separately would give too great an insight into the services' modus operandi. These numbers are therefore considered to be state secrets in their separated form and may only be recorded as a joint number for both services. The Ministers did not consider the joint number to be a state secret.

Summary

The Investigatory Powers Commission (TIB) was introduced in the ISS Act 2017 which entered into force on 1 May 2018. When the intelligence and security services AIVD and MIVD wish to use certain special investigatory powers, they need the authorization of the Minister of the Interior and Kingdom Relations and the Minister of Defence respectively. The TIB then reviews whether that authorization was given lawfully. In practice, the TIB reviews the request underlying the authorization. If the TIB deems the authorization to be lawful, the service may use the investigatory power. Only in urgent cases does the TIB review the request after the fact. In this annual report the TIB accounts for the way it assesses the authorization of requests.

In the past year, TIB implemented the legal framework in practice. There must be a necessity for exercising a special investigatory power. The importance of the investigatory power to be used is weighed against the detriment the use will cause (proportionality). This concerns 'targets', but also people who are not targets but who will be impacted by the investigatory power. In addition, it is ascertained made to see whether the lightest remedy was used to obtain the required information (subsidiarity). Furthermore, an assessment is made whether the use of the intended means is as targeted as possible.

In the period from 1 May 2018 to 1 April 2019, the TIB assessed a total of 2,159 requests from both services. In 4.5% of those requests from the AIVD, the TIB ruled that the authorization had been granted unlawfully. That percentage is a decrease compared with the period 1 May to 1 October 2018 (5.5%), which is due to the fact that the requests are now better substantiated and the number of avoidable errors has decreased. In 5.8% of the requests from the MIVD, the TIB ruled that the authorization had been granted unlawfully. That is a relative increase compared with the preceding period (4.1%). This representation is not entirely accurate, however, because the use of a single power was deemed unlawful for which separate requests had been submitted. If this investigatory power had been submitted in one request, the percentage of MIVD requests that were deemed unlawful would have been lower.

The main reasons for ruling that requests were unlawful were flaws in the substantiation of the proportionality or in the proportionality itself and/or the subsidiarity of the use of the investigatory power. In the annual report this is illustrated by a bulk hack to be carried out on a company which was deemed unlawful, because of a lack of substantiation justifying the untargeted acquisition of data from millions of people (proportionality). In that case, requesting data regarding individual 'targets' was also an option (subsidiarity).

The TIB also assessed requests related to a new investigatory power of the intelligence and security services: the investigation-specific interception on Internet cables. The TIB initially ruled that the required use was not proportional and not as targeted as possible and that therefore the authorizations granted by the Ministers were unlawful. New requests were subsequently submitted to use this investigatory power, in which the scope of the use was limited. The TIB ruled these requests as lawful with a proviso.

Table of contents

1 Preface

It is my pleasure to present the first annual report on the work conducted by the Commission for the Review of the Exercise of Investigatory Powers (or the Investigatory Powers Commission and referred to in Dutch as: TIB). On 1 April 2018, the TIB initiated an induction programme. The following month, the TIB began its task of assessing the Ministers' authorizations for the use of special investigatory powers by the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). This annual report is a summary of the results of the TIB's first year of work.

TIB's first year was marked not only by assessing requests but also by building its organization. The TIB is housed in the building of the Ministry of General Affairs at the Binnenhof in The Hague. The TIB was set up with the support of various employees from this ministry, to whom we are grateful.

The formation and implementation of the TIB in legislation was no easy task. The expectations for the lawfulness review to be conducted by the TIB varied widely. Some thought that the TIB would rubber stamp authorizations whereas others feared the services would get entangled in red tape. Neither has happened. The assessments are conducted with diligence and a critical eye. The Minister of the Interior and Kingdom Relations stated: "The TIB is an independent body, whose review is a substantive match for that of the courts"[2]. In short, the bar was and is set high.

From its inception, the TIB has greatly valued its independence. Independence is a significant prerequisite to conduct balanced and credible assessments. The TIB must take into account the interests of the services working to keep our society safe, but on the other hand it must also consider the legitimate interest of citizens' privacy.

Generally citizens are unaware if their privacy is infringed. The services are aware when the TIB rules an authorization granted as unlawful. The TIB's assessment was recently described as 'strict' by the Minister of the Interior and Kingdom Relations and the Minister of Defence. It was also remarked that the assessment contributed to the improved quality of the requests submitted by the services and that it has even resulted in a new standard being set. The TIB has also noticed this. This improvement was necessary on a number of points. The services have far-reaching investigatory powers and in a democratic society the services are expected to use these powers with due deliberation and to be able to justify their use.

You may rightly expect the TIB to be strict in its assessments. That is what the TIB did in the first year of its existence and what we will continue to do.

Mariëtte Moussault
Chair of the Investigatory Powers Commission

[2] House of Representatives, session year 2016–2017, 34 588, no. 18, p. 35.

2 Introduction

The TIB's composition and investigatory powers are regulated by the new Intelligence and Security Services Act 2017 (ISS Act 2017), which fully entered into force on 1 May 2018. That was also the day the TIB started its assessment work. In setting up the TIB, the legislator responded to the criticism expressed in the consultation phase of the ISS Act 2017 about the lack of prior independent assessment of the use of an investigatory power by the intelligence and security services. That would have resulted in a failure to comply with the requirements arising from case law related to the European Convention on Human Rights.

The TIB's task is described in Article 32 of the ISS Act 2017. The TIB is charged with reviewing the lawfulness of the authorizations granted by the Minister of the Interior and Kingdom Relations or the Minister of Defence for the use of investigatory powers by the AIVD and the MIVD. The TIB's ruling is binding. That means that if the TIB rules an authorization granted by the Minister to be unlawful, that investigatory power may not be used. Thus there is an independent binding review before the services' use a special investigatory power. If the urgency is so high that review by the TIB cannot be awaited, the urgency procedure may be applied. Only in that case may an investigatory power be used *before* review by the TIB.

The Minister's authorization is based on a written request. In practical terms, the TIB reviews the contents of that written request. For readability purposes this annual report will from this point on refer to 'requests' that are reviewed.

The TIB consists of three members of whom at least two have six or more years' judiciary experience. The third member is not required to have judicial experience, which is how the ISS Act 2017 offers room to appoint a member with technical expertise. Members are appointed following an extensive procedure involving firstly the judiciary power, subsequently the legislative power and finally the executive power. The TIB's supporting structure has both judicial and technical expertise, so that both of these aspects are addressed when preparing for decision making.

The TIB spent April 2018 completing an intensive preparatory programme in the run up to the ISS Act 2017 entering into force. This included presentations from the Review Committee on the Intelligence and Security Services (hereinafter: CTIVD), the Ministry of the Interior and Kingdom Relations and the Ministry of Defence as well as the AIVD and the MIVD. These presentations covered the legislative framework and provided an understanding of the services' procedure and the various ongoing operations. The TIB then drew up the internal legal framework. Its procedure is laid down in Rules of Procedure[3]. This sets out when the TIB meets and how decisions are made.

On 1 November 2018, the TIB published a letter of progress. This annual report elaborates on a number of elements that were already touched on in the letter of progress. The TIB must report on

[3] Government Gazette 14 May 2018, 26358.

the preceding 12 months before 1 May of each year, based on the ISS Act 2017. The figures used in this report are based on the period 1 May 2018 to 1 April 2019.

The TIB considers it important to shed light on how it implements the lawfulness review. Key terms in this respect are proportionality and subsidiarity. These terms are general legal terms and not limited to the ISS Act 2017. Chapter 3 discusses this in more detail. That chapter specifically addresses automated data analysis and hacking power.

Following the referendum on the ISS Act 2017, the Minister of the Interior and Kingdom Relations and the Minister of Defence indicated the importance of the TIB reporting explicitly on the investigation-specific interception on internet cables. The TIB underlines this importance to provide insight into the use of this investigatory power. In Chapter 3 the TIB will therefore, as far as publically possible, discuss the way in which it has implemented the lawfulness review where this investigatory power is concerned.

It essential that the TIB is fully informed. That applies to the specific requests submitted and in a broader context. Chapter 4 examines how the TIB was informed during the preceding year.

Chapter 5 contains the results of the reviews conducted by the TIB. This chapter will provide an overview of the number of requests reviewed by the TIB and their results. Chapter 6 draws conclusions on the basis of these results and offers an outlook for the coming year.

Special investigatory powers assessed by the TIB

Not all investigatory powers that the AIVD and the MIVD are allowed to use require the Minister's authorization, which is subsequently assessed by the TIB. The TIB only assesses requests related to the following special investigatory powers under the ISS Act 2017:

- Surveillance within a home (Article 40, paragraph3)
- Investigation of enclosed areas and enclosed objects where it concerns a home (Article 42, paragraph 4)
- DNA testing (Article 43, paragraph 2 and 4)
- Hacking (Article 45, paragraph 3, 5 and 10)
- Investigating communication such as intercepting telephone communication (Article 47, paragraph 2)
- Investigation-specific interception (intercepting satellite or cable communication), selecting the outcome and automated data analysis aimed at identifying individuals or organizations (Article 48, paragraph 2, Article 49, paragraph 4, and Article 50, paragraphs 2 and 4)
- Duty to comply for communication services providers (Article 53, paragraph 2)
- Providing data by communication services providers or data storage providers (Article 54, paragraph 2)
- Cooperating with data decryption (Article 57, paragraph 2)

3 Review framework

The TIB reviews whether the authorization to use a special investigatory power granted by a Minister to the MIVD or the AIVD is lawful[4]. How does the TIB conduct that review? Which factors are weighed and which are not? To answer these questions, this chapter discusses the review framework that the TIB uses[5]. The TIB first sets out the outlines it uses which apply to the majority of the requests. Some topics are looked at in greater detail such as automated data analysis, hacking and investigation-specific interception on the cable. However, each request is reviewed on its own merits and all aspects included in a request are carefully weighed each time.

3.1 Legal uniformity

In its reviews of requests for authorization, the TIB uses the legal framework as established in the ISS Act 2017 and the corresponding legislative history against the background of the European Convention on Human Rights. Where the legislation needs to be interpreted for application in practice, the TIB and the CTIVD consult to formulate a joint legislative interpretation promoting a uniform and consistent application of law[6]. The resulting legal uniformity letters published by the CTIVD and the TIB specify the criteria that an authorization request considered lawful by the Ministers must meet to fall within the legal framework and to be ruled as lawful by the TIB. This framework is the starting point for review by the TIB.

3.2 The review by the TIB

It is clear from the legislative history of the ISS Act 2017 that the TIB's lawfulness review is not a marginal one[7].

> "The TIB will be presented with the same body of facts as the Minister and will be able to subject to a lawfulness review the full extent of investigatory powers intended in that context."

A request must meet a number of formal legal requirements and subsequently a review is made based on the criteria necessity, proportionality, subsidiarity and 'as targeted as possible'. These criteria are not only reviewed in isolation but also in conjunction with each other.

[4] Section 36 of the ISS Act 2017.
[5] For the sake of completeness it should be remarked that if it concerns one of the situations as described in Section 30, subsections 2 and 3, of the ISS Act 2017, the court of The Hague must grant authorization at the Minister's request before the investigatory power can be used.
[6] House of Representatives, session year 2016–2017, 34 588, no. 18, p. 40.
[7] House of Representatives, session year 2016–2017, 34 588, no. 18, p. 39.

3.2.1 Legal requirements for a request

The Minister grants authorization based on a request by the service. This request with the Minister's authorization is then submitted to the TIB and forms the basis of the review. Firstly the TIB reviews whether the request meets the formal legal requirements[8]. The request must list which investigatory power is being requested, who or what the target[9] is, which investigatory power it concerns, what the purpose of this investigatory power is and why it is necessary to use this investigatory power.

Where it concerns an extension of an investigatory power, the request must also record the results of the previous use of that investigatory power. The TIB considers it important to be sufficiently informed in this area. If multiple telephone numbers belonging to a target are intercepted, for example, the TIB will want to know the results for each telephone number in the preceding period, as a phone number listed as the target's could in actual fact turn out to be used by the partner. In that case, the intercepted calls are not automatically of interest to the investigation and as a consequence, the requested extension to intercept that particular telephone number might not be lawful.

3.2.2 Necessity

The request must adequately substantiate the necessity to use the investigatory power. The TIB firstly reviews to what extent a request may be linked to one of the goals from the Integrated Security and Intelligence Order[10]. However, reviewing the criterion necessity is not limited to this procedural check. The Integrated Security and Intelligence Order alone is not concrete enough to serve as a basis on which to review the necessity of using an investigatory power against a specific target. For example, it must be safeguarded that any current or former resident of a country listed in the Integrated Security and Intelligence Order, or anyone who has ever visited that country or been in contact with someone from that country, becoming the subject of these investigatory powers. For that reason, the nature of the threat posed by that specific person or organization must be substantiated and made plausible in light of the abstract goals as included in the Integrated Security and Intelligence Order.

The TIB does not make its own evaluation of the presented threat, but reviews whether the threat presented in the request has been sufficiently substantiated and forms a reason to use the requested investigatory power. It thus reviews whether the necessity has been adequately substantiated[11].

By way of illustration: far-right extremism is one of the AIVD's focus areas[12]. If the AIVD wishes to intercept the communication of a far-right target, the TIB does not review whether this focus area is

[8] Section 29 of the ISS Act 2017.
[9] 'Targets' are persons or organizations that, because of the goals they pursue, potentially represent a threat to the continued existence of the democratic rule of law, or to the security or other vital interests of the State.
[10] The Integrated Security and Intelligence Order is the substantive implementation of the services' legal duties and serves as the instrument with which the government shows the services what it considers necessary to ensure a safe country, a well-informed government and effective international security.
[11] House of Representatives, session year 2018-2019, 34 588, no. 18, p. 18.
[12] House of Representatives, session year 2018-2019, 30 977, no. 154.

necessary for the Netherlands. The TIB does, however, review if sufficient reasons have been given to show that the target supports extremist ideology and that this target poses a threat that justifies using a special investigatory power against him or her.

3.2.3 Proportionality

In the case of proportionality, the importance of the investigatory power to be used is weighed against the detriment the use will cause to the parties involved, which is generally an infringement of privacy. The TIB is of the opinion that everything that contributes materially to the weighing of interests must be considered. In the case of a large threat, the use of a severe investigatory power is more likely to be justified than in the case of a small threat. Everything that contributes materially to the detriment of privacy must be weighed. The number of parties involved that may be affected by the use of the investigatory power is also relevant. When intercepting data from satellite or cable communication, the privacy of as many as millions of individuals may be affected. That not only includes targets, but mainly people in whom the services have no interest. That use of investigatory power may be considered proportional if an attack could be prevented in that way.

In a legal uniformity letter[13] on the scope of review, the TIB and the CTIVD asserted that they also consider it necessary to be informed if data can reasonably be expected to be shared with other – foreign – services when investigatory powers are used. The TIB reviews the infringement of individual privacy as greater if the data will be obtained not by one but by multiple services, in particular if this affects individuals who are not the focus of the services' attention. It is not always clear what the exact content is of the bulk data provided to other – foreign – services. In the context of proportionality, the extent of the entire possible infringement must be reviewed.

The TIB does not review whether the data, once obtained, may or may not actually be shared, nor whether cooperation with the partner service is appropriate. That decision is reserved for the Minister and is reviewed by the CTIVD.

3.2.4 Subsidiarity

The subsidiarity test means reviewing whether the lightest possible investigatory power is used. Sometimes that is easy to review: if information is accessible through open sources, intercepting telephone communication is not necessary.

However, more complex hacking operations often require legal and technical expertise to be able to review if the lightest means will be used. That also applies to the question whether the means is used as targeted as possible (see below). The TIB has the expertise to do this. The TIB has a member and an employee with extensive technical knowledge.

In some cases, the subsidiarity review may coincide with the assessment of necessity and proportionality. For example, information may emerge of an imminent attack. In that case, it may be necessary, proportional and subsidiary not to first use a relatively light means which, if that does

[13] The scope of the lawfulness assessment. For more information, refer to the legal uniformity letter: https://www.tib-ivd.nl/documenten/brieven/2018/11/23/reikwijdte-rechtmatigheidstoetsing-tib

not have the desired effect, would be followed by a heavier means. In a case of this kind, the use of a heavy means or a combination of heavy means may well be ruled lawful.

3.2.5 As targeted as possible

The TIB uses the following criterion for 'as targeted as possible', as described in its response to the amendment proposal of the ISS Act 2017[14]:

> "The extent to which the acquisition of information that is not strictly necessary for the investigation is restricted to a minimum, given the technical and operational circumstances of the case"

This criterion is particularly relevant for special investigatory powers that infringe the privacy of many parties involved, such as in the case of investigation-related interception on the cable. The section on investigation-specific interception on the cable further details how this criterion is implemented.

3.3 Automated data analysis

In short, automated data analysis means the computerized processing of information which includes comparing the data or conducting comparisons, profile-based searches and correlations of the information in order to recognize certain patterns. Automated data analysis is described in Article 50, paragraphs 1b and 4, and Article 60 of the ISS Act 2017.

Automated data analysis of meta data files which are obtained by investigation-specific interception on the cable or satellite and which are aimed at identifying persons or organizations may potentially have far-reaching consequences for the infringement of that person's or organization's privacy. The files obtained through investigation-specific interception on the cable consist by their nature and contents for the greatest part of information from individuals who are not the focus of the services' attention. A simple search in these files may have major consequences. In technical terms, a search for telephone numbers called by one particular number is just as easy as the search which IP addresses contacted the internet from what location and which websites were accessed in the process over the past three years.

The CTIVD and the TIB conducted a legal uniformity meeting as a result of several submitted requests relating to automated data analysis based on Article 50, paragraph 1(b), of the ISS Act 2017. This meeting resulted in a legal uniformity letter that was sent to both Ministers[15]. The TIB and the CTIVD also discussed with the services and the ministries about the practical implementation of automated data analysis while observing the legal uniformity letter. At the time of writing this annual report, further discussion has been scheduled. Where it concerns the implementation of automated data analysis, it is important that the requirements of necessity,

[14] https://www.tib-ivd.nl/documenten/brieven/2018/08/23/reactie-wijzigingsvoorstel-wiv-2017
[15] https://www.tib-ivd.nl/documenten/brieven/2018/08/23/geautomatiseerde-data-analyse-ex-art.-50-wiv

proportionality, subsidiarity and as targeted as possible are complied with while at the same time the investigatory power remains effective.

3.4 Intruding into automated information systems (hacking)

Many people tend to think of hacking as breaking into a specific computer or the telephone of a target, but the reality is far more complex. The current technical world no longer consists only of computers that can be touched and picked up. In fact, virtual computers (virtual machines)[16] are the rule rather than the exception. These virtual computers can operate under full self-management and ownership but may also easily be rented anywhere in the world with just a few mouse clicks. The environment where these virtual computers operate may also accommodate other computers which belong to persons or companies who are not one of the services' targets and which could contain information of random other parties.

The technical interconnectedness of hardware, virtual hardware, software and network layers must be described in a request for complex hacking operations. The request must specify whether only the computerized device or system of the target will be hacked or whether other systems will be hacked as well. The request must also clarify how the service will operate within the network environment: can the devices of any other parties in that network environment also be affected? Are there technical risks for these parties, such as that a server of a random third party could fail, with all the associated consequences?

Strict interpretation of legislative history could lead to the situation where hacking is only permitted if conducted through another party, if an attempt was first made to enter the target directly and it was shown that the target could not be hacked directly[17]. This is not always feasible in practice. In the TIB's view, if there is sufficient substantiation in a specific case that it is not possible to hack a target directly as a result of considerable operational reasons, it may - under circumstances - be lawful to conduct the hack through another party without first having attempted to do so directly.

3.4.1 Technical risks

The ISS Act 2017 stipulates that in hacking operations the technical risks connected to breaking into systems by using this investigatory power must be listed. As the saying goes, you can't make an omelette without breaking eggs. The TIB must be able to review on the basis of the requests what the technical risks are and to what extent these risks are acceptable. The technical risks should therefore be described in unequivocal terms[18]. When reviewing the use of the hacking power, the TIB takes the following minimum elements into consideration:

- The risks regarding the accessibility and integrity of the computer systems involved. It may be unacceptable if significant risks arise for the accessibility or integrity of systems in the

[16] A virtual machine is a computer program that imitates a computer and on which other programmes can be executed.
[17] House of Representatives, session year 2016-2017, 34 588, no. 3, p. 78.
[18] Senate, session year 2016-2017, 34588, C, p. 15.

vital infrastructure or important systems of service providers being hacked as third parties or as 'non-target'[19].

- The risk that the technical means introduced by the services to maintain remote access to the hacked systems could be abused by others to also gain access to these systems[20].
- The risks associated with the use of known and unknown vulnerabilities. Exploiting vulnerabilities is part of the use of the investigatory power to hack an automated information system. The TIB must include this in its lawfulness review[21]. Where the use of an investigatory power includes exploiting a known or unknown vulnerability, that fact, including the corresponding technical risks, must be explicitly described and reviewed[22].

> "Where a vulnerability is exploited in the use of this investigatory power, this must transpire from the request for authorization, as must the associated technical risks"

The use of these vulnerabilities can have major societal consequences. This was evidenced by the outbreak of the WannaCry worm, for example, which abused leaked exploits for previously unknown vulnerabilities and which amongst others led to critical hospital systems becoming unavailable[23].

- The risks ensuing from potential detection of a hack, for example any consequential loss or reprisals following the hack of a third party.

3.4.2 Bulk hacks

At the request of the Minister of the Interior and Kingdom Relations, the TIB issued a response to the amendment proposal of the ISS Act 2017. The TIB included an additional point in its response that there is a difference in safeguards where it concerns bulk hacks and investigation-specific interception on the cable or in the ether. In both cases, data may be obtained in bulk, for example from service providers designated as 'non-target', including information that for the greatest part concerns individuals who are not the focus of the services' attention. Additional safeguards have been included in Article 50 of the ISS Act 2017 for investigation-specific interception, where it concerns learning the contents of data and conducting metadata analysis. As the situation currently stands, the TIB sees no grounds for the difference in safeguards – between interception via the cable or via the ether and interception via a hack – of how the data of these individuals is handled.

Where interception on the cable will only yield information about the communication sent from the time of interception, it is a different matter when it concerns a hack. Using bulk hacking powers, the

[19] The use of an investigatory power against a 'non-target' means that this person or organization is not designated an independent 'target' of the services, but that the use of that special investigatory power could lead to the information position regarding one or more targets being improved.
[20] House of Representatives, session year 2016-2017, 34588, no. 3, p. 80.
[21] House of Representatives, session year 2016-2017, 34588, no. 3, p. 12.
[22] Senate, session year 2016-2017, 34588, E, p. 4.
[23] Department of Health – National Audit Office (UK), "Investigation: WannaCry cyber attack and the NHS", October 2017.

information obtained in bulk may also be historic. Depending on the hacked party's storage method, this can precede the maximum term[24] that applies to the services themselves before they must review the information for relevance and destroy non-relevant data.

The hacking power also allows for the possibility that information is again obtained that was previously judged to be irrelevant or was not judged on relevance within a year and therefore destroyed. In this regard, the hacking power differs from investigation-specific interception, as in the latter case it is not possible to obtain the same information twice.

3.5 Investigation-specific interception on the cable

An important amendment in the ISS Act 2017 compared with the ISS Act 2002 is the investigatory power of investigation-specific interception on the cable[25]. This is an investigatory power where data may be obtained in bulk. It is inevitable that this data also contains data from a great many people who are not the focus of the services' attention.

At the end of 2018, the Minister of the Interior and Kingdom Relations and the Minister of Defence submitted authorized proposals to the TIB related to investigation-specific interception on the cable[26]. Given the major societal debate on including this investigatory power in the Act and the explicit request by the Minister of the Interior and Kingdom Relations and the Minister of Defence to report on this investigatory power[27], the TIB will specify in greater detail its review of requests for investigation-specific interception on the cable.

Following the submitted requests, the TIB posed a number of questions related mainly to the criterion as targeted as possible and proportionality of the proposed use of the investigatory power.

In the absence of an explicit definition of the criterion 'as targeted as possible' in the act, the TIB reviewed the requests by implementing its view as described in the response to the amendment proposal of the ISS Act 2017: "The extent to which the acquisition of information that is not strictly necessary for the investigation is restricted to a minimum, given the technical and operational circumstances of the case"[28]. It is a fact that investigation-specific interception on the cable can yield large amounts of data that is not required for the investigation. That fact alone is not a reason to review the granted authorization as unlawful, as it is inherent to the legally permitted investigatory power. The TIB is of the opinion that the more extensive the interception point, the greater the effort required to limit to a minimum the acquisition of data not strictly necessary for the investigation.

[24] Section 27 of the ISS Act 2017.
[25] The ISS Act 2002 allowed for the possibility to obtain untargeted satellite traffic. The ISS Act 2017, however, has one legislative regime for investigation-related interception regarding information conducted either by satellite or by cable.
[26] The requests came from both services, who each requested authorization for their own investigation assignments. That has no bearing on the number of 'access points' sought.
[27] House of Representatives, session year 2017-2018, 34588, no. 70.
[28] https://www.tib-ivd.nl/documenten/brieven/2018/08/23/reactie-wijzigingsvoorstel-wiv-2017

The TIB has identified a number of relevant factors regarding the submitted requests. These are (a) the chosen access point and the magnitude of the information flows accessible there, (b) the self-imposed limits by the AIVD and the MIVD regarding the actual information flows to be intercepted, (c) the way technical filters are applied, (d) the proposed handling of the metadata obtained and (e) the period for which the authorization is requested.

The factors (a) and (e) should be seen as communicating vessels. Should one of these factors be used widely as it were, the other factor should be restricted to ensure that the use is as targeted as possible. The TIB is of the opinion that this was not adequately done in the submitted requests. The TIB ruled that the use was not proportional and not as targeted as possible and therefore that the authorizations granted by the Ministers were unlawful.

As it concerned a new investigatory power and the services lacked experience in submitting requests for this investigatory power, the TIB not only substantiated its decision fully in writing but also provided a detailed explanation in a meeting with both services.

New requests regarding investigation-specific interception on the cable were again submitted in 2019. These new requests differed in scope from the previous requests. The requests also contained more specific information about the available information flows and in that way provide a greater understanding of the data that might be obtained. However, these requests still raised questions about the ‘as targeted as possible’ use of the power. The TIB asked further questions about this. The TIB ultimately judged that the authorizations related to the new requests could be reviewed as lawful with a proviso. The TIB cannot provide further comment on the exact contents of this decision in public, because this would give too great an insight into the modus operandi of the services.

4 How is the TIB informed?

What information does the TIB have and does it have sufficient information on which to base its decision? Does the TIB fully understand how the services operate? On the other hand, does the TIB risk obtaining one-sided information if it is only informed by the services? More generally: how is the TIB informed?

At the start of its work, the TIB completed an intensive induction and introduction programme. This programme provided information about the services' procedure, the intelligence process, the legal framework, the means to be used and the services' focus areas. That laid the groundwork on which to base the review of requests. During the past year, the TIB has further extended and updated its acquired knowledge through presentations on specific topics held by staff of the services and by speaking to external experts from the business community and social organizations. In addition to keeping up to date with general knowledge, it is important that the TIB is sufficiently informed in specific requests. This chapter looks at how the TIB is informed and makes inquiries.

4.1 Information in the case of a specific authorization request

The TIB reviews the authorization granted by the Minister for the use of a special investigatory power based on the request underlying that authorization. That request contains information about the investigation assignment and the specific investigation for which authorization is being sought, the person or organization against whom the investigatory power is used, which investigatory power is used and how it will be exercised. In addition, the request describes why the use is necessary, subsidiary, proportional and as targeted as possible. If an extension is requested, the request should also set out if the previous period(s) in which the investigatory power was used yielded any results. Where it concerns urgent requests, the urgency must be specified.

The request should contain sufficient information to review the granted authorization. The requests made by the MIVD contain extensive information about the scope of the operation, the investigatory power to be used and the results yielded where it concerned an extension request. The TIB is thus fully informed. In some cases the requests contain information about related investigatory powers used for which review by the TIB is not required. Thus the TIB obtains a full picture of the extent of the operation, allowing it to arrive at a balanced opinion.

The TIB has signalled that up to the end of 2018, the requests submitted by the AIVD were frequently incomplete or insufficiently transparent, as a result of which requests could not immediately be reviewed or the granted authorization was ruled unlawful. The TIB has no means of independently accessing the services' information systems to learn this information independently. The TIB can ask questions and in that way obtain the required information. In 12.3% of cases, the TIB asked questions regarding a request by the AIVD[29]. In the initial period in particular, the TIB was only able to review many requests (as lawful) after questions had been posed and answered.

The questions posed by the TIB are usually answered within a week. In some cases, the TIB considered the answers rather sparing. It is then necessary to ask further questions in order to

[29] This concerns the period 1 May 2018 to 31 March 2019.

obtain the information required to review a request. The TIB has repeatedly brought this to the AIVD's attention. Since the beginning of 2019, the TIB has seen a change for the positive. The information in the requests is becoming increasingly complete. The TIB has high hopes that the current positive development will continue.

Sometimes the TIB will ask the AIVD for certain information on a structural basis. For example in the case of selection lists. Investigation-specific interception consists of an acquisition phase, a processing phase and an analysis phase. In order to learn the contents of the acquired intercepted information (analysis), authorization must be sought from the Minister. The TIB reviews the granted authorization. These requests are also known as selection requests. These requests describe the persons, organizations or subjects against whom this investigatory power will be used. The services are authorized to establish selection criteria to conduct an investigation for which a selection requirement is submitted. These selection criteria are, for example, the persons who are targeted for selection and the telephone numbers, email addresses or key words on the basis of which their communication content is selected. These criteria are then placed on a list, known as selection lists.

It has occurred that a list for the selection of communication content contained the names of foreign journalists. The TIB pays sharp attention that the requested investigatory powers are not used against lawyers and journalists where the use could reveal their sources, as the TIB would then lack competence to rule[30]. In the first place it is up to the services themselves to be aware of this, and they generally are. Establishing lists containing selection criteria is a power belonging to the Minister or the head of the service that is not reviewed by the TIB. However, the TIB does consider it important to see the content of these lists on a structural basis, among other things to review whether the umbrella selection requests do not "select" persons who fall outside of the TIB's competency. These lists also provide an insight into the extent to which the requested investigatory power is as targeted as possible in the selection requests. The request to inspect the selection lists on a structural basis is now complied with.

4.2 Information on operations, trends and procedures of the services

In addition to information obtained from requests for authorization, the TIB sometimes asks for additional general information about a particular operation, a particular focus area or a particular procedure of the AIVD or the MIVD. This contributes to the TIB's knowledge of the broader context in which the requests are submitted. In this way, the TIB is also able to gain substantive in-depth knowledge about the means to be used and the underlying considerations. The services cooperate generously with these requests and staff have always proved prepared to hold presentations on various topics. The TIB is very positive about this.

4.3 Information from third parties

The TIB is aware of the fact that in reviewing requests, it could be presented with a one sided view of the balance of interests where fundamental rights are concerned. The TIB feels it is important to avoid habituation or tunnel vision. The TIB therefore also obtains information from other persons or

[30] Section 30 of the ISS Act 2017.

organizations than the services. In the past year, the TIB has held talks with companies in the ICT sector and Bits of Freedom, among others.

The focus of these meetings was on enhancing understanding of current technologies and infrastructure. This knowledge helps the TIB to review whether an intended use will be exercised as targeted as possible or what the technical risks could be of hacking.

These talks yielded valuable information about how these parties view the services' duties, the ISS Act 2017 and also the TIB itself. These talks provide the TIB with food for thought about how it can continue to develop its review of tasks and gain insight into the implementation of those tasks.

5 Results and findings

5.1 The quality of the authorization requests

The TIB had concerns about the quality of the requests made by the AIVD, in particular during 2018. The TIB raised this issue at various times because its lawfulness review is based on these requests.

As early as May 2018, the TIB raised a number of concerns with the Minister of the Interior and Kingdom Relations. These included the way technical risks were described when drafting hacking requests and the accuracy and comprehensiveness of the information in the requests. Initially this did not result in a sufficient improvement in the quality of the requests. In November 2018, the TIB again explicitly raised the issue of the worrisome quality of the requests with the Minister of the Interior and Kingdom Relations. To a large extent this included the same concerns as listed in the letter of May 2018. In addition, attention was demanded for the quality of the proportionality and subsidiarity considerations.

In December 2018, the AIVD took a number of internal measures to improve the quality of the requests. It is not up to the TIB to explain these measures in great detail as they are part of the AIVD's business operations. The TIB established that the quality of the proportionality and subsidiarity considerations has improved since the measures were implemented. There has also been a considerable drop in the number of unlawful requests as a result of avoidable errors (the lack of relevant text sections, an inconsistent request because of inaccurate copying and pasting, failure to report previous results in the case of extension requests, et cetera).

5.2 The TIB's decision-making period

Although the ISS Act 2017 does not prescribe a term within which the TIB must issue its decision, the TIB considers it important to keep the term as short as possible. Some requests are so self-evident that a review can take place relatively fast. Not much time is required to review an extension request where the circumstances are the same as in the initial request and where there are relevant results. A new request that raises fundamental points may take a lot of time. In that case the TIB will also take that time.

Requests are usually submitted early on Tuesday mornings. Tuesday is when the preparatory work is done. In general, the TIB members consult on Wednesday and on Friday morning. A decision on the majority of requests is taken on Wednesday. Requests requiring further discussion are (again) handled on Friday. If the TIB rules an authorization granted by the Minister as unlawful, it will have to substantiate its decision in writing. These decisions are generally submitted to the relevant Minister (and head of the service) on Thursday or Friday. If more time is required to carefully substantiate the decision - for example in the case of complex requests or fundamental decisions - the substantiated decision may be submitted to the relevant Minister in the following week.

5.3 Urgency procedure

The ISS Act 2017 provides for an urgent procedure, in cases where the use of an investigatory power cannot wait for a lawfulness review. That means that the services may use an investigatory power on the basis of the Minister's (generally) oral authorization, without a review by the TIB of that authorization in advance. The granted authorization must then be submitted to the TIB for review as soon as possible afterwards.

Thus the legislator implemented the principle that the TIB's review must take place before infringing the privacy of citizens. The TIB is of the opinion that only operational urgency can be considered a reason to lawfully use the urgent procedure. There is no reason to apply the urgent procedure if for example information on a target has been available for weeks but has not yet been processed.

In the past year, the MIVD applied the urgent procedure for 1.9% of the requests. The use of the urgent procedure by the MIVD was ruled lawful in all cases for both the use of the investigatory power and the application of the urgent procedure.

In the past year, the AIVD used the urgent procedure for 3.3% of the requests. For 88.4% of those urgent requests by the AIVD, the granted authorization in an urgent procedure was ruled lawful for both the use of the investigatory power and the application of the urgent procedure. In granted authorizations of requests by the AIVD, the use of the investigatory power and the urgent procedure were never both ruled unlawful. In 11.6% of the urgent requests by the AIVD, the granted authorization in an urgent procedure was ruled lawful but the use of the urgent procedure was not. In a number of cases this could be ascribed to insufficient substantiation of the reason for applying the urgent procedure. When the TIB deems the application of the urgent procedure as unlawful, it must review what should be done with any results generated up to the time of the TIB's review. In one instance, the TIB ruled that the information obtained up to that time had to be destroyed.

5.4 Number of regularities and irregularities

In the period from 1 May 2018 to 1 April 2019, the TIB reviewed a total of 2,159 requests.

For 4.5% of those requests from the AIVD, the TIB ruled that the authorization had been granted unlawfully. In the period 1 May to 1 October 2018 that was 5.5%. This decrease set in mainly after improvements were made by the AIVD since December 2018. The quality of the requests made by the AIVD has since increased and the number of avoidable errors has been reduced. The number of requests that had to be ruled unlawful decreased in this period. In the period 1 December 2018 to 1 April 2019, 2.1% of the requests by the AIVD were ruled unlawful.

The reverse seems true for the MIVD when the percentage of unlawful reviews is viewed in isolation. For 5.8% of the requests by the MIVD, the TIB ruled that the authorization had been granted unlawfully. That number was 4.1% in the period 1 May to 1 October 2018. However, this should be put in perspective. The TIB has not noticed a decrease in the quality of the requests

submitted to the Minister of Defence since it published its progress letter[31]. Expressed in absolute terms, the number of requests ruled unlawful is small. In the second half of the reporting period, separate requests were submitted that in fact related to the use of a single investigatory power. These requests were ruled to be unlawful. If this use had been submitted as one request, the percentage of authorized requests by the MIVD ruled to be unlawful would have been lower.

The services may repeatedly submit requests that have been ruled unlawful by the TIB. In the majority of operations, this will lead to modified requests being ruled lawful at some point, for instance because the investigatory power is used in a more targeted way or the infringement of fundamental rights is otherwise limited. In a number of cases, requests ruled as unlawful are not resubmitted by the services or these have repeatedly been ruled unlawful. In the reporting period, this was the case in 41% of the unique requests by the AIVD that were ruled as unlawful. This percentage for the MIVD was 44%.

5.5 Grounds for ruling requests as unlawful

The lawfulness review involves various relevant elements as described previously. Figure 1 shows in what proportion these elements contributed to a request being ruled unlawful. The figure relates to both the AIVD and the MIVD. There can be more than one ground for ruling a single request as unlawful. For example, the criterion *necessity* may be *inadequately substantiated* and the use of the investigatory power may then be ruled disproportional. In that case, a single request is ruled as unlawful based on *necessity*, *substantiation and information* and *proportionality* in the tally on which Figure 1 is based.

[31] https://www.tib-ivd.nl/documenten/brieven/2018/11/01/voortgangsbrief-tib-oktober-2018

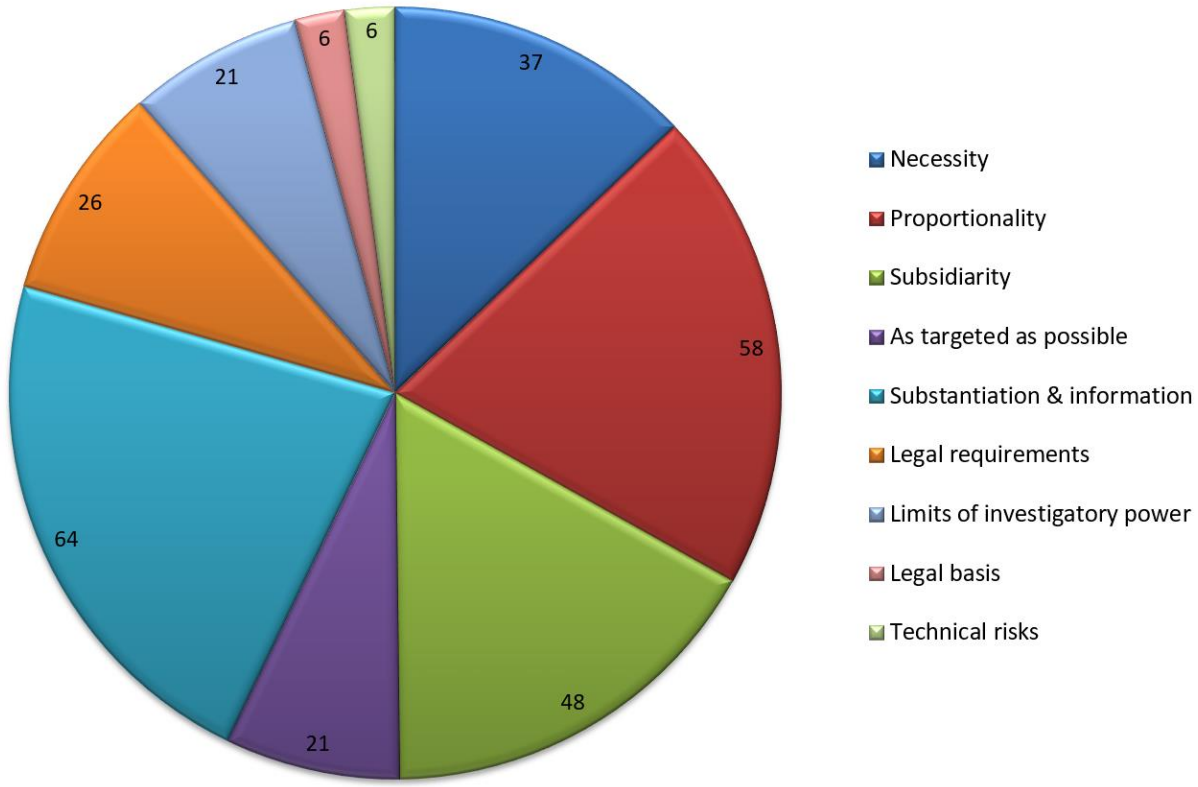

Figure 1 - grounds for unlawful conduct

Explanation regarding the assessment elements

The TIB assesses if the use of a special investigatory power is *necessary*, if its use is not incommensurate with the necessity (*proportionality*), if the goal can also be achieved through less invasive means (*subsidiarity*) and if the investigatory power is exercised *as targeted as possible*.

In addition, the TIB also assesses other aspects of lawfulness, including whether there is a *legal basis* for the use of the investigatory power, for example if the requested use corresponds with a section of the law. The TIB also assesses whether the use does not exceed the scope of the law (*limit of the investigatory power*) Furthermore, it is important that the requests to use investigatory powers contain sufficient *information* about the relevant facts and circumstances, but also that the required elements relating to the proposed use of the investigatory power are adequately *substantiated*. Where the hacking power is concerned, the *technical risks* must be explicitly described.

The following may serve as an example of multiple elements of the lawfulness review. The TIB ruled as unlawful a request for a bulk hack on a company to obtain the details of millions of people, including the details of 'targets'. The threshold for a bulk hack of this kind is high - there have to be considerable operational reasons[32].

> "In regard to compelling operational reasons, situations may be envisaged where there are one or more concrete signs that national security is directly at risk"

The sole fact that unspecified 'targets' also used the company's services was in this case insufficient *substantiation* of the *necessity* to justify the use against this company, according to the TIB. Furthermore, the use was not *subsidiary* because in this case it was possible to obtain the same information about targets by issuing a targeted search request to the company.

A significant percentage of the granted authorizations was ruled unlawful because the proposed use was not *proportional* (or proportionality had not been sufficiently substantiated). The infringement of privacy this would ensue ranges between a single individual and millions of persons. For example, it could be that the infringement of privacy of one or more housemates was not taken into consideration when intercepting a landline house phone. But it could also be that the infringement of privacy of people that are not the focus of the services' attention was not taken into account in a bulk hack to obtain all data of an organization.

A number of requests were ruled unlawful because they failed to meet the minimum legal requirements which authorization requests must meet[33]. These are requests, for example, in which it is unclear against whom the investigatory power is being requested (target's identity). This category also pertains to requests to extend an investigatory power, without describing the results (or lack of them) achieved so far. A number of requests were deemed unlawful due to the *legal basis* or the *limit of the investigatory power*, for example where services requested the investigatory power to compel companies that are not subjected to the duty to comply to provide information regarding users.

[32] CTIVD report no. 53, p. 20 and 27.
[33] Section 29 of the ISS Act 2017.

6 Conclusions and looking ahead

In the first year of its existence, the TIB built its organization and developed the lawfulness review. The TIB's review is a lawfulness review to the full extent. Sometimes legal uniformity meetings were held with the CTIVD about the implementation of the law in practice and letters were sent to the Ministers and the House of Representatives regarding the outcome. The TIB thus provides insight to everyone how the TIB reviews the use of investigatory powers.

The TIB has no means of independently accessing the services' information systems. It has to rely on the information gathered from the requests or from the questions it asks if the requests are unclear. The requests drafted by the MIVD were and are of good quality where it concerns the provision of information. After a difficult start in the first six months, the TIB now has the general impression that the provision of information by the AIVD has improved.

Requests made by the MIVD have been of consistent and high quality. In contrast, the TIB has repeatedly had to raise the issue of the quality of the AIVD's requests in the past year. However, since December 2018, the TIB has noticed an improvement and the number of AIVD requests ruled as unlawful has decreased as a result. The TIB considers itself sufficiently informed to make the necessary material considerations.

The years 2019 and 2020 will see important developments for the lawfulness review and the TIB's organization. This year the cabinet is expected to put to the House of Representatives a proposed change to the ISS Act 2017. The debate on this law is relevant to the TIB in view of the codification and explanation of the criterion 'as targeted as possible'. In addition, the Ministers have already committed, through answers to parliamentary questions, to provide for the option in the amendment of appointing deputy members of the TIB.

Next year will also see the start of the evaluation of the ISS Act 2017. In preparation for this, the TIB will record relevant observations made during its lawfulness reviews, so that these can be made available to the evaluation committee. In the coming year the TIB will, following the insight offered in this annual report, search for ways in which it can continue to provide insight on how it conducts its reviews and which aspects are involved in those reviews.

Furthermore, the TIB aims to continue to invest in its expertise, to stay abreast of the latest developments in the security domain regarding technology and oversight. The meetings with third parties provide an understanding of the other parties' views and keep the TIB on its toes for conducting its review.

The TIB looks forward to informing you on its activities again next year.

7 Composition of the TIB

The Investigatory Powers Commission consists of three members. One of the committee members is chair. At least two of the three members must have a background as judge. The third member does not require a judicial background but may be appointed on the basis of technological expertise. That is currently the case. The committee is supported by a secretariat.

Figure2 - Composition of the Investigatory Powers Commission

Pictured from left to right:

- A.R.O. (Lex) Mooy, member
- A.P.M. (Paul) Pols, deputy secretary
- M. (Mariëtte) Moussault, chair
- L.W. (Lennart) Schroijen, secretary
- J.R. (Ronald) Prins, member